Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems

Jae Hyung Lee

Working Paper CISL# 2019-05

February 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems

by

Jae Hyung Lee

B.S., University of Oregon (2001)
M.S., Carnegie Mellon University (2004)

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

February 2019

Signature of Author _____
System Design and Management
January 18, 2019

Certified by _____
Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management &
Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Accepted by _____
Joan Rubin
Executive Director, System Design & Management Program

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgement

Foremost, I would like to express my sincere gratitude to my thesis supervisor *Prof. Stuart Madnick* for everything about this paper. This work would not have been possible without his encouragements and directions. His challenges brought this work towards a completion.

My sincere thanks also goes to *MIT SDM* program, including the faculty, staff and classmates; it has been a wonderful experience and learning opportunity. Special thanks to *Pat Hale*, who welcomed to the *SDM* conference 4 years ago, later encouraged me to apply.

Nobody has been more important to me in the pursuit of this project than the members of my family. I would like to thank my parents, whose love and guidance are with me in whatever I pursue. They are the ultimate role models. I am also very thankful to my two wonderful children, *Anais* and *Ines*, who provide unending inspiration. Most importantly, I wish to truly and deeply thank my loving and supportive wife, *Eunhee*. This thesis is heartily dedicated to her who encouraged me and prayed for me throughout the time of my research.

THIS PAGE INTENTIONALLY LEFT BLANK

Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems

by

Jae Hyung Lee

Submitted to the System Design and Management Program on January 18, 2019
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

ABSTRACT

Recent hacks into blockchain systems and heists from such systems have raised serious questions about whether this new technology can be secured from ongoing, evolving cyberattacks. While the technology is known to provide an environment that is fundamentally safer than other existing centralized systems offer, security professionals warn that the current blockchain ecosystem is still immature, harboring many known as well as unknown defects [1].

This thesis draws upon a number of research studies and various other inquiries into blockchain systems security. In addition, this paper gathers and summarizes information regarding 78 recent blockchain cyberattacks and heists, analyzing and categorizing them as to their cause: platform breach, dApps exploit, access point attack, or endpoint hacking. Two of these attacks (the Ethereum blockchain system and the Bitfinex cryptocurrency exchange) are analyzed in detail using Causal Analysis using System Theory (CAST) method.

A novel top-down security assessment method inspired by System Theoretic Process Analysis for Security (STPA-Sec) is used to evaluate a sample blockchain system, such as might be proposed for voting. An analysis of possible vulnerabilities is conducted, and suggestions for remediation and protection.

Thesis Supervisor : Stuart Madnick
Title : John Norris Maguire Professor of Information Technologies,

MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1 - Introduction

"Never have so many people sought so much from a technology understood by so few, like Blockchain."

- Forrester Research

1.1 Blockchain fever

Blockchain technology is currently the most significant topic in the IT industry. In the last couple of years, blockchain has made the headlines in business and technology news, as business leaders continue to admire the success stories of cryptocurrency and smart contracts [2]. Numerous major companies around the world have made tremendous strides in adopting Blockchain technology as shown in Figure 1.1 below. For example, Nasdaq and Citigroup announced their new integrated payment solutions that enable straight-through payment processing and automated reconciliation by using Blockchain's distributed ledger technology [3]. FedEx also announced testing of its new Blockchain system for commercial supply chain use with critical cargo shipments [4]. Lo3energy, an energy supplier based in Brooklyn, New York, implemented a Blockchain system to improve the tracking of clean energy [5].

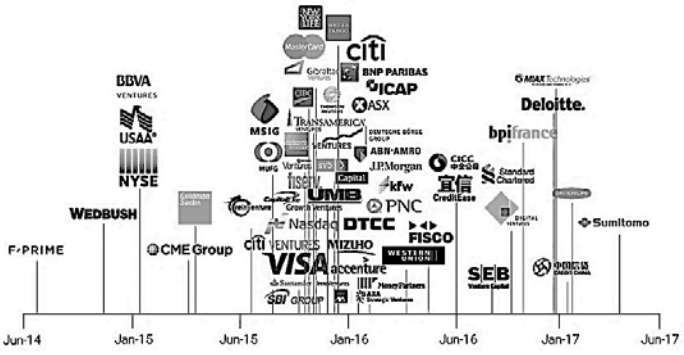


Figure 1. 1 – Early Investment of Financial Services Industry in Blockchain [6].

With its explosive popularity, Blockchain technology has now grown to an industry of $339.5 million in annual revenue in less than 10 years since its inception. The market for the technology is expected to grow to $2 billion within the next couple of years as seen below in Figure 1.2. Moreover, as of April 2017, cryptocurrency and Ethereum, the two best known applications based on Blockchain technology, have a total market value of about $2.3 billion and

$6.3 billion, respectively [7]. From finance and capitalization, to supply chain, social media, digital ID management, to IoT devices around us—replacing or upgrading existing technology with a Blockchain system has become a must-do trend in the IT industry. It is believed that this technology will lead a tremendous revolution in our daily lives, similar to the impact of the Internet in the mid-1990s [8].

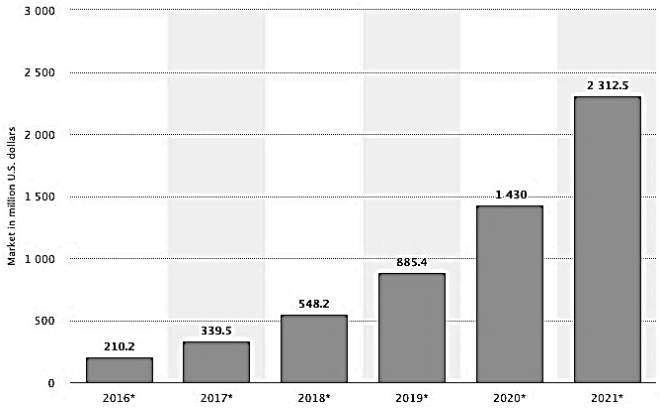


Figure 1. 2 – Size of the Blockchain Technology Market Projection from 2016 to 2021 in World Wide [9].

1.2 The revolution of system safety and security

In simple terms, Blockchain technology is a public ledger of data transactions in decentralized form. As the word *public* indicates, the same ledgers are stored on all nodes, or participants, within a system network.

	Safety and Security Features of Blockchain
Decentralization	No single point of failure. All node can view data transactions in the system network.
Confidentiality	Users verify identity with public-key cryptography as authentication. This guarantees anonymity of transaction and transmission of data.
Integrity	All data transactions are signed and time-stamped, so all node can easily validate and trace history of transaction.
Transparency	All data transactions should have a consensus from all node in the system network.
Immutability	Once data are added, they cannot be modified or destroyed.

Table 1. 1 – Main advantages of Blockchain technology for cyber security [10].

In other words, every node will obtain the same copy of the public ledger and will also have simultaneous updates as any data changes within the system. Therefore, all data transactions occurring in the system can be viewed, validated and verified by all peer participants. Such transparency of data management makes it virtually impossible for one actor within the system network to invisibly alter the ledger. This is the primary reason Blockchain technology is currently considered to be unbreakable and a game changer in the system security industry [10]. Above Table 1.1 summarizes the subset of major advantages of Blockchain technology from the system security perspective.

1.3 Motivation of research

Despite the common notion that Blockchain technology is virtually impossible to hack, the Blockchain system has been subject to numerous cyberattacks in recent years. In 2017, more than 10 percent of all cyberattacks in the world targeted Blockchain systems [11]. Further, the annual growth rate of hacking incidents and their loss against Blockchain systems surpass all other types of IT systems during their technology maturity periods.

Some IT specialists consider these phenomena as a natural pattern of cyber threats against emerging technologies, because as new technology becomes popular, the number of cyberattacks against that technology inherently increases. Many researchers also point out that most system implementations of Blockchain technology has been focused solely on the cryptocurrency industry, where huge financial transactions provide high monetary rewards to a hacker once a cyberattack succeeds.

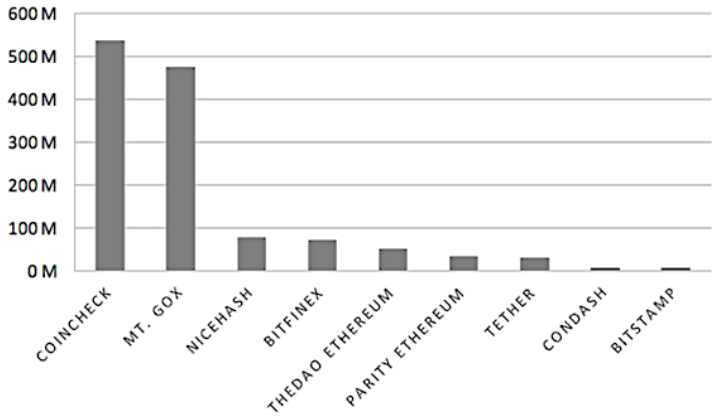


Figure 1. 3 – Biggest crypto currency hacks in dollar amount, as of Dec. 2017 [12].

In researching numerous cyberattacks against Blockchain systems, one surprising theme emerged: despite the number of security incidents, most victims still believe the Blockchain system remains safe, sound and secure. They looked outside the system for the root cause of the heists and the cyberattacks, such as human mistakes, programming errors, immature usage of technology or even government regulations. This research paper was motivated by this question:

Blockchain is widely considered the most secure and hack-proof of all systems, so why is it still subject to cyberattacks?

1.4 Thesis questions

The following thesis questions are proposed from a system safety control perspective:

Thesis question #1 ***How different are Blockchain and traditional centralized systems in terms of system security control?***

This paper starts with an explanation of differences between centralized and decentralized systems, then describes the complex technology in simple terms and discusses the technology adoption as well as limitations of Blockchain from system security perspectives.

Thesis question #2 ***Why does a Blockchain system become the victim of cyberattacks?***

This paper identifies reasons that Blockchain systems allow cyberattacks even though its core technology provides strong security protections.

Thesis question #3 ***What are the vulnerabilities and security risks of a Blockchain system?***

This paper discovers and summarizes security weaknesses and cyber threats, which Blockchain systems have experienced.

Thesis question #4 ***What are the technical difficulties to preventing cyberattacks on a Blockchain system?***

This analysis focuses on identifying root cause(s) of security incident(s) occurring in Blockchain systems. The analysis utilizes known causal analysis framework and compares it with centralized systems from the aspect of system security.

Thesis question #5 ***How can a Blockchain system detect and remediate potential security threat(s) in advance?***

As the final goal, this paper suggests possible ways Blockchain systems can prevent exploitation and theft from cyberattacks.

1.5 Research and exercise

In this paper, the following exercises answer the above-referenced questions from a system security perspective:

Exercise #1: ***Establish security control domains in Blockchain systems.***

From a system control point of view, I created a security domain for a block-chaining system that collects computer and network components. This exercise helps to identify security flaws in the distributed system architecture from a high-level perspective.

Exercise #2: ***Review heists and hacking incidents against Blockchain systems.***

In order to better understand the scope and depth of recent cyberattacks, I have gone through a comprehensive review of publicly known hacking targeted to Blockchain system. The reviews examined system security holes, exploitation techniques, financial loss and the incident responses.

Exercise #3: ***Categorize Cyberattacks against Blockchain systems.***

This exercise categorizes each hacking incident into the security control domain model developed in Exercise #1 with information obtained from Exercise #2. It discovers exploitation techniques and security vulnerabilities of Blockchain systems as victims of cyberattack.

Exercise #4: ***Conduct causal analysis of security incidents against Blockchain systems.***

This analysis focuses on identifying root cause(s) of security incident(s) in Blockchain systems. The approach involves both causal analysis and systematic comparison with other centralized systems from a security perspective.

Exercise #5: ***Design a security diagnostic framework for Blockchain systems.***

This design proposal attempts to suggest novel cybersecurity risk-elicitation methods by modifying existing STPA-sec. This includes a new hazard analysis technique and “best practice” security guidelines for Blockchain systems.

1.6 Structure of thesis paper

As shown in Figure 1.4 below, this thesis paper consists of a total of 6 chapters (excluding Chapter 1 as the overall introduction and Chapter 8 as future work). To obtain a reasonable systematic approach to analyzing the security vulnerabilities of the Blockchain system, each chapter sets different but closely related research goals to its following chapters. Results throughout the study and exercises in each chapter will be used for later chapters.

The goal of Chapter 2 is exploration of Blockchain in terms of technology, the motivation for this study. In Chapter 3, security domains will be established for the Blockchain system for a systematic approach to analyze cyberattack(s) and security vulnerability(s). The goal of Chapter 4 is investigation of real cyberattack cases targeting Blockchain systems by applying the security domains established in Chapter 3. In Chapter 5, a causal analysis framework will be proposed for in-depth security incident analysis. Chapter 5 also applies the framework to significant cyber incident cases from Chapter 4, where similar types of cyberattacks have continued for a long period of time. Chapter 6 will discuss the common misconceptions and difficulties associated with Blockchain system security with appropriate solutions for each of the security vulnerabilities identified in Chapter 4. The goal of Chapter 7 is to propose a security assessment methodology for Blockchain systems as concatenation of all research throughout this thesis paper.

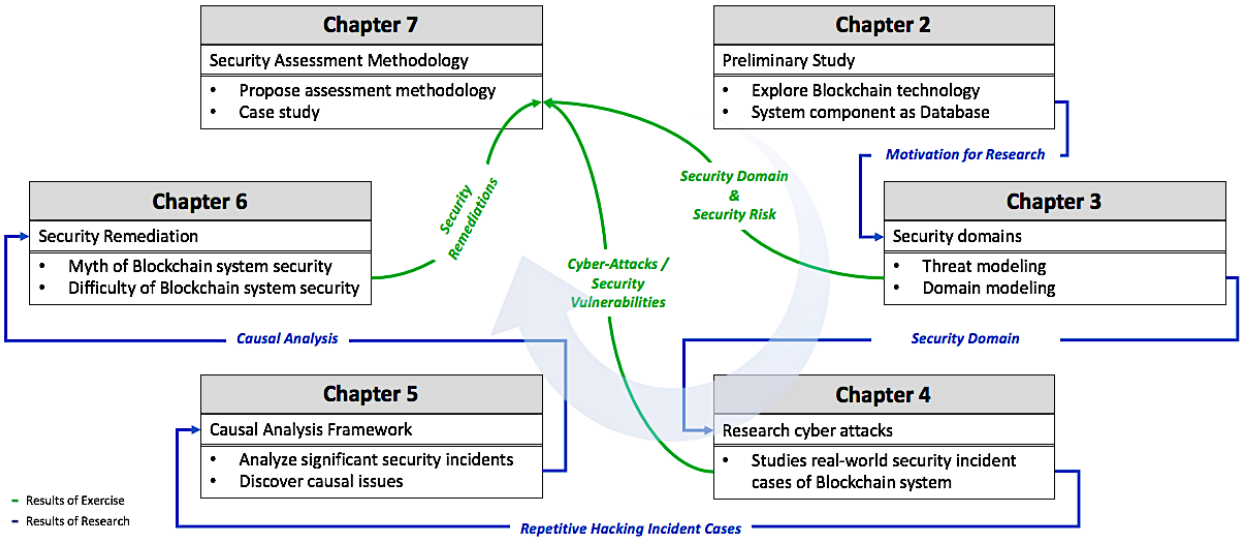


Figure 1. 4 – Structure of this thesis paper.

CHAPTER 2 - Database for Autonomous Systems

"Blockchain pays for autonomy by sacrificing everything else"

- Bharath Rao, the founder of Ethereum exchange, Leverj [13]

2.1 The birth of blockchain technology

The initial form of Blockchain technology originated in 1991, as shown in Figure 2.1. A paper entitled, "How to Time-Stamp A Digital Document," introduced a trusted timestamping protocol which can guarantee the integrity of data within a chain structure and maintain the privacy of data in an unaltered state without system level record keeping [14]. The following year (1992), Bayer, Haber and Stornetta presented a primitive form of Blockchain technology in their paper entitled "Improving the Efficiency and Reliability of Digital Time-Stamping." The Merkle tree is integrated into a reliable timestamping protocol that collects multiple documents and stores them in a single data type called a *block* [15]. For the next 20 years, however, this technology did not receive much attention due to the emergence of centralized systems.

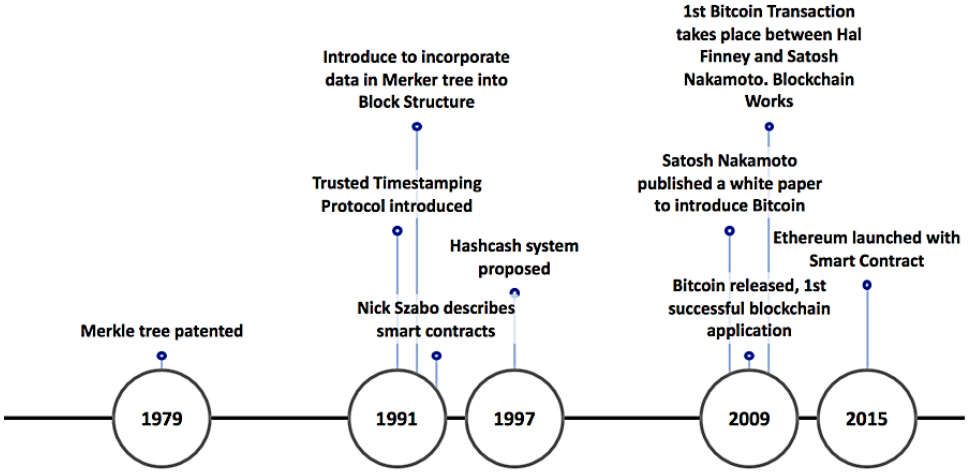


Figure 2. 1 – Brief History of Blockchain [16].

2.2 The Realization of DAO

Blockchain technology began to attract attention again with the introduction of the Distributed Autonomous Organization (DAO). A DAO is an organization that aims to operate without

centralized authority or control. Let's imagine an example of DAO using a taxi service with a self-driving car. Suppose that an owner is able to program the self-driving car and is also able to set up its taxi-service operation rules, such as connecting Internet-based taxi service providers (Uber or Lyft) to provide customers. Once the owner completes the initial setup, the car will drive out by itself and will start providing taxi service to passengers according to direction from Uber or Lyft. When the car runs out of fuel during the service, the car drives itself to recharging stations, refuels by paying from its collected fares, and then goes back into service, and so on [17] [18].

Except for initial investments, such as the purchase of the self-driving car and programming the operation rule set, the small taxi service organization does not need to control or manage to perform its mission. This example of a self-driving taxi service is a very simplified form of DAO that can create monetary benefits through autonomous operation and can operate infinitely as a source of profit. For many years, the implementation of DAO in cyberspace was the dream of many system researchers and computer scientists. But commercialization was not realized due to various technical difficulties.

In 2009, the very first practical DAO was introduced to the computer Internet space in the form of cryptocurrency called Bitcoin. For the first time, Satoshi Nakamoto published a short paper entitled, "Bitcoin: Peer-to-Peer Electronic Cash System," which covered the concept and operation of the cryptocurrency system as a DAO [19]. Much before Bitcoin became known to the world, there have been many attempts to implement peer-to-peer (P2P) digital currency transactions in a distributed manner. However, it was very difficult to keep the security and integrity of the system data even after completely removing the central authority [20]. Satoshi was able to solve these problems by adapting Blockchain technology. The technology addressed problems of decentralization by adding the following two innovative operations to the system.

First, is distribution of data (ledger) to all nodes, so they are transparently monitored by the entire system network. Since all system activity is watched and reviewed by all peers (users), the system can operate in a secure state without any centralized control and governance. Second, is incentive structure for data set (block) processing. Blockchain is designed to provide financial compensation to the node (user) that has succeeded in creating a new data set (block) and adding the data set to the existing data chain (Blockchain). Financial compensation is funded from the profits generated through the operation of the encrypted currency system, which collects a certain percentage of the transactions between users. With such an ingenious structure, the cryptocurrency system can be operated as a DAO [21].

Below, Figure 2.2 shows how an incentive structure runs a cryptocurrency system on its own fuel without centralized authority in system dynamic view. As the number of data transactions in a cryptocurrency system increases, so does the total amount of transaction fees. As the fee total increases, the miners will have a greater chance of reward, and more miners will voluntarily participate in the system network. The involvement of more miners makes the operation of the system much more stable, and the increased stability of the system leads to more user participation, resulting in more commissions. Hence, once the system operation rules are set

and begin to run, the Blockchain-based cryptocurrency system operates infinitely as a DAO, which does not require any type of maintenance and management.

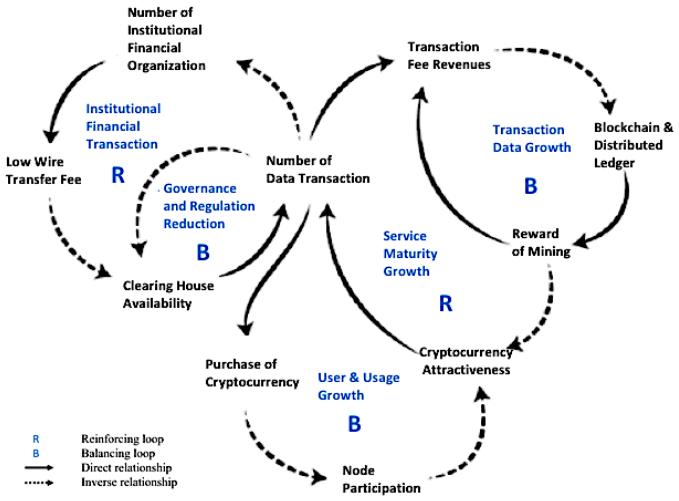


Figure 2. 2 – Overview of autonomous operation in Crypto Currency Blockchain System.

2.3 How does Blockchain work?

For exploration of the technology, this section describes how Blockchain works from a high-level view. The main process in Blockchain is adding transaction records to a public ledger that lists past transactions. The collection of records is called a block. The public ledger of past transactions is called the Blockchain, as it is a chain of blocks. The Blockchain is responsible for verifying to the network that a transaction has occurred. A node (user) on the Blockchain network verifies the validity of the transaction and prevents attempts to misuse or alter legitimate data transactions. [22]. As shown in Figure 2.3, the process within Blockchain is divided into six phases: initial request of data transaction, initiation of new block creation, start mining, complete mining, validation of the new block and chaining of the new block at the end.

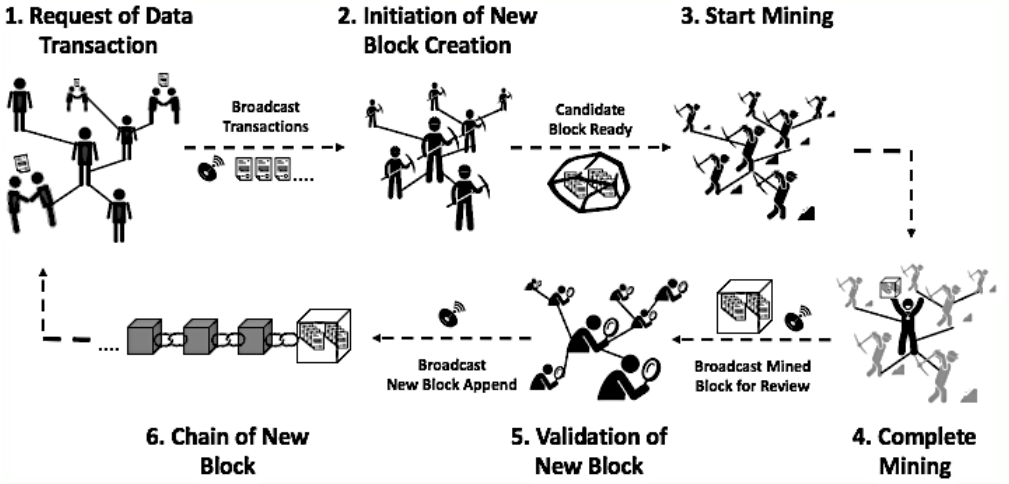


Figure 2. 3 – Overview of how a Block is added to Blockchain.

1. Request of data transaction

Nodes are Blockchain users with access (usually via the Internet, in this case) to the Blockchain network that stores all the transaction data from the very start as a chain of information called blocks [23]. Once any of two nodes (users) initiate a data transaction, the data broadcasts to the entire system network. For example, in a cryptocurrency Blockchain system, a data transaction is information about movement of cryptocurrency from one node to another, recording the sender, receiver, time of initiation and amount of cryptocurrency. Typically, during the system's operation, a huge amount of broadcasting occurs simultaneously between nodes (users).

2. Initiation of a new block

Miners are responsible to validate new data transactions and record them on the global ledger, known as Blockchain. At this initial stage prior to actual mining, each miner independently verifies the validity of all new incoming transaction data, such as compliance with the Blockchain protocol, identity verification using digital signatures, and conflicts with previously viewed transactions [24]. Once validity of data is confirmed, the miner begins to organize these transactions as part of a candidate block. Candidate blocks are created individually and locally by the miner, but are not yet part of the blockchain at this stage.

Miners continue grouping all valid transactions into candidate blocks until the candidate block reaches the predefined size limit set by the protocol. When the candidate block is ready for the mining process, the miner records the timestamp of the information transaction and the previous block's hash value (cryptographic signature) into the header of the candidate block. Using timestamps, Blockchain can chain data linearly to avoid

duplication. Using the previous block's hash values, Blockchain can keep the data block secure from alteration, which is illustrated as the value of the second row within the new Block Header in Figure 2.4 below and also illustrated as chains between two blocks in Figure 2.5 below.

3. & 4. Starting and completing mining of a new block

After the candidate block is completed, the miner starts its mining process, called puzzle-solving. Puzzle-solving is a process for obtaining a cryptographic value known as *hash*: in this case, Block ID or Proof-of-Work (PoW). To solve the hash puzzle, the miner puts a given set of data (in this case, the candidate block) through a hash function: for Bitcoin cryptocurrency the hash function is SHA-256.

On modern computers, generating a hash for data is trivial, so to turn this simple process into a valuable task, Blockchain sets a certain level of difficulty. For example, Blockchain gives the miners a puzzle to find a hash value starting with, say, "10 zeros in the candidate block." The miners continue to adjust the *nonce* (number used once) value in the candidate block header while putting the candidate block into the hash function to find a hash value starting with 10 zeros.

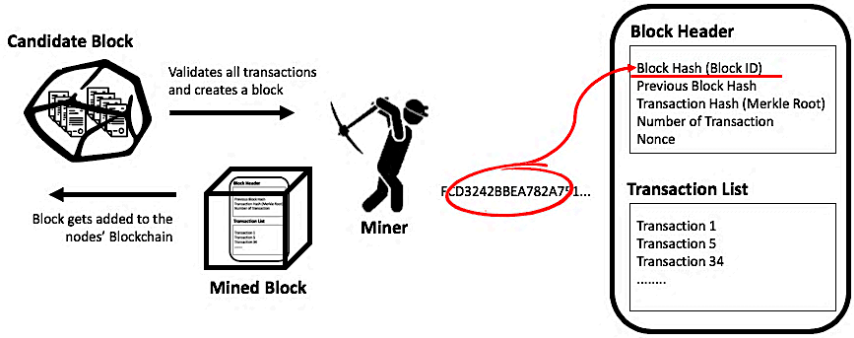


Figure 2. 4 – Block mining requires calculation of "Proof of Work" and the calculation is going to be used as Block Hash (Block ID).

Note that the miner can change only the nonce value in the candidate block. The remaining fields of the candidate block have a defined meaning and cannot be altered. Also, note that it is not easy to find the hash value in the candidate block except to continue to change the nonce value and attempt to generate the hash [25]. In other words, puzzle-solving (mining) is a competitive process, but it also needs to be more of a lottery than a race. Blockchain intentionally designed it simple to attract more participation to the network, but time consuming and resource intensive for fairness to all participants. Otherwise, one miner or the group can become the only producer of the blocks and potentially dominate and control the entire Blockchain.

Once the puzzle is solved, to obtain a desired hash value, a miner is able to complete the mining process by adding the hash value into the block header as illustrated in Figure 2.4 [26]. Individual blocks must contain its own PoW (Proof-of-Work) within its header to be considered as valid data set. The low probability and unpredictability of PoW thus serves as an important safeguard for the Blockchain system to address data security and integrity issues without central control [27].

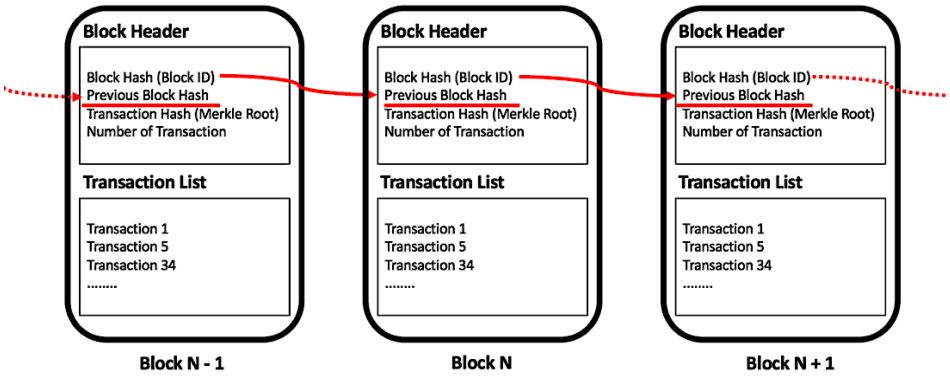
5. Validation of the new block

After a block is successfully mined, the miner forwards the block, broadcasts to the network and waits for confirmation by another node. The network nodes (users) then start validating the mined block. If the nodes find something incorrect or a discrepancy, the block is rejected. If not, the block will obtain consensus from the entire network's nodes and be ready to join the existing data chain (Blockchain).

However, please note that due to the *avalanche effect*[1] even a tiny change to any portion of the original data will result in a totally unrecognizable hash. Whatever the size of the original data set, the hash generated by a given function will be the same length [28].

6. Chain of the new block

The validated block is timestamped and added to the chain in a linear and chronological order. The addition to the existing data chain (Blockchain) is broadcast to the entire system network and distributed to make changes for locally stored public ledgers [29]. The miner who created the newly appended block becomes the winner and receives financial reward from the incentive structure of the Blockchain.



[1] In cryptography, the avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. The actual term was first used by Horst Feistel, although the concept dates back to at least Shannon's diffusion [431].

Figure 2. 5 – Appending Blocks to Blockchain in simple view.

2.4 Technology for autonomous data management, but not for security

As explained in previous sections, Blockchain is a technology for data management in the distributed system environment. The adoption of the technology aims to achieve fail-proof, infinite system operation that is self-fueled without central intermediaries. That is, Blockchain technology is not designed to protect the entire system environment. The use of this technology can securely store information in a decentralized system environment, but system security is not the ultimate goal of this technology.

For example, Blockchain's data security is maintained by distribution of the same data to entire nodes. The meaning of security in this way is limited within the inherent permanence and invariance. For instance, Blockchain cannot handle data which requires privacy, such as military classified data or corporate business secrets. Further, Blockchain cannot perform other data processing besides storage, such as modification and deletion. This indicates that separate security protections must be implemented to protect the rest of the data processing tasks other than Blockchain at the system level. Therefore, it is dangerous to assume that Blockchain can secure an entire system environment, making it invulnerable to outside cyberattacks. Even if the discussion about the technology were confined to database domain, Blockchain is not superior to any centralized database in any aspect besides decentralization.

Table 2.1 below summarizes the comparison between Blockchain and a central database. In terms of functionality and performance, the comparison between a centralized database and Blockchain cannot conclude that Blockchain manages system data better than a centralized database.

	Central Database	**Blockchain** (permission less)	**Difference in Blockchain**
Transaction	2000 Data Transaction/sec	7 Transaction/sec.	One block will be added to the chain in every 10 min. VISA requires at least 300 Trans/sec.
Latency	Fast	Low	Append new data block requires multiple level of consensus.
Throughput	High	High	
Number of Readers	High	High	
Number of Writers	High	High	
Number of Un-trust Writers	None	All	Any node participated in Blockchain cannot be trusted. Blockchain relies on notion of "majority". Even if one or

	Central Database	**Blockchain** (permission less)	**Difference in Blockchain**
			some node turns in to be malicious, other majority of participants can maintain data security.
Fault-Tolerance / Robustness	Depends of system architecture.	High	Fault occurrence rate might be low on Blockchain. However, when system mal-function or mis-function, central DB provides better robustness.
Data Type	Any type is possible.	Very limited.	Only one kind of data can be used in Blockchain.
Accessibility	Accessibility is controlled in multiple layers: Authentication, Authorization, Input validation.	Only one access control by Authentication.	Anyone can participate in the Blockchain. Simple identification is needed for access.
Alteration / Immutability	Data can be added, changed and deleted.	Data can only be appended.	Data cannot be altered.
Integrity	High	High	
Transparency	Optional. Controlled based on data requirement.	All data is transparent as design.	Central DB can also make whole data to public.

Table 2. 1 – Blockchain vs. Centralized Database in financial IT system [30].

CHAPTER 3 – Blockchain System Security Domains

"People like to understand and categorize things in order to understand."

– Max Riemelt, German Actor

3.1 Blockchain is decentralized, but its system is not

Chapter 2 confirmed that Blockchain technology can autonomously operate its system without refueling or central control. However, to drive more node (user) participation, the technology has this limitation: the system needs to be publicly opened (decentralized) and the system must have a business model that includes an incentive structure.

Moreover, as briefly mentioned in Section 2.4 of Chapter 2, the only role of Blockchain technology is to record system data and to maintain the integrity of the recorded data in a decentralized system environment. Table 3.1 below lists the sub-elements that make up the cryptocurrency system currently considered the most common form of Blockchain. According to the table, a Blockchain system consists of a mixture of centralized and decentralized system components. When system components are intricately interconnected, its architecture becomes complex. This complexity makes system security more difficult and generally requires more security protection. Therefore, it is hard to believe that the use of one type of database can protect the entire system's boundary. In conclusion, a Blockchain system should also implement security protection for its components from cyberattack in the same way centralized systems do.

Blockchain System Component	Example	Description
Authentication Service (3rd party)	ChainID, Multi-sig, etc.	Multi-geniture (Multisig) refers to requiring more than one key to authorize a crypto-currency transaction. The 3rd party authentication solution is generally used to divide up responsibility for approval of transaction request [31].
Decentralized Applications (dApps)	Golem, Augur, Argon, etc.	Applications established on Blockchain. Due to the characteristic of blockchain technology, dApps is autonomous, un-stop-able and does not require a middleman to function or to manage a user's information. Currently, the two most successful dApps are crypto-currency and Ethereum [32].
Digital Wallet	Airbitz, Copay, Parity, etc.	Digital wallet stores the public and private keys which can be used to receive or spend a cryptocurrency. A wallet can contain multiple public and private key pairs [33].
External Interface	Web host service, Web Server, etc.	System components for external interface in Blockchain system are the same as existing centralized system.

Blockchain System Component	Example	Description
Key Storage	Hot & Cold storages.	Hot wallet refers to any cryptocurrency wallet connected to the internet. It is easy to setup, access, and use. However, hot wallets are also more susceptible to cyberattack. On contrast, cold storage refers to any cryptocurrency wallet disconnected from the internet. It is not each to access and use, but considered more secure than hot wallet. Usually, hot wallet is provided in a form of software (web application), but cold wallet is provided in a form of hardware (USB key) [34].
Network Device	Router, Switch, DNS, VPN, IDS, etc.	System components for Network Devices in Blockchain system are the same as existing centralized system.
Nodes	Personal computer (PC), mobile phone, printer, any IoT device, etc.	Node (user) can be any active electronic device, as long as it is connected to the network or internet. The role of a node is to support the network by maintaining a copy of a Blockchain (public ledger) and, in some cases, to process transactions [35].
Miners	AntMiner, Avalon, Bitmain, etc.	Miners can maintain Blockchain network secure by approving transactions. Mining is an important and integral part of Blockchain that ensures fairness while keeping the Blockchain network stable, safe and secure [36].

Table 3. 1 – Simplified list of Blockchain system components [37].

3.2 Difficulty securing a decentralized system in autonomous operation

Figure 3.1 below illustrates data flows between system components of a Blockchain system in simplified form. In most cases, a node (user) communicates with Blockchain through one of three channels, including distributed applications (dApps), online web-based wallets with Multi-Sig authentication, or third-party organizations or exchanges (as in the case of cryptocurrency). As shown, after a node (user) is authenticated, no further data protection or security controls any data originating from that node (user) to the Blockchain.

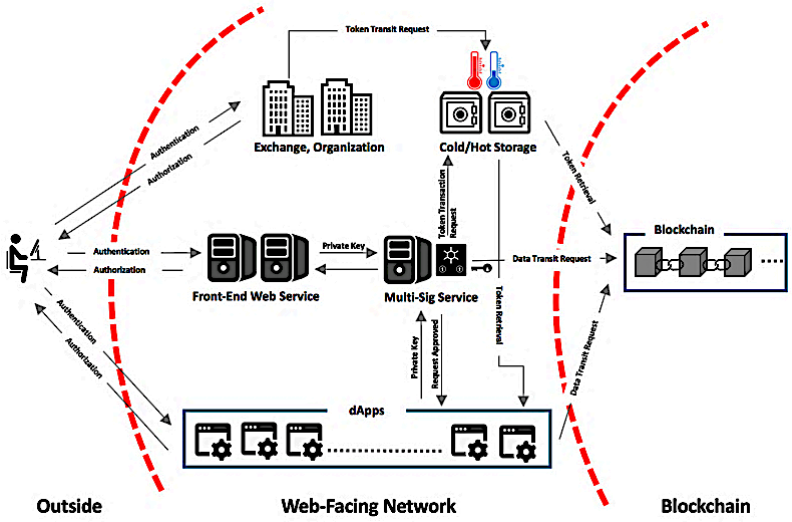


Figure 3. 1 – Simplified data flow in Blockchain system.

In other words, authentication is literally the only security control in the Blockchain system. This is mainly due to the character of the technology, which requires open access to the network node (user) for autonomous operation. This structure makes it difficult to implement security controls other than strong cryptography-based authentication. Further, as previous research in Chapter 2 has shown, Blockchain technology only guarantees the security of system data inside the Blockchain boundary from external threats. Therefore, no matter how secure your data is within Blockchain, robust authentication mechanisms alone cannot provide adequate security for the entire system.

Figure 3.2 below illustrates the comparisons of architecture and data flow between the two systems at a high level. In the centralized system described on the right, system components are grouped and placed in their respective hierarchies. This means that only certain paths can exchange data both inside and outside the system, minimizing the cyberattack surface. In other words, centralized system architecture is clear for on where to place its security control components to prevent potential cyber threats. However, in Blockchain-based decentralized system architecture, the system’s layers are not clearly delineated. Failure to adequately protect system boundaries increases the system's attack surface, which increases the number of hacking and exploitation attempts. The increase in hacking and exploitation attempts suggests that the system is likely to become a victim of cyberattacks. In addition, without centralized control and management in the distributed system’s architecture, cyberattacks can have a devastating effect on incident response and emergency response for the Blockchain system.

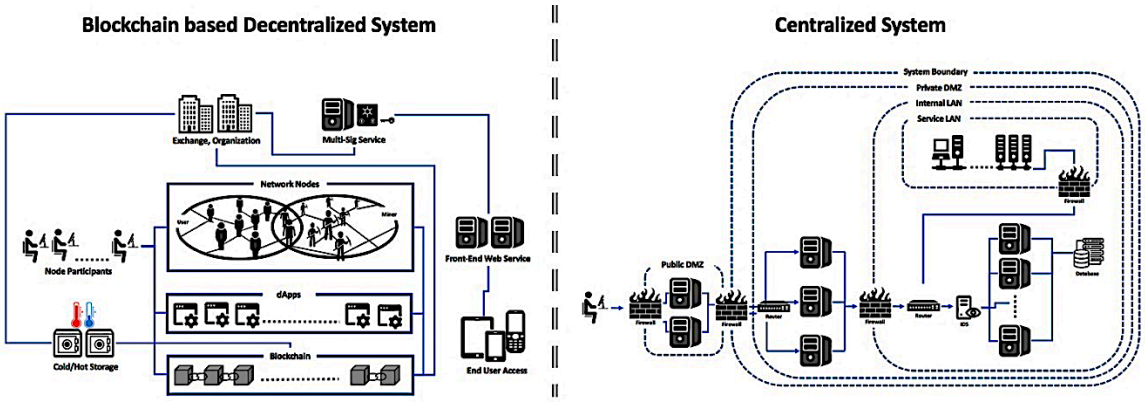


Figure 3. 2 – Distributed (Blockchain) vs. Centralized System: To exploit centralized system, attacker should be able to penetrate or bypass firewall, intrusion detection system, network monitoring to reach actual hacking targets such as database, application server etc. However, a Blockchain system contains sustainably fewer security related components that protect and monitor cyber threats than centralized system does. There is no security system control component other than user authentication in Blockchain system boundary.

3.3 Threat modeling

Threat modeling is a common exercise conducted by most organizations to approach cyber threats more systematically and identify potential system security issues in advance [38]. In order to fully analyze hackings and security incidents to Blockchain systems in Chapter 4, this section performed threat modeling exercises. The goal of these exercises is to categorize Blockchain system components in terms of system security, then establish security domains specifically for Blockchain systems (described in Section 3.4) [39].

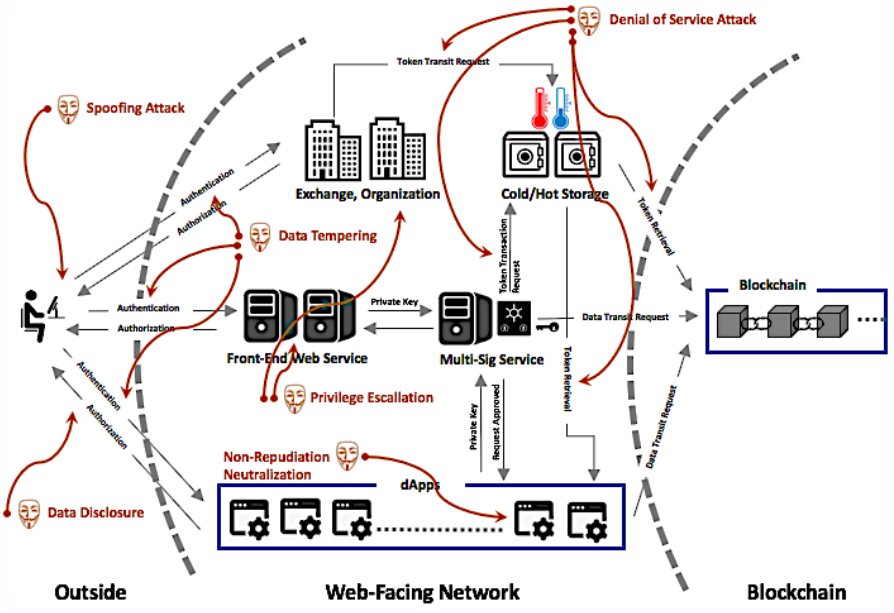


Figure 3. 3 – Results of threat modeling on Blockchain system.

Throughout this threat modeling exercise based on the data flow of a Blockchain system, as illustrated in Figure 3.1, a total of six potential Blockchain system security threats were discovered as shown in Figure 3.3 above. First, it uncovered a cyber threat of data spoofing, a situation in which a person or program successfully masquerades as another by falsifying data to gain an illegitimate advantage [40]. In general, this threat exposes a system to cyberattacks attempting to steal transmitting data or eavesdrop on communication channels for identify theft, breaking into a secure channel or interrupting user access. Threat modeling also discovered the cyber threat of data tampering, an act in which user-submitted data is changed to malicious data. In general, data tampering exposes a system to data manipulation causing incorrect or unintended system execution including: component tampering, data corruption, data manipulation or ledger malleability that corrupts Blockchain protocol. Another cyber threat, denial of service, is a situation in which an authorized user's access to a computer network is interrupted with

malicious intent. Denial of service exposes public-internet-accessible system components to the cyberattacks of operation halt, system malfunction or data corruption. A cyber threat of privilege escalation is also possible. Privilege escalation exposes centralized system components (such as Multi-Sig authentication or cryptocurrency exchange) to cyberattacks involving access control circumvention, system monitoring bypass or third-party security solution break-ins. The cyber threat of data disclosure is also in system components designed to process or store sensitive data such as cold/hot wallet and online/offline storage. In general, data disclosure includes security risks like data loss or data theft. A cyber threat of broken non-repudiation occurs in distributed application (dApps) such as smart contracts. In general, this threat includes security risks such as bypassing security logic, re-entry or race condition within source code or consensus protocol manipulation. Table 3.2 below lists the results of threat modeling by mapping the 6 identified threats (in rows) and their 17 associated security risks (in columns). Please note as a naming convention for later chapters: each security risk is numbered as SR-N, which means Security Risk Number N.

	(SR-1) Identity Theft	(SR-2) Component Disabled	(SR-3) Component Tampering	(SR-4) Data Corruption	(SR-5) Data Manipulation	(SR-6) Data Loss	(SR-7) Secure Channel Broken	(SR-8) Unsecure Communication	(SR-9) User Access Control Broken	(SR-10) Security Sovereignty / Logic Bypass	(SR-11) Un-secure 3rd-Party Solution	(SR-12) Security Monitor Circumvention	(SR-13) Code Reversing	(SR-14) Untested Code Running	(SR-15) Re-entry / Race Condition	(SR-16) Ledger malleability	(SR-17) Consensus Protocol Manipulation
Data Spoofing	✓			✓	✓	✓	✓							✓			
Data Tampering	✓		✓				✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Denial of Service		✓		✓									✓				
Elevation of Privilege					✓		✓		✓		✓	✓	✓				
Data Disclosure						✓	✓				✓	✓	✓	✓			
Non-Repudiation Broken	✓				✓				✓	✓					✓	✓	✓

Table 3. 2 – Mapping between 6 system security threats (rows) through threat modeling based on Figure 3.1 and 17 potential security risks (columns) in Blockchain System based on the 6 discovered system security threats based on Figure 3.3.

3.4 Four security domains of Blockchain system

From the threat modeling exercise in Section 3.3, the following 4 security domains were categorized as a collection of Blockchain system components, as illustrated in Figure 3.4 below. Please note that the described domains are assigned a naming convention (D-N) for later chapters, which means Domain Number N.

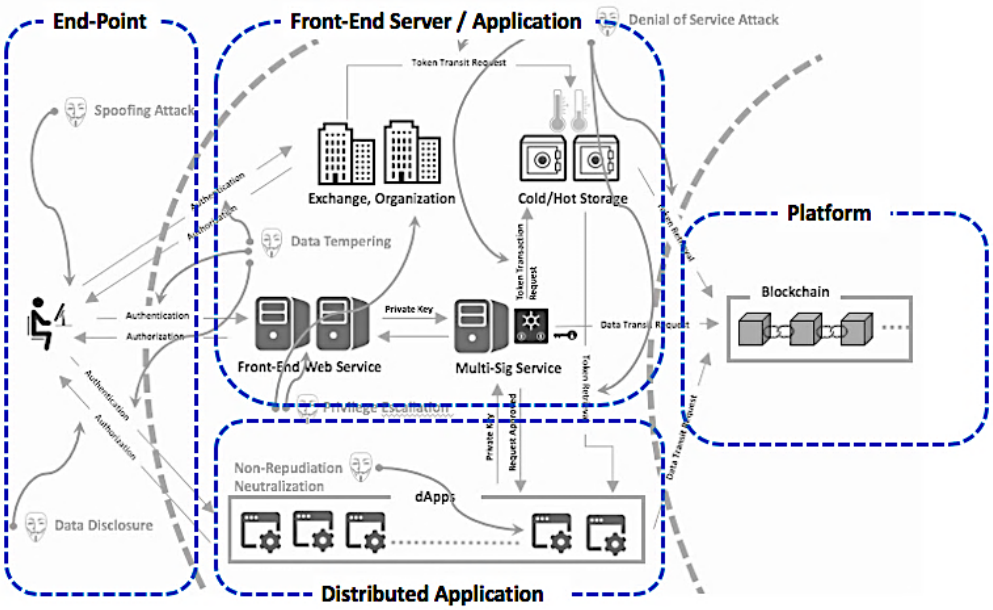


Figure 3. 4 – Four Blockchain system security domains are categorized throughout threat modeling exercises in section 3.3 *[41]*.

A platform domain (D-1) mainly includes Blockchain elements such as nodes (users) and shared data (public ledgers). Since a consensus of all nodes reviews data validation and decides on block addition, nodes (users) are considered the most important components in a Blockchain system. Ledgers are the data in the system stored at each node. In this domain (D-1), security review is mainly focused on redundancy, synchronization and communication for ledger (data) processing. A front-end domain (D-2) includes a front-end facing server and an application such as a web server for a digital wallet or third-party security solution, cryptocurrency exchange servers and online-based cold/hot storage. This is the same or very similar to the prevalent centralized IT system environment. Hence, security assessment methodologies should be similar to existing security assurance reviews, such as the OWASP Top 10. A distributed application

(dApps) domain, (D-3) includes mostly proprietary applications that run based on Blockchain. Unlike conventional and existing computer applications, the dApps are not isolated within web servers or personal workstations, but shared across the entire Blockchain system environment. Hence, security evaluation in this domain should be considered from the aspects of static (source code based) and also dynamic (running and execution cases). The end-points domain (D-4) includes terminals, computers or even mobile devices through which users communicate with a Blockchain system for usage and services. Data is entered as an input, sent as a request and produced as an output in this domain, considered the most vulnerable area in a data flow chain. This domain will be the optimum target area for a potential attacker, so it requires effective protection in the end-user environment from malware attacks against personal computing devices, Cross-Site Scripting attacks or Cross-Site Request Forgery attacks against client web browsers or computer virus infections.

CHAPTER 4 - Cyberattacks against Blockchain Systems

"Nothing matters but the facts. Without them, the science of criminal investigation is nothing more than a guessing game."

- Blake Edwards, American Director

4.1 Major cybersecurity incidents in the Blockchain system

To have better understanding of Blockchain systems security, actual hackings incidents are studied and researched in this section. Table 4.1 shows a chronological list of publicly notable cyberattacks targeting Blockchain systems from 2011 onward.

The first and second columns of the table show the name of each victim organization and the date each cyberattack occurred. If an organization experienced multiple cyberattacks, the number of occurrences is appended at the end of the name in parentheses, such as (*1*st) or (*2nd*). Each cybersecurity incident is categorized as one of the four Blockchain system security domains, established through modeling exercises in Chapter 3. Columns 3 to 6 in the table show which of the four domains experienced the cyberattack. Column 7 provides a brief description of the cyberattack, such as the exploitation method, the loss amount, consequences and any backstory related to the security incident, if necessary.

Most of the organizations listed are related to cryptocurrency or smart contracts. These are the most common applications using Blockchain technology over the last decade since the advent of cryptocurrency [42]

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
Allinvain	**2011. Jun**				**E**	Allinvain, a screenname of bitcoin.org forum, posted its wallet.dat file stolen by malware and lost $600,000 (250,000 BTC) [43]. This incident was not a direct cyberattack against a blockchain system or a company. Nevertheless, in terms of the Blockchain system security, it is considered a very important event, since it was the first publicly known hacking incident related to a Blockchain based system [44].
MT Gox (1st)	**2011. Jun**				**E**	Mt. Gox, the largest Bitcoin exchange at the time, was exploited as a system auditor's computer was compromised in a cyberattack [45]. The attacker was able to access to the exchange with the information from the auditor's computer and artificially altered bitcoin prices to one cent. Then, the attacker purchased about 2,000 Bitcoins from customer accounts and sold them immediately for cash. The loss was estimated at $30,000. [46].
Bitomat.pl	**2011. Jul**	**P**				The Poland based bitcoin exchange announced it lost about $222,000 (17,000 BTC) by deletion of Bitcoin Wallet. The operator set periodical server reboot and the process somehow destroy the Virtual Machines on Amazon Web Service. The company suspected it was a third party's fault from the beginning. However, it was subsequently discovered that a "breach" was occurred during a major upgrade. Then, the server was forced to reboot after the deletion of the Bitcoin Wallet instances. Because data of Bitcoin Wallet were not backed up at the time, the exchange lost all in the wallet [47].
MyBitcoin	**2011. Jul**	**P**				The crypto-currency wallet service provider had security flaws in its Blockchain implementation that resulted in improper confirmation of transactions. Attacker was able to forge Bitcoin deposits via the Shopping Cart Interface (SCI) and withdrew confirmed/older Bitcoins. This incidence is known as the first case of hot wallet exploitation. $833K worth of crypto-currency (154,406 BTC) vanished in this incident [48]. MyBitcoin was closed after the heist [49].
Bitcoin7	**2011. Oct**		**A**			The third-largest BTC/USD exchange reported loss of $25K (5,000 BTC) from cyber-attacks originated in Russia and Eastern Europe [50]. Attackers were able to hack into the infrastructure and steal wallets and personal information in the database [51]. Subsequently, the Bitcoin7 was closed and the domain was later sold for $10,000 USD in 2013. The exchange has been offline, since this incident [52].
Slush Pool (1st)	**2012. Mar**		**A**			Linode was cloud web host service provider for several crypto-currency companies at the time. Hacker(s) attacked the Linode server and was able to exploit Bitcoin wallets of several crypto-currency companies' serviced by Lonide [53]. According to company's announcement, a super admin password for its server management panel was leaked. This allowed a malicious attacker to target multiple Bitcoin-related servers [54]. Slush pool, the largest Bitcoin mining pool at the time, became one of the victims of the heist. Its backup image with pool data was saved on a hosted server at Linode and hacker(s) was able to obtain access information to Bitcoins (3094 BTC) stored in the hot wallet. The loss from this attack was estimated at $14,760 [55].
Bitcoinica (1st)	**2012. Mar**		**A**			At the same time of Linode cloud web server breach, $226,320 (43000 BTC) was stolen from Bitcoinica, a crypto-currency trading platform8.

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
Bitcoinica (2nd)	**2012. May**		**A**			About 10 weeks after its first hack, Bitcoinica was attacked again. At this time, its email address, associated with its Rackspace server, was compromised. This resulted in a loss of $92,500 (18500 BTC) from hot storage which allowed direct access from users [56]. The attacker was able to use the breached administrative email accounts to receive password reset links of user accounts [57]. It was revealed that Bitconica did not move their large amounts of liquid crypto-currency to cold storage from hot storage even after the first heist [58].
Bitcoinica (3rd)	**2012. Jul**	**P**				A third exploitation occurred at Bitcoinica, resulting in a loss from the MtGox account that had funds of $350,000 from the remaining users. Couple of days prior to the attack, Bitcoinica server's source code was publicly released to the internet for an unknown reason. And the API key in the source code was used as the LastPass account password. The LastPass account was used to access the MtGox account when Bitcoinica was running in business [59].
BTC-E	**2012. Jul**	**P**				BTC-E was a crypto-currency exchange based in Russia. As a provider of anonymous virtual currency transfer services, the company's system was compromised, and its API secret key was broken. The number of characters in the secret key was only 16, which is considered inadequate [60]. The attacker was able to initiate massive forged deposits in U.S. Dollar with the API key and purchased huge amount of Bitcoin. Subsequently, the attacker sold the Bitcoin [61]. The loss was 4,500 BTC which was equivalent to approximately $35,000. As a result of the incident, extremely large buy orders affected the Bitcoin market with temporary spikes [62].
Bitfloor	**2012. Sep**		**A**			Bitfloor, the fourth largest Bitcoin exchange in the world at the time, was hacked. The attacker compromised several servers in cloud infrastructure and was able to obtain un-encrypted backup of the wallet keys. The wallet keys were managed securely with encryption in production areas. The loss was estimated at about $250K at the time of the incident [63].
Bitinstant	**2013. Mar**		**A**			A Bitcoin brokerage, Bitinstant was hacked by DNS hijacking. The attacker was able to gain access to and control DNS registrar via social engineering [64]. With control of the DNS, the attacker was also able to obtain control over Bitinstant's email. Then, the attacker performed password reset of Bitinstant's accounts in the Bitcoin exchange, VirWox, and emptied the account. The company lost $12,000 worth of Bitcoins [65].
Instawallet	**2013. Apr**		**A**			The Instawallet, an online Bitcoin wallet provider, has been suspended indefinitely after hackers compromised its infrastructure. According to subsequent investigations, a hacker was able to access database and transfer Bitcoins. The loss was not disclosed and remain unknown at this time [66]. Prior to the hacking, Bitcoin Magazine recommended the Instawallet as one of the easiest services to use and for its "URL as password" mechanism that offers enhanced protection [67].
Ozcoin	**2013. Apr**	**P**				Hacker managed to infiltrate Ozcoin's payout script of mining pool. All money in the pool was paid out to the hacker's address by using online Bitcoin wallet, Strongcoin. Fortunately, Strongcoin was able to seize most of the stolen funds and promptly returned them to Ozcoin. The lost was estimated at about $105,000 [68].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
Slush Pool (2nd)	**2013. Apr**		**A**			Slush Pool reported an unknown intruder reset administrator password through email in OVH, a web hosting solution provider in U.K. The intruder was able to gain access to a hot wallet and steal stored Bitcoins. Slush Pool blamed OVH for this issue, but did not reveal loss amounts from the cyberattack [69].
Bitcoin Central	**2013. Apr**		**A**			Bitcoin Central, European Bitcoin Exchange, reported a few hundred bitcoins stolen from a hot wallet after an intruder managed to reset the password through an email for its hosting provider's web interface in OVH. The attacker then requested a reboot of the exchange's machine, in a rescue mode, locking the exchange out of its own site [70]. The OVH had been compromised for a couple of days prior to this hack against a hot wallet in the exact same way.
Vircurex	**2013. May**		**A**			The alternative cryptocurrency exchange service Vircurex, was hacked and lost about $163,000. The attacker was able to acquire login credentials to access the VPS (Virtual Private Server) control account of a web hosting service provider and made a request to reset root password of all servers. As a result, both hot and warm wallet were emptied by the attacker [71]. In March 2014, the exchange became insolvent after losing large amounts of its reserve funds and was closed indefinitely [72].
Bitfunder	**2013. Jul**		**A**			BitFunder, a cryptocurrency platform with flaws in the codes, was able to credit one's accounts from multiple Bitcoin Exchanges, such as WeExchange etc. The loss was estimated at about $775,000 (6,000 BTC) [73]. Bitfunder was abruptly shut down in November 2013. In February 2018, BitFunder's founder, Jon Montroll, was charged by the SEC in the U.S. District Court for the Southern District of New York with operating an unregistered securities exchange that defrauded users by allegedly misappropriating bitcoins and failing to disclose the cyberattack [74].
Inputs.io	**2013. Oct**				**E**	Inputs.io, a well-known high-security bitcoin web wallet at time, was hacked and lost about $1M worth of bitcoins (4,100 BTC) from its hot storage in two different attacks [75]. The attacker was able to access an old email account in an unknown way and take control of the account by resetting the password from a cloud-hosting provider, Linode. Then, the attacker compromised the company's two-factor authentication system by exploiting a server-side vulnerability and accessed the database containing wallet data and user information [76]. Inputs.io became no longer operational as of November 7th, 2013 [77].
Bitcash.cz	**2013. Nov**				**E**	The Czech Republic-based bitcoin exchange has been hacked and lost about $100,000 worth of cryptocurrency from customers' wallets [78]. One of Bitcash.cz's email accounts was compromised, and the attacker sent phishing emails to users as a staff member. Approximately, 4,000 recipients followed the phishing email instructions and sent their bitcoins to the attacker's wallet address [79].
Bidextreme.pl	**2013. Nov**		**A**			Poland's digital currency exchange, Bidextreme.pl, was hacked. According to the company's announcement, its customers' wallets were emptied and $33,000 worth of crypto-currencies (BTC and LTC) were stolen [80] [81]. Following the attack, the site was shut down by its owner and put up for sale at a minimum price of 170 BTC [82].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
BIPS	**2013. Nov**		**A**			Danish bitcoin payment process provider BIPS was hacked and lost $1M (1,295 BTC). Prior to the hacking, the attackers launched Distributed Denial of Service (DDoS) attack on BIPS, originated from Russia and neighboring countries. While the technical detail remains unknown, the hackers were able to steal from online accessible wallets [83].
Picostocks	**2013. Nov**				**E**	PicoStocks, a cryptocurrency exchange, was compromised, and about $6,000,000 was stolen (about 6,000 BTC) [84]. The company reported that the attacker used an old access key, which had not been terminated and remained dormant for a long period of time to transfer from both company's hot and cold wallets to own address [85].
Silk Road 2	**2014. Feb**	**P**				The dark market web-site, Silk Road 2, lost all of its crypto- currency stored in hot wallet which was worth of $2,700,000 [86]. According to announcement, the vendor exploited newly discovered "transaction malleability" vulnerability in Bitcoin Blockchain protocol at the time. The company claimed that "despite its hardening and penetration testing procedures, the attack vector was outside of penetration testing scope due to being rooted in the Bitcoin protocol itself," [87].
MT Gox (2^{nd})	**2014. Feb**	**P**				A Japan-based bitcoin exchanged, MT Gox announced about $450,000,000 worth of cryptocurrency theft by hacking. The company filed bankruptcy immediately after the heist [88]. According to investigations, the hack was found to be continued for years with abusing "transaction malleability" issue in Bitcoin protocol [89].
FlexCoin	**2014. Mar**		**A**			Flexcoin was attacked and lost all its coins in the hot wallet. Due to the heist, the company did not have enough resources to cover a loss of 896 BTC, approximately $700,000 at the time [90]. The electronic wallet provider incentivized users for keeping their Bitcoin balances on hot wallets and charged 0.02 BTC or 1% of transaction amounts for funds transferred out of cold storage [91]. The un-known attacker was able to log into the flexcoin front end under a newly created account and then exploited a flaw in the code which allowed transfers between Flexcoin users. By sending thousands of simultaneous requests, the attacker was able to "move" coins from one user account to another until the sender account was overdrawn, and before the balances were updated [92].
CoinEX.pw	**2014. Mar**	**P**				CoinEX was a Russian crypto-currency exchange handling a small volume of Bitcoins and variety of alt-coins. Wallet server was compromised, and all of the funds were withdrawn [93]. According to an un-confirmed source, the attacker might have founded security flaws in an API document that was deleted from the Gist page right after the incident [94]. The loss was not clearly identified and the exchange has been out of business since Dec 2015.
Poloniex	**2014. Mar**	**P**				A crypto-currency exchange, 'Poloniex', reported that it lost 12.3 percent of its total crypto-currency supply in an attack, [95] resulting in a loss of approximately $50,000 in Bitcoin (76.69 BTC) [96]. The hacker discovered a security issue in the company's withdrawal process. When a user placed several withdrawals orders in a very short period time, the 'Poloniex' server processed them without verifying the remaining balances. This resulted in a negative balance or an overdraft, but valid insertions into the database, which then get picked up by the withdrawal daemon [97].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
Dogevault	**2014. May**		**A**			Dogecoin storage system, Dogevault, closed after a loss of $55K due to a cyberattack. According to the company website, hackers infiltrated the online wallet service. Further investigation later found that the attacker gained access to the node where Dogevault's virtual machines contained encrypted credentials of all users [98]. After the heist, the Dogevault service was shut down [99].
Cryptsy	**2014. Jul**				**E**	This crypto-currency exchange announced that it had been a target of cyberattack and lost $7,500,000 worth of Bitcoin (13,000 BTC) and $2.08M worth of Lite Coin (300,000 LTC). The exchange has been closed since then [100]. It was explained two years later that an alleged hacker claiming to be the developer of Lucky7Coin had inserted a type of Trojan horse malware (an IRC backdoor) into the code of the wallet thus allowing him to collect information from the inside of Cryptsy. This enabled the cyber attacker to transfer Bitcoin and litecoin, as well as a couple of other smaller crypto-currencies, from Cryptsy's "hot/cold" wallet [101].
Mintpal	**2014. Jul**		**A**			Due to a cyberattack, MintPal, a crypto-currency exchange, lost about $2,000,000, which was equivalent to about 8,000,000 Vericoin crypto-currency. According to a subsequent investigation, an attacker was able to circumvent internal controls and obtain authorization to withdraw request on Vericon's hot wallet by SQL injection [102].
BTER (1^{st})	**2014. Aug**		**A**			A crypto-currency trading platform BTER lost $1.65M worth of crypto-currency (51M NXT) [103]. According to subsequent investigations, studies and researches on the internet, the attacker was able to obtain information related to developers' accounts and hack into a main exchange server from a front-end. Even if BTER set up 2-factor authentication for user access, the main exchange server's access control was not set up at the same level. To worsen the situation even further, most of the NXT crypto-currency was stored in a hot wallet. The attacker was able to access BTER database and transfer the 51M NXT to its own address. [104]
Cryptothrift	**2014. Oct**		**A**			Cryptothrift, one of the most popular crypto-currency sites at the time, was hacked, losing $5,000. According to an investigation, the attacker conducted SQL injection and manipulated crypto-currency bitcoin transfers from its hot wallets [105].
Justcoin	**2014. Oct**	**P**				A Norway-based crypto-currency exchange, Justcoin, was exploited due to the vulnerability of "tfPartialPayment" function in the Ripple and Stellar. This function was designed to handle transactions by granting access to the platform's hot wallet-stored funds [106]. Ripple puts blame on Justcoin's implementation and confirmation of gateway. However, according to many incident reports, Ripple was already aware of this issue few months ago. Ripple's instructions for the gateways setup did not explain the issue properly. Later, several other exchanges were exploited in the same way. The total loss of the exploitation was about $300,000, mostly related to crypto-currencies stored at hot storage [107].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
BTC-E (2nd)	**2014. Oct**				**E**	A crypto-currency trading platform, BTC-E, announced its 2nd heist to the public. An attacker was able to compromise 568,355 accounts and stole approximately $26,000,000 (70,000 BTC) [108]. According to an unconfirmed source, a hacker was able to post a malware link on ajax chat program called Troll Box and spread it out to BTC-E users to steal credentials. After discovery of this attack, the company suspended all of the compromised accounts and set rules to ban a protocol for potentially affected users. However, the remediation was not effective to stop the malware from spreading out further because it disconnected all communication channels among users that could be used to warn them of accessing the infected domains [109].
Bitpay	**2014. Dec**				**E**	Bitpay's CFO email account was hacked by a phishing attack. Then, the attacker sent spoofed emails from the CFO's email account to the company's CEO requesting 5,000 BTC on three separate occasions. In response, CEO of the company sent out the crypto-currencies without any suspicion. As a result, this Atlanta based crypto-currency payment company lost $1,800,000 [110].
796	**2015. Jan**				**E**	This China-based crypto-currency exchange lost approximately $313,000 (1,000 BTC) [111]. According to Nelson Yu, CEO of the exchange, the attacker found a flaw on a trading platform and was able to replace one user's address with another address [112].
Bitstamp	**2015. Jan**				**E**	The U.K. based crypto currency exchange was hacked and lost approximately $5,200,000 (19,000 BTC) [113]. According to an unconfirmed incident report of the company, six employees were targeted in a weeks-long phishing attempt. The attacker sent emails with MS Word documents that contained obfuscated malicious VBA script. When the document was opened, the script was executed, retrieving a malware from a remote location, thereby successfully compromising the machine. Ultimately, the attackers were able to access two servers containing the wallet.dat file of Bitstamp's hot wallet and the passphrase for access [114].
LocalBitcoins	**2015. Jan**				**E**	One of the first and the most popular crypto-currency platforms, Localbitcoins, suffered from a distribution of malware and lost about $5,000 (17 BTC) from customers' wallets [115]. According to the company, the attacker spread out a key logger through a live chat program and had users execute programs with a social engineering technique. Although the live chat program provided by LocalBitcoins had embedded virus scanning capability, it could not detect the malicious software [116].
BTER (2nd)	**2015. Feb**		**A**			A China-based crypto-currency exchange, BTER, lost $1,750,000 (7000 BTC). It was reported that the company's cloud infrastructure account was compromised and that the company lost most of its funds from cold storage. The exchange was closed due to the hack [117].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
KipCoin	**2015. Feb**		**A**			A China-based crypto-currency exchange, KipCoin, was compromised by a cyberattack and lost $690,000 (3,000 BTC) [118]. According to the company's announcement, the exchange had previously experienced a breach of its cloud server accounts from a 2014 hacking. The attacker was able to obtain and reset a root password in a Linode cloud server. A wallet.dat file was stolen, and the control of the entire KipCoin server was under the attacker's control for months. Although the company became aware of the breach and the loss of control at the time of the cyberattack, it remains unclear why the exchange did not secure its funds during this time. [119].
Cavirtex	**2015. Feb**		**A**			This Canadian-based crypto-currency exchange was exploited in its database, resulting in a disclosed user data. Cavirtexn announced to the public that the compromised database contained two-factor authentication secrets and hashed password and that none of the identification documents was impacted. Cavirtexn decided to cease all active operations in its crypto-currency business due to the heist [120]. The loss from this attack was unknown but all affected users were fully paid back [121].
Cryptoine	**2015. Mar**	**P**				The attacker exploited a race condition from the trading platform in Cryptoine, a crypto-currency exchange. The attacker was able to manipulate orders and transfer funds to one's own account. The amount of loss was not announced but it was revealed that 60% of the funds stored in hot wallet were stolen [122].
Allcrypt	**2015. Mar**				**E**	The attacker was able to obtain access to one of technical assistant's email accounts. Then, the attacker proceeded to request a password reset for the Marketing Director's WordPress account, which was running as the exchange main site. Upon possession of Marketing Director's password, the attacker uploaded PHP-based database management to the WordPress site and manipulated crypto-currency balances in the system. At the end, the attacker transferred crypto-currencies to his or her own Bitcoin wallet. [123] Due to the cyberattack, Allcrypt lost about $11,000 (42 BTC).
Coinapult	**2015. Mar**		**A**			One of the longest-operating crypto-currency startups suffered a hot wallet attack that resulted in the loss of $42,900 (150 BTC) [124]. According to Coinapult, there are very few people granted with access to the hot wallet through SSH keys. Also, only 2 people had physical access to the affected servers kept in a tier 3 data center that had layers of physical security. The entry point of cyberattack remains unknown at this time. [125]
Bitfinex (1st)	**2015. May**		**A**			Bitfinex, a Hong Kong-based crypto-currency exchange, lost about $356K (1,500 BTC) due to a cyberattack [126]. While the technical detail of this attack was not released, it is widely known that the hot wallet was compromised. According to a public announcement, the loss amounted to only 0.5% of its entire deposits and the remaining 99.5% was stored in a multi-sig wallet. The firm also emphasized that it was in the process of developing a more secure hot wallet [127].

Blockchain System Organization (*Number if attacked more than once*)	**Date**	**(D1) Platform Breach**	**(D2) Access Point Attack**	**(D3) DApps Exploit**	**(D4) Endpoint Hacking**	**Incident Detail**
Cloudminr.io	**2015. Jul**		**A**			A Norway-based crypto-currency cloud mining platform, Cloudminr.io, was breached. Attackers were able to break into the system and compromise the company's back-end database [128]. There was no loss or theft announced from the attack. However, the hacker offered to sell the information stolen from 79.267 accounts including usernames, passwords, and email addresses for a single Bitcoin. The company was out of service shortly after the incident [129].
BitQuick	**2016. Mar**		**A**			The U.S.-based crypto-currency exchange, BitQuick, was hacked, and its database was breached. According to a statement from the exchange, the attacker was able to obtain access to a server by a SQL injection attack and obtain user's personal information such as phone numbers, names and email addresses. As publicly known, there was no theft involved in this cyberattack [130].
Cointrader	**2016. Mar**		**A**			This Canada-based crypto-currency exchange announced loss of $33,600 and a company closing due to debilitating cyberattack [131]. It remains unknown how the exchange was exploited.
Coinwallet.co	**2016. Apr**		**A**			Coinwallet.co, an online wallet service, announced a data breach. The attacker was able to conduct a SQL injection attack and gained access to the database [132]. Coinwallet.co claimed that there was no loss due to the hacking. However, it announced a service closure without providing any schedule or plan to-reopen the business [133].
ShapeShift.io	**2016. Apr**		**A**			This crypto-currency exchange was suffered by a series of cyberattacks within a month, losing about $230,000 and ultimately closing the business [134]. According to a report, the attacker was able to gain access to a hot wallet and drained stored crypto currencies (469 BTC, 5,800 ETH and 1,900 LTC) [135]. The exchange believed that the former employee released critical security information to the attacker. However, there was no strong evidence found to support the claim since all traces were cleaned after the cyberattack and could not be restored [136].
Ethereum (1st)	**2016. May**			**D**		TheDAO, the most anticipated dApps at the time was hacked and lost about $70M worth of Ethers. Bugs in the code were shared in a forum prior to the attack. While a developer was fixing the dApps, a hacker found a way to steal most of ICO funds and transfer them to the hacker's own address [137].
Coinkite	**2016. May**		**A**			This Canadian Bitcoin startup developed a hardware wallet for safe offline storage. The company reported its database was exploited [138]. Although all of its user passwords were leaked, Coinkite claimed that there was no financial loss because all of the stolen passwords were securely encrypted [139].
Gatecoin	**2016. May**	**P**				Gatecoin, a Hong Kong-regulated financial institution for Blockchain assets, publicly announced that a hacker exploited its multi-sig system who was able to obtain direct access to the cold storage [140]. The estimated loss was approximately $2 million, or 15% of total crypto currency in the exchange [141]. This breach was very unique in the theft occurred from Cold Storage [142].

Blockchain System Organization (*Number if attacked more than once*)	**Date**	**(D1) Platform Breach**	**(D2) Access Point Attack**	**(D3) DApps Exploit**	**(D4) Endpoint Hacking**	**Incident Detail**
Steemit	**2016. Jul**		**A**			This Blockchain-based social media company, where users get rewarded for creating or curating good content, was attacked and more than 250 user accounts were compromised. As a result of the attack, $85K worth of Steemit coin were stolen from its hot wallet storage [143].
Bitfinex (2nd)	**2016. Aug**	**P**				In 2015, Bitfinex, one of the largest crypto-currency exchanges, announced its plan to create a new multi-signature wallet with BitGo where keys were divided among a number of owners in order to better manage risk. When a user sends or broadcasts a transaction to the Bitcoin Blockchain, it requires a first level of approval from Bitfinex and a second level of approval from Bitgo as a co-signer [144]. According to a public announcement issued by Bitfinex, a hacker was able to exploit the Bitfinex system and obtain a private key of Bitgo API private key. Then, the hacker broke the multi-sig by instruct Bitgo's authentication functions to automatically sign BitGo into all transactions with only Bitfinex authentication. The hacker was able to execute one transaction that stole 119,756 Bitcoins in the amount of $72,000 [145].
Bitcurex	**2016. Oct**		**A**			Bitcurex, established in Poland in 2012, was one of the largest Bitcoin exchanges in Europe. In July 2016, Bitcurex upgraded to a third party system service to assess customer risk and personal data protection as required by the Poland Compliance Association. On October 13 2016, Bitcurex announced to the public that the exchange encountered problems with the update and that the exchange decided to temporarily suspend all transactions in order to resolve the problems. About two weeks later (October 20, 2016), the exchange abruptly posted a new message stating that its incident response team is working on a network upgrade and security updates to back the system up so that users can withdraw their funds. However, about one week later (October 27, 2016), Bitcurex posted another message finally revealing that a hacking attack occurred on October 13, 2016 and lost assets worth of estimated $1,500,000 [146]. Based on an investigation conducted by the Polish Authority, Bitcurex stored funds within a hot wallet in a platform level, and the hacker transferred all of the funds in 3 seconds after the break in [147]. Consequently, the exchange shut down, and users most likely lost all of their funds. Customer data of the exchange was also compromised and stolen from system [148].
Zcoin	**2017. Feb**	**P**				Zcoin is an open-source crypto-currency which implements Zero-Knowledge proofs on top of Bitcoin to guarantee complete financial privacy and anonymity [149]. Zcoin discovered that a malicious attacker was able to "double spend" to receive Zcoin multiple times within one transaction initiation [150]. Zcoin explained that during non-security focus transaction analysis, developer found a single-symbol error in a piece of code that allowed the attacker to create Zcoin spend transactions without a corresponding mint" [151]. A further investigation found that the attacker(s) exploited and manipulated the security vulnerability over a period of several weeks, who was able to steal about $600,000 (370,000 Zcoin). Zcoin implemented neither real time monitoring nor fund transaction tracing at the system level [152].
Yapizon (1st)	**2017. Apr**		**A**			The South Korea-based crypto-currency exchange suffered a cyberattack and lost $5,000,000 (3816.2028 BTC) which represented 37% of all user funds. According to the exchange, the attacker broke into the system in an unknown way and compromised four of the exchange's hot wallets [153]. The exchange later changed its name to Youbit.

Blockchain System Organization (*Number if attacked more than once*)	**Date**	**(D1) Platform Breach**	**(D2) Access Point Attack**	**(D3) DApps Exploit**	**(D4) Endpoint Hacking**	**Incident Detail**
Jaxx	**2017. Jun**				**E**	A hacker targeted users who installed JAXX Wallet on rooted Android phone, which turned off most of default security guards within the mobile OS system. After gaining access of the victims' phones with this method using the known vulnerability of rooted Android phone, the hacker retrieved a 12-word back up phrase of JAXX Wallets, pulled out private keys, and then transferred away all of users' cryptocurrency. Approximately $400K worth of Ethers and Crypto-currencies were transferred to the hacker's account over the next two months [154]. According to security analysis from VXLabs, Jaxx Wallet software encrypts the mnemonic using a hard-coded encryption key, instead of making use of a strong user-supplied password [155]. In response to the hack and the security analysis, Nilang Vyas, CTO of JAXX, explained that the wallet was designed as a hot wallet which was not meant to be used for long-term crypto-currency storage [156]. He clearly stated that JAXX does not have any plan to change or upgrade of its software to address this security issue and asked users not to use JAXX if they are not comfortable with its security model [157].
QuadrigaCX	**2017. Jun**	**P**				The Canada-based crypto-currency exchange, which is the largest in Canada, announced a $15,000,000 (67,316 ETH) loss due to a programming error [158]. When the Ethereum Blockchain was upgraded from Geth 1.5.3 to 1.5.9, the exchange did not update its software appropriately. The exchange should have been able to handle the smart contract execution between Ethereum and Ethereum class differently, which had Blockchain split last year due to theDAO hack, but did not do so [159].
Bithumb (1st)	**2017. Jul**				**E**	Bithumb, one of the largest crypto currency exchange based in Republic of Korea (South Korea), was hacked, and its customer data were stolen [160]. The exploitation occurred at one of employee desktop computers in the main office. About 31,506 user IDs and personal information stored in excel files without any kind of encryption were stolen. The attacker launched brute force attacks with the stolen user information on 2,000,000 occasions for the next 3 months. 266 accounts were successfully exploited, which had the same values for user IDs and passwords [161]. The incident was announced to the public 3 months after the theft. The exchange confirmed that there was no impact other than a $870,000 loss. However, many customers subsequently complained that they became subject to "voice phishing", "identity theft," and other types of cyberattacks because of the user information leakage [162].
Coindash	**2017. Jul**		**A**			Coindash was able to raise $7,500,000 through an ICO (Initial Coin Offering) but had to shut down abruptly. This was due to a discovery that the company's Ethereum address was altered to a fake one. The exploitation was utilized PHP web-shell against its public website. As a result, the Ethers were transferred from investors to an unknown party [163]. The incident showcases the growing pains experienced by ICOs, which despite raising massive amounts of funds, still had to navigate the complexities of an early-stage technology. The loss was estimated at $7M [164].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
Ethereum (2nd)	**2017. Jul**			**D**		A Smart contract coding company Parity reported $30,000,000 worth of Ethers (about 150,000 ethers) stolen by hacker [165]. The share wallet library, which contain methods to initialize the wallet, was not securely controlled within the Multi-Sig Wallet DAPP. Attackers were able to reinitialize existing contracts and overwrite the owners address with a single transaction. By invoking three transactions with utilizing the security bug, attackers could trivially extract the remainder of the balance from three of the largest wallets [166]. In response to the incident, a white-hat recovery team utilized the same code used by the hacker and drained all the remaining vulnerable wallets into one safe location in order to avoid further hacks [167]. This was recorded as the second largest hack on the Ethereum Blockchain system and the first case of preventing further hacking with the same exploitation method in cyber security history. Details on this hack and attack will be further discussed below.
Enigma	**2017. Aug**				**E**	Enigma was the most notable Blockchain project launched by MIT. It was incubated at Media Lab, but lost about $500,000 worth of Ethers. Enigma's public website was compromised, and hackers were able to gain possession of the Slack channel containing mailing lists and administrator accounts. Then the fraudsters sent out fake information to thousands of users about a token pre-sale in August,2017. Unsuspecting consumers donated Ethers to defrauding potential investors. Although the Enigma team regained control of the company's accounts, the Ether wallet used by the hackers was emptied, and the funds were never recovered [168]. This hacking incident is quite similar to Coindash, which the public access point was breached as described previously. Ironically, after the hack of Coindash's website, the co-founder and Chief Product officer of Enigma stated during an ICO interview with Business Insider that Enigma has a simple solution that can prevent similar situations from recurring in the future [169].
Ethereum (3rd)	**2017. Nov**			**D**		Another bug found in Parity Wallet remained even after the major heist in July, 2017, and a user accidentally triggered that bug in a software code. As a result, $275,000,000 worth of Ether was frozen. To restore the funds, developers pushed subsequent updates, which required all Ethereum users to upgrade their software [170].
Tether	**2017. Nov**		**A**			Tether allows users to send and receive digital tokens pegged to actual currencies like dollars, euro and yen. The company announced its treasury wallet was breached, which drained $31,000,000 worth of tokens to a Bitcoin address of hackers. According to the Tether teams, while the root cause was identified as a system breach, they were unable to find how the attackers broke into the access point of the system [171].
Nicehash	**2017. Dec**		**A**			Slovenian company Nicehash, a market place for trading computer hashing power to mine crypto-currency, lost $75,000,000 worth of crypto-currency [172]. The hacker was able to infiltrate an internal system through VPN with one of the company engineer's credentials. After the VPN login, the hacker transferred the funds to his or her own account [173]. It is still unknown how the hacker could obtain the credential and how long the hacker maintained the connectivity to the internal network. However, the active attack timeline was only a couple of hours [174]. Later, many Nicehash users have expressed a surprise to learn that the company's Chief Technology Officer recently served several years in prison for operating and reselling a massive botnet, and for creating and operating 'Darkode," one of the world's most bustling English-language cybercrime forums [175].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
Youbit (2nd)	**2017. Dec**				**E**	This South Korea-based crypto-currency exchange, which had been known as Yapizon, experienced another theft, losing 17% of its crypto-currency from a hot wallet [176]. The loss was estimated at about $15,000,000. Similar to the first exploitation that occurred in April 2017, a publicly accessible server was breached, and the attacker was able to access the hot wallet. The company declared bankruptcy shortly after the heist [177].
Blackwallet	**2018. Jan**		**A**			Blackwallet provides online wallet services to connect Endpoint users with crypto-currency Blockchain as a "Public Access Point". Its Domain Name Server was hijacked by an attacker, and all network traffic to the system was re-routed to malicious on-line wallet in Cloudfare. Once user did login the wallet, the wallet automatically sent customer balances of 20 Stellar Lumen (XLM) to an address under the hacker's control. The amount of total loss was $400,000 in XLM crypto-currency. As a result, the company was out of business after 5 months of its start [178]. Please note that in August 2017, "1&1", a host provider of Blackwallet had social engineering attack that led to a loss of control over classic Ether Wallet's domain [179].
CoinCheck	**2018. Jan**				**E**	$600,000,000 in NEM crypto-currency was stolen from the Japanese crypto-currency exchange, Coincheck [180]. A hot wallet accessible to the external internet was exploited, since its "Endpoint" security was not enforced to use a cold wallet and 2 factor authentication [181]. By March 18, the NEM Foundation ceased to track the stolen coins, which accelerated the movements of the currency. According to NHK, experts believe that tracking the stolen coins became impossible after two months of the incident [182].
BitGrail	**2018. Feb**	**P**				This Italy-based crypto-currency exchange, BitGrail, announced that an un-authorized transaction of 17,000,000 in Nano crypto-currency occurred [183]. According to the exchange's security investigation, the attacker exploited two vulnerabilities. The first issue involved a user account validation mechanism which was only placed on client-side browsers as a JavaScript code. The attacker was able to bypass it easily and withdrew more funds than actual account balances. The second issue involved a server side fund transfer permission bug. The attacker was able to manipulate the funds withdrawal requests to transfer account balances from customers to the hacker's own account. The exchange lost $195,000,000 due to these two significant security flaws [184].
Bee	**2018. Feb**		**A**			Bee Token partnered with San Francisco-based financial services platform, WeTrust, to create a decentralized home-sharing service provider that competed against AirBnB. $1,000,000 worth of Ethers were stolen during its public ICO in a phishing attack [185]. According to an investigation, the attackers were able to obtain the personal data and email addresses of Bee Token mailing list participants. Then, the attacker sent out a fraudulent emails stating that the ICO crowd sale was open to contributions [186].
CoinSecure	**2018. Apr**		**A**			The India-based crypto-currency exchange lost $3,300,000 worth of crypto-currency (438.318 BTC) [187]. The private key of the hot storage was compromised and was released online. Since all data log has been removed from the system, the root cause of the hacking was not identified. CSO of the exchange allegedly claimed that the theft was due to the cyberattack. However, CEO of the exchange blamed the CSO for the incident, since he was the only person who managed the private key [188].

Blockchain System Organization (*Number if attacked more than once*)	Date	(D1) Platform Breach	(D2) Access Point Attack	(D3) DApps Exploit	(D4) Endpoint Hacking	Incident Detail
MyEtherWallet	**2018. Apr**		**A**			The online crypto-currency wallet provider, MyEtherWallet, lost $152K (215 ETH) [189] in this cyberattack. According to the company's announcement, a few of DNS servers of the exchange were compromised, which redirected client requests to a phishing site [190].
Coinrail	**2018. Jun**		**A**			The South Korea-based crypto-currency exchange lost $42,000,000 (NPXS, ATX, NPER and DENT) in this cyberattack [191]. The attacker was able to obtain access to hot storage and transfer 30% of the exchange's total crypto-currencies in 20 minutes [192]. According to a Korean newspaper, Chosun Daily News, several banks had identified suspicious transactions at the exchange and stopped providing services to the exchange several months before the incident. The exchange was closed shortly after the heist [193].
Bithumb (2nd)	**2018. Jun**				**E**	The South Korean crypto-currency exchange, Bithumb has suspended all deposits and withdrawals after losing $30 million worth of crypto-currencies held at hot storage due to a cyberattack [194]. According to Yeonhap News, phishing emails had been previously sent to Bithumb users earlier that month. The malicious emails were designed to obtain account information of users who clicked on the URL links provided in the phishing emails [195].

Table 4. 1 – Major cyberattacks against Blockchain system between 2011 1st quarter and 2018 2nd quarter.

4.2 Increasing loss due to cyberattacks

According to the U.S. State of Cybercrime survey conducted by the U.S. Secret Service and CERT at Carnegie Mellon University, the number of security events has been declining in recent years although their impacts have become more serious. Based on their report, on average, each company in the U.S. suffered 148 cybersecurity exploitations in 2017, which is about an 8 percent decrease from the previous year. However, the loss and damage from cybersecurity crimes rose by 14 percent during the same period [196]. This suggests that cyberattacks are becoming more targeted, planned and sophisticated, since many organizations in the U.S. have become well prepared for cyberattacks after years of experiencing hackings and heists. However, based on data compiled from Table 4.1, the number of cyberattacks targeting Blockchain systems has remained the same or increased only a little over the years, as illustrated in Figure 4.1. This analysis indicates that the security protection of Blockchain systems is inadequate and insufficient compared to the IT industry as a whole, in terms of cyberattacks.

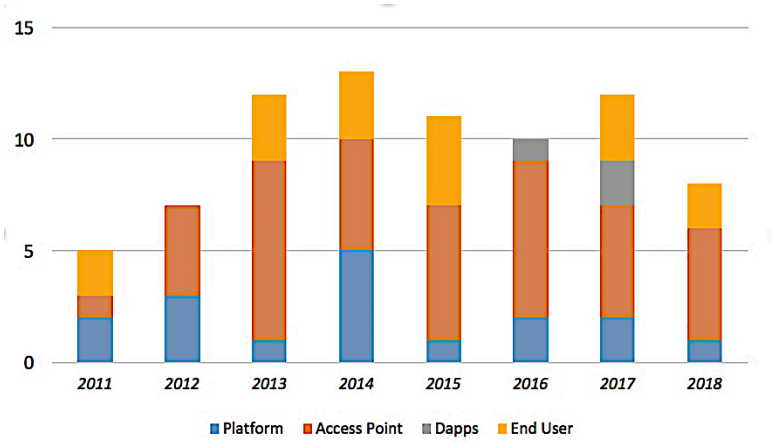


Figure 4. 1 – Number of public notable heist against Blockchain system in recent years.[2]

Table 4.2 below shows, annual financial losses due to cyberattacks on the Blockchain system. As you can see, the losses have increased tremendously. In particular, notice the amount of loss has tripled every year from 2015 to 2017. The total financial loss by the second quarter of 2018 is about 30 times (2,787%) more than the total financial loss in 2011.

[2] For 2018, the incidents until 2nd quarter were reflected.

	Platform	Access Point	dApps	End User	Total
2011	$1,055,000	$14,760	$0	$630,000	$1,699,760
2012	$385,000	$583,580	$0	$0	$968,580
2013	$105,000	$2,210,807	$0	$7,495,411	$9,811,218
2014	$12,630,000	$454,410,000	$0	$27,800,000	$494,840,000
2015	$0	$2,838,900	$0	$33,329,000	$36,167,900
2016	$74,000,000	$1,848,600	$70,000,000	$0	$145,848,600
2017	$15,600,000	$133,000,000	$305,000,000	$1,770,000	$455,370,000
2018	$796,400,000	$46,852,000	$0	$630,000,000	$1,473,252,000

Table 4. 2 – Public notable loss by cyberattack against Blockchain system.[3]

4.3 Cyberattacks in terms of security domain

Table 4.3 shows a total number of cyberattacks in terms of security domains since 2011. As shown, the access point (D-2) is the most commonly exploited domain. More than half the entire Blockchain system heists were due to inadequate security in front-end system components, such as web host servers, Internet-based wallets, and two-factor authentication services. Conversely, the domain of Distributed Applications (dApps) (D-3) has so far suffered only three cyberattacks.

	Platform	Access Point	dApps	End User
2011	2	1	0	2
2012	3	4	0	0
2013	1	8	0	3
2014	5	5	0	3
2015	1	6	0	4
2016	2	7	1	0
2017	2	5	2	3
2018	1	5	0	2
Total	**17**	**41**	**3**	**17**

[3] For 2018, the incidents until 2nd quarter were reflected.

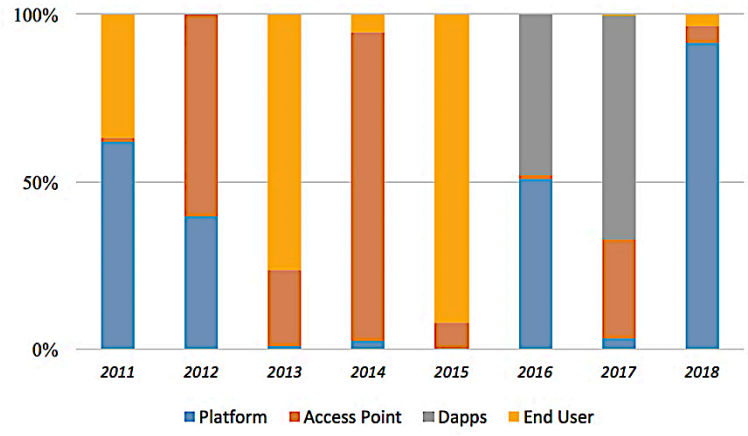
Table 4. 3 – Number of cyberattacks against Blockchain system in security domain.[4]

However, this does not mean that dApps is the most secure domain in the Blockchain system. To date, most dApps focus on only smart contracts that run on the Ethereum Blockchain system, which was launched in 2015. In other words, Ethereum Blockchain systems and smart contract applications were less exposed to cyberattacks than other Blockchain systems, such as cryptocurrency and exchange. Nevertheless, the total loss due to cyberattacks in the dApps domain is estimated at $375 million. This is not a small number compared to other domains. In addition, as shown in Table 4.4, the average loss in the dApps domain is four times more than the average of all other security domains in the Blockchain system.

	Platform	Access Point	dApps	End User	Total
Avg. Loss	$52,951,471	$15,652,650	$125,000,000	$41,236,730	$33,563,564

Table 4. 4 – Average financial loss per incident against Blockchain system in terms of security domain since 2011.

Figure 4.2, shows the annual loss per security domain as a percentage to view trend changes in cyberattacks over the years. For instance, in 2015, about 90 percent of the financial losses from cyberattacks targeting Blockchain systems occurred in the end-user domain. (D-4) This figure shows that most of the losses and damages caused by cyberattacks in the early days of the Blockchain system (between 2011 and 2015) are related to the domains of access points and end users which are still using existing centralized system components. On the other hand, in recent years (since 2016) the losses in the domains of dApps (D-3) and platforms (D-1) have increased significantly, which are the areas utilizing new distributed technologies such as Blockchain protocol and distributed applications.



[4] For 2018, the incidents until 2nd quarter were reflected.

Figure 4. 2 – Contribution to financial loss from each security domain in terms of percentage.[5]

In fact, this pattern is considered normal in the field of information security. When a new technology is introduced, it experiences relatively fewer number of cyberattacks in the beginning. As more vulnerability information is gathered and more exploitation techniques are evolved, the technology becomes more vulnerable to cyberattacks. In this sense, the IT security industry's longstanding belief that the Blockchain system prevents all types of cyberattacks and that all security incidents in the Blockchain system are caused by human error or by usage of traditional centralized system components are not accurate.

4.4 Cyberattacks for considerable periods of time

In the jargon of system security, a zero-day attack[6] (also known as 0-day attack) means an attack targets system vulnerability that has not been patched or migrated [197]. Day Zero is the day on which detailed information of the vulnerability becomes known to the public and the interested party (presumably the vendor of the targeted system) learns of the vulnerability. Once the vulnerability is brought out, the vendor will create patches or advise workarounds to mitigate it promptly, or within 30 days in most cases [198].

As previously shown in Table 4.1, a fairly large number of different Blockchain systems have been victimized by the same types of cyberattacks over a short period of time. To visualize the occurrences of such cyber incidents, Figure 4.3 below shows the 8 most significant incidents in the graph in Figure 4.2. Also, Table 4.5 below both summarizes and gives details about these 8 cyber incidents. For example, a security incident (a red dotted circle) with a description of "Malware Spread-out to End Users," is displayed in Figure 4.3 between the fourth quarter of 2014 and the first quarter of 2015 (roughly in the middle of the graph). The details of the cyber incident can be found in Row 5 of Table 4.5, such as that Cryptsy, BTC-E, BitPay, BitStamp and LocalBitcoin were victimized by an end-point targeted cyberattack during that period.

[5] For 2018, the incidents until 2nd quarter were reflected.

[6] The term “zero-day” refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, official patch or update to fix the issue hasn’t been released. The vendor has to work quickly to fix the issue, but may fail to release a patch before hackers manage to exploit the security hole. That’s known as a zero-day attack [432].

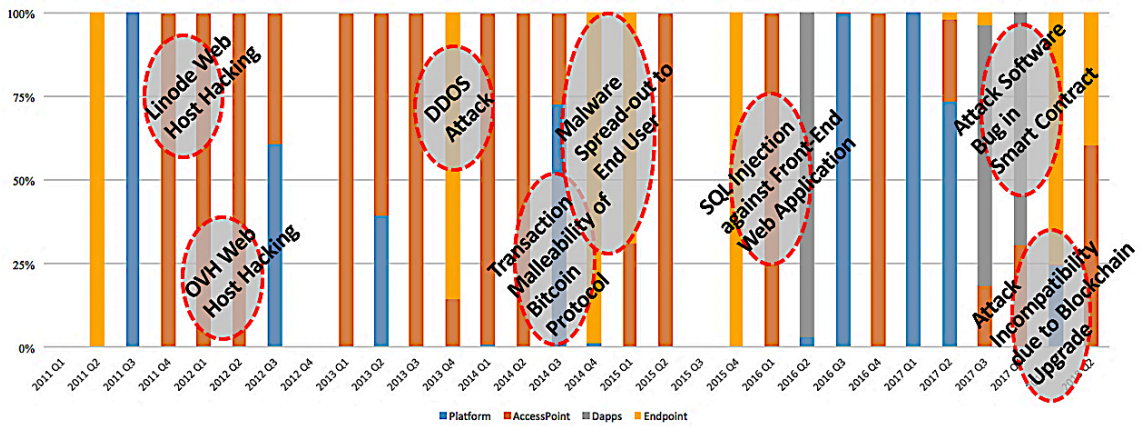


Figure 4. 3 – Types of cyberattacks affected multiple Blockchain systems over short time period.

From Figure 4.3 and Table 4.5, it is particularly notable that a number of Blockchain systems often remained vulnerable for 3 to 6 months even after the exploitation details were publicly known. In the IT security industry, it has been customary to suspect that human error would be the primary cause of most security issues in Blockchain systems. The aforementioned delay in addressing a security breach suggests difficulty and complexity in remediating the Blockchain systems to resolve security vulnerabilities in a timely manner.

Type of Cyber Attack(s)	**Period(s)**	**(D1) Platform Breach**	**(D2) Access Point Attack**	**(D3) DApps Exploit**	**(D4) Endpoint Hacking**	**Blockchain System(s) Affected**
Web Host (Linode) Hacking	2012 Q1		**A**			Slush Pool, Bitcoinica
Web Host (OVH) Hacking	2013 Q2		**A**			Slush Pool, Bitcoin central
DDOS Attack against Front-End Web Application	2013 Q4		**A**			BIPS, Input.io
Transaction Malleability of Bitcoin Protocol	2014 Q2	**P**				SilkRoad2, MT.Gox
Malware Spread-out to End-Users	2014 Q4 ~ 2015 Q1				**E**	Cryptsy, BTC-E, BitPay, BitStamp, LocalBitcoin
SQL Injection against Front-End Web Application	2016 Q1		**A**			Bit quick, Coinwallet.co
Attack Software Bug in Smart Contract on Ethereum	2017 Q3 ~ 2017 Q4			**D**		Parity Wallet Multi-Sig on Ethereum

Type of Cyber Attack(s)	Period(s)	(D1) Platform Breach (D2) Access Point Attack (D3) DApps Exploit (D4) Endpoint Hacking	Blockchain System(s) Affected
Attack Incompatibility due to Blockchain Upgrade	2017 Q4 ~ 2018 Q1	P	Black wallet, QuadraCX

Table 4. 5 – Types of cyberattacks affected multiple Blockchain systems over short period.

4.5 Victims of cyberattacks over multiple times

Nowadays, one of the most critical security policies for business continuity is establishing processes for incident response and security issue remediation in the event of a cyberattack. In today's banking and finance industries, it is quite rare for an organization's IT system to be subject to multiple cyberattacks over the years.

Figure 4.4 below illustrates a number of Blockchain systems which experienced multiple cyberattacks (grey) over the total number of cyberattacks (black plus grey) in a given year. On average, at least 10 to 20 percent of victims have experienced cyberattacks multiple times, and the percentage increased to 40 percent in 2017. This suggests that the nonexistence of a central authority in decentralized system architecture negatively impacts the setup and execution of business contingencies and system security policies. It can also be interpreted that many Blockchain systems are simply utilizing the inherent security features of Blockchain technology to protect the system, rather than implementing additional security protection.

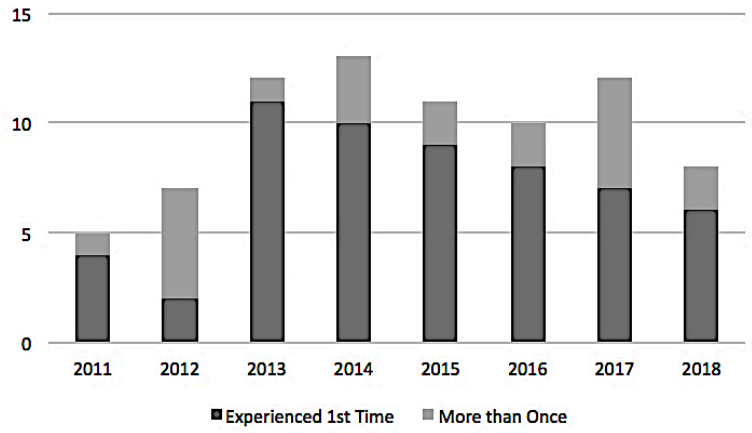


Figure 4. 4 – Number of Blockchain systems, which experienced multiple Cyberattacks (grey), over total number of Cyberattacks (black plus grey) in the year.[7]

4.6 Fatalities from cyberattacks

Below, Figure 4.5 graphically illustrates the number of Blockchain system organizations that closed due to cyberattacks. According to the U.S. Department of Homeland Security, 33 percent of all cryptocurrency exchanges were hacked, and nearly half of the victims were closed between 2009 and 2016 [199]. Moreover, according to crypto asset and Blockchain technology digital media, "Coin Desk," 5 out of 12 victims went out of business due to heists in 2017 [200].

By contrast, data from the Privacy Rights Clearinghouse showed that only 67 out of the 6,000 operational U.S. banks that have centralized systems experienced a publicly disclosed data breach since year of 2010. This is roughly 1 percent of the total number of banks in the U.S. [201]. This suggests that cyberattacks on the Blockchain system are far more critical to an organization, and damages are not easily controlled and remedied by the system in the event of a cyberattack.

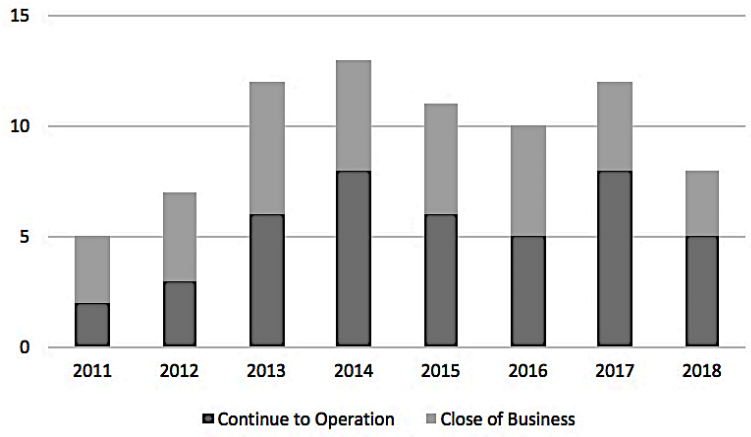


Figure 4. 5– Number of close of business organizations due to the cyberattacks (grey) over total number of Cyberattacks (black plus grey) in the year.[8]

4.7 Patterns of the cyberattacks

As shown in Table 4.1, a large number of cyber incidents occurred at the system area of authentication and identification. More than a half of 78 security incidents were closely related to either authentication bypass or user's identification theft, caused by phishing email, malware spread-out, credential brute-forcing or enumeration.

[7] For 2018, the incidents until 2nd quarter were reflected.
[8] For 2018, the incidents until 2nd quarter were reflected.

One of the reasons hackers prefer authentication and identification as their exploitation target can be found in Table 4.6 below. The table lists the exploitation phases between a centralized distributed system and a distributed (Blockchain) system in A&P (attack and penetration) from a testing methodology standpoint. As described, many of the exploitation steps required to perform a cyberattack on a centralized system are unnecessary for hacking Blockchain systems.

For example, in the case of an existing centralized system, hackers expend a lot of effort obtaining knowledge about the target through reconnaissance. This process takes usually weeks or even months since an organization rarely discloses centralized system information to the public without a compelling reason, for security purposes. However, as mentioned in Chapter 3, the decentralized (Blockchain) system must open a significant portion of its system assets to public access due to its characteristic as open source and also due to its autonomous operation. Thus, an attacker does not need to conduct reconnaissance. Blockchain system information can be easily obtained from the Internet (publicly accessible cyberspace). In addition, the complete anonymity of Blockchain technology allows hackers to penetrate the system without worrying about identity disclosure and evidence destruction (See Phase 4 and Phase 5 in the table below).

This suggests that the security of the Blockchain system relies heavily on user identification and authentication, and Blockchain system hacking can be relatively simple if the hacker can disable or bypass the user validation process.

Exploitation Phase(s)	Centralized System	Blockchain System
Phase 1 - Reconnaissance	Reconnaissance involves gathering information about target system without individual's or company's knowledge.	No Need. As characteristic of Blockchain, most of technical and implementation details are open source and available on-line for easy access.
Phase 2 – Scanning	Attacker should obtain information about target user, node, application or system for success exploitation. Hence, in most case, attacker should spend lots of effort to find data related to the victim(s).	No Need. All information is transparently disclosed on-line. Attacker can simply find target without much effort. Furthermore, as characteristic of decentralized system, attacker can easily join the system as user or minder (nodes) to be part of the system.
Phase 3 – Gaining Access	Attacker should be able to obtain access to target application and conduct malicious activity.	Attacker needs to obtain access to target application and conduct malicious activity.
Phase 4 – Maintaining Access	Since in most case of cyberattack takes days, weeks or even months to succeed complete exploitation, attacker(s) tries to find way to maintain the access to system such as back door, hidden service running etc.	No Need. The exploitation against Blockchain would be simple, fast and quick. And it does not require multiple steps but simple transfer fund to one's own address. Hence, attacker does not have any reason to keep one's access within system for later usage.

Exploitation Phase(s)	Centralized System	Blockchain System
Phase 5 – Covering Track	Attacker should cover the tracks related to the cyberattack to avoid detection or even to be anonymous.	No Need. The transition record in Blockchain is irreversible. However, there is no need for attacker to remove tracks after exploitation since all of data transition is anonymous. In other words, system can trace and monitor of malicious activity, but cannot find actually who conducted the activity.

Table 4. 6 – Comparison of cyberattack methodology between centralized and decentralized (Blockchain) system [202].

4.8 Identified cyberattacks and security vulnerabilities

Table 4.7 below lists all attacks and vulnerabilities identified from the investigation of 78 cyberattack cases in Table 4.1. The first column, which contains the name of the attack or security problem, begins with the naming convention AV-N that indicates Attack/Vulnerability Number N for later use in this paper. The third column represents the attack/vulnerability target for the Blockchain security system domain set in Chapter 3. The forth column contains the security risks discovered by Threat Modeling Exercises in Chapter 3. The fifth column describes the potential for adverse consequences of cyberattacks or system exploitation.

Cyberattack(s) / Security Vulnerability(s)	**Description**	**Security Domain** *(D-N)*	**Security Risk** *(SR-N)*	**Adverse Consequence(s)**
(AV-1) 51% attack	51% attack refers to an attack on a Blockchain by a group of miners controlling more than 50% of the network's mining hash rate, or computing power [203].	D-1	SR-1	• Un-authorized data addition to Block can be occurred. • Data content alteration can be occurred.
(AV-2) Transaction malleability vulnerability	Transaction malleability vulnerability caused when the data transaction hash (created by user's private & public key pair) was not properly validated by Blockchain. The security vulnerability lets an attack change data transaction ID or hash and makes it possible for the attacker to pretend that a transaction associated to someone else [204].	D-1	SR-13, SR-14, SR-16	• Data content alteration can be occurred. • Authorized but incorrect data transaction can be occurred. • System resource may be malfunction.
(AV-3) Double spending attack	Double spending attack means more than one data transition occurrences prior to proper update on Blockchain. In case of crypto-currency Blockchain system, the attack specially refers as spent twice without account balance update [205].	D-1	SR-13, SR-14	• Intended process alteration can be occurred. • Authorized but incorrect data transaction can be occurred.

Cyberattack(s) / Security Vulnerability(s)	Description	Security Domain *(D-N)*	Security Risk *(SR-N)*	Adverse Consequence(s)
(AV-4) Timestamp dependence vulnerability	Timestamp on Block is generated by miners. Hence, if Blockchain protocol does not implement additional timestamp validation, its critical operation related to Block timestamp (such as random number generation based on timestamp) is going to be vulnerable [206].	D-1	SR-13, SR-14, SR-17	• Timestamp of Block can be manipulated. • System resource may be malfunction.
(AV-5) Sybil attack	A Sybil attack refers assigning several identifiers to the same node in Blockchain system environment. This attack is possible if a hacker can take control of multiple nodes so that the victim is surrounded by fake nodes that close up all their transactions. Finally, the victim becomes open to various type of attacks with fake data [207].	D-1, D-3	SR-13, SR-16, SR-17	• System resource may be un-available. • System resource may be malfunction.
(AV-6) DNS attack	A DNS attack refers an exploit in which an attacker takes advantage of vulnerabilities in the domain name server [208].	D-2	SR-7, SR-8	• System resource may be un-available. • System resource may be malfunction.
(AV-7) In-secure implementation of cold/hot storage	When Blockchain system cannot secure the cold/hot storage enough to prevent cyberattack, attacker can exploit and manipulate data (in case of crypto currency Blockchain, stored fund can be stolen) [209].	D-2	SR-3, SR-5	• Secured system resource(s) may be turned into state of vulnerable. • System resource may be un-available. • System resource may be malfunction.
(AV-8) SQL injection attack	A SQL injection attack refers insertion or injection of a SQL query via the input data from the client to the application [210].	D-2	SR-3, SR-5	• Un-authorized data disclosure may be occurred. • Un-authorized data alteration may be occurred.
(AV-9) 3rd party authentication bypass attack (multi-sig or 2nd factor authentication)	3rd party authentication bypass attack on Blockchain system refers that an attacker can gain accessibility of other user(s) by evading or circumventing a 3rd party authentication mechanism [211].	D-2, D-4	SR-11	• System resource may be un-available. • Un-authorized data transaction can be occurred. • Un-authorized data disclosure can be occurred.
(AV-10) Public & Private key pair theft attack	Public & private key pair theft attack has been major target for years in terms of Blockchain system hacking. Attacker can obtain users' key pair in various ways, such as system exploit, end-user computer device hacking, malware, phishing email etc.	D-2, D-4	SR-7, SR-8, SR-9	• Un-authorized data transaction can be occurred. • Un-authorized data disclosure can be occurred.
(AV-11) Reentrancy vulnerability	With calling external contact feature in Smart Contract, attacker can take over the control flow, and make changes to victim's Smart Contract data that the calling function wasn't expecting [212].	D-3	SR-15, SR-16, SR-17	• Function(s) may be called repeatedly, before the first invocation of the function was finished. • Different invocations of the function may triggered in destructive ways.
(AV-12) Cross-function race condition vulnerability	A race condition is the behavior of Smart Contract where the output is dependent on the sequence or timing of other uncontrollable events. It is coding bug when events do not happen in the order the programmer intended [213].	D-3	SR-5, SR-6	• Smart contract(s) may be triggered to conduct process in un-desired way.

Cyberattack(s) / Security Vulnerability(s)	Description	Security Domain *(D-N)*	Security Risk *(SR-N)*	Adverse Consequence(s)
(AV-13) Distributed Denial of Service attack (DDOS)	DDOS on Blockchain system refers that attacker attempt to disable the system by consuming all its processing resources with tremendous amount requests in short period time. The attacker aims to disconnect mining pools, e-wallets, or crypto currency exchanges [214].	D-3	SR-5, SR-6	• Smart contract may be malfunction. • Smart contract may not execute due to out of token consumption limit.
(AV-14) Self-destruction attack	As nature of Ethereum Blockchain system, an attacker can craft malicious Smart Contract with self destructive functionality and send it to others. The self destructive function can remove all bytecode from the victim's Smart Contract address and sends all ether (ETH) to the parameter-specified address [215].	D-3	SR-15, SR-16, SR-17	• Smart contract may be malfunction. • Smart contract may be deleted by itself with deleting bytecode at the target address.
(AV-15) In-secure implementation of delegate function	Smart Contract with in-correct usage of delegate function can leave its function(s) accessible from public. This vulnerability can allow attacker's crafted Smart Contract to modify ownership of victim's Smart Contract [216].	D-3	SR-13, SR-14	• Token may be lost. • Un-authorized data transaction can be occurred.
(AV-16) AJAX (JSON) Cross-Site Scripting (XSS) attack	Cross-site Scripting (XSS) is a technique by which malicious content is injected in the form of HTML/JavaScript code. XSS exploits can be used for triggering various other attacks like cookie theft, account hijacking, phishing, and denial of service [217].	D-4	SR-1, SR-3, SR-4	• Valid but un-intended data transaction can be occurred.
(AV-17) AJAX call (JSON) hijacking attack	When end-user browser makes AJAX call (as "XMLHTTPRequest" object) to server, the user browser replays cookies for each request for proof of authenticity. If server does not implement same origin policy verification, attacker can trigger the user browser to send victim's data to one-self [218].	D-4	SR-1, SR-3, SR-4	• Un-authorized data transaction can be occurred.
(AV-18) Malware attack	A malware attack is a type of cyberattack in which malware or malicious software performs activities on the victim's computer system, usually without his/her knowledge. In order to obtain victim's credential or private/public key pair, attacker infects end user personal computing device to malware [219].	D-4	SR-1, SR-3	• Un-authorized data transaction can be occurred.
(AV-19) Session hijacking attack	Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token [220].	D-4	SR-1, SR-3	• Valid but un-intended data transaction can be occurred. • Authentication data theft can be theft. • Sensitive data theft can be occurred.
(AV-20) Malicious code execution attack	When an attacker can send malicious code to victim as form of software and can successfully trigger victim to execute the code, victim's computing device would be under control of attacker.	D-4	SR-2, SR-3	• Complete end user computing system exploitation may be occurred. • Un-authorized data transaction can be occurred.

Cyberattack(s) / Security Vulnerability(s)	**Description**	**Security Domain** *(D-N)*	**Security Risk** *(SR-N)*	**Adverse Consequence(s)**
(AV-21) Phishing attack	By posing as a legitimate individual or institution via SNS message or email, an attacker use social engineering technique to manipulate victims into performing specific actions, such as clicking on a malicious link or attachment or willfully divulging confidential information [221].	D-4	SR-4, SR-5, SR-6	• Data may be altered by malicious attacker. • Authentication data theft can be theft. • Un-authorized data disclosure can be occurred.
(AV-22) BGP hijacking attack	BGP hijacking is an illicit process of taking control of a group of IP prefixes assigned to a potential victim. The attack can be achieved by changing paths used for forwarding network traffic, exploiting the weaknesses of BGP [222].	D-4	SR-7, SR-8	• Un-authorized data transaction can be occurred. • Un-authorized data disclosure can be occurred.
(AV-23) Communication channel hijacking attack	If a end-user communicates with server via in-secure channel, attacker can sniff or eavesdrop the transit data in the middle, such as man in the middle attack.	D-4	SR-7, SR-8	• Un-authorized data transaction can be occurred. • Authentication data theft can be theft. • Un-authorized data disclosure can be occurred.

Table 4. 7 – Identified cyberattacks and security vulnerabilities of Blockchain System from section 4.1 and their consequences.

CHAPTER 5 - Causal Analysis of Hacking Incidents in Blockchain Systems

“Trusted third parties are security holes.”

– Nick Szabo
(inventor of Bit gold, a precursor to Bitcoin)

"The measure of success is not whether you have a tough problem to deal with,
but whether it is the same problem you had last year."

— John Foster Dulles
(Former Secretary of State)

5.1 Causal analysis for security incidents in a Blockchain system

Extensive research and studies on security incidents in Chapter 4 showed that the Blockchain system contains a significant number of security flaws, unlike what is commonly thought. For example, a review of collected data in Table 4.1 reveals that many blockchain systems were victimized by successive hacks using similar methods in a short period of time. The review also indicates that many Blockchain systems do not properly perform a security remediation process. However, such a simple analysis alone cannot diagnose the security mechanism of the Blockchain system and examine the root cause of the accident.

For in-depth analysis, Table 5.1 suggests a seven-step holistic analysis framework for system security incidents. The framework is designed to achieve two goals: (1) analyzing security for a non-centralized system and (2) compiling successive hacking cases into one analysis. Most of the approaches described in the framework are based on CAST (Cause Analysis using System Theory). Compared to traditional cyber incident analysis, CAST provides a new approach of managing cybersecurity risks to understand the reasons for the loss and implement countermeasures to prevent future violations [223]. The approach allows an analyst to expand beyond a single failure event and analyze a broader sociotechnical system to understand systematic causal factors for security incidents [224].

Step #	Step	Brief Description(s)
1	Describe intrusion and hazard of the security incident.	This step describes intrusion of the cyberattack and hazard of the Blockchain system. Brief description of the exploitation and heist is included in high level view.

Step #	Step	Brief Description(s)
2	Identify the system security constraint(s) and requirement(s).	In order to understand security requirement, this step list out all safety constraints of Blockchain system.
3	Identify system security structure to avoid cyberattack.	This step identifies and explains security defense and protection structure in system perspective. The identification includes not only system level security, but also code level protection.
4	Summarize the proximate events chain leading to the accident or incident.	This step lists timeline of all of major events related to the security incident.
5	Analyze the hacking incident(s) against the Blockchain system.	This steps starts analysis exploitation and hacking incident as of following: a) System safety controls failures. b) System operational failures. c) Unhandled external disturbances. d) Communication / incident response failure.
6	Identify incident response and remediation process after cyberattack(s). Discover ineffectiveness and deficiency in aspect of system security.	This step examines coordination / communication in security control structure and hierarchy in Blockchain system.
7	Summarize cause of series of hacking incident and major security weakness of Blockchain system in security control perspective.	This step summarizes misplacement of security control and key weaknesses that contributed to the consecutive heists.

Table 5. 1 – Causal analysis steps for series of heists against a Blockchain system [225].

In the remainder of this chapter, I will enumerate the process of applying the causal analysis framework to two of the most publicly notable Blockchain system cyberattack cases. Sections 5.2 and 5.3 address three consecutive hacking incidents in the Ethereum Blockchain system and two consecutive hacking attacks in the Bitfinex Crypto-Currency Exchange (Bitfinex). In these sections, each cyberattack case will be analyzed in detail by applying Steps 1 through 6 described in Table 5.1. More specifically, in Section 5.2 a series of causal analysis of three different cyberattacks in the Ethereum Blockchain system will be performed in chronological order to analyze the difficulties of security modification and the limitations of defense. On the other hand, in Section 5.3 one causal analysis about two different cyberattacks in Bitfinex will be conducted to analyze how the former affect the events that occur later. Finally, as Step 7, Section 5.4 will summarize the misplacement of security controls and weaknesses in system security, which are the main causes of continuous cybersecurity incidents.

5.2 Ethereum Blockchain heists

Ethereum is an open-source, Blockchain-based system focused on enabling users to create and use distributed applications (dApps) known as smart contracts [226]. Essentially, Bitcoin is also a type of smart contract, but its functionality is limited to handling currency data transactions. Ethereum, on the other hand, is a decentralized programming platform that creates an operating environment in which smart contracts can provide a much wider range of data processing and execution [227]. Just like other applications built on top of Blockchain technology, the smart contract also runs autonomously without any outside purview or the control of a single authority [228].

The lifecycle of an Ethereum smart contract can be divided into two stages: development and execution. During the development phase, developers program smart contracts using the Solidity programming language with information such as functions, data, and user addresses. In the execution phase, users will enter into mutual smart contracts without central control using Ether (ETH), a cryptocurrency designed specifically for Ethereum [229]. When Ethereum first appeared, many people applauded the technology that enables the promise and fulfillment of contracts without the need for a centralized control or guarantor, and without the need for existing contract law systems.

Causal Analysis #1 – *"TheDAO"* hack

"*TheDAO*" was the first DAO implementation based on the Ethereum Blockchain system created by the German company Slock.it [230] and intended to operate as a hub that dispenses funds to projects, like a crowdfunding vehicle governed by participants' votes [231].

To briefly describe "*TheDAO*" from a business perspective, once a "*contractor*" (who made a proposal to produce a product or offer a service) submits a funding proposal to "*TheDAO*," the "*investors*" (who are the nodes of the Ethereum Blockchain system) will cast votes on the investment proposal. If the proposal collects enough votes, "*TheDAO*" transfers the investment funds to the "*contractor*." The "*contractor*" then starts executing the commitments specified in the proposal, such as service delivery or product production in the real world [232]. When the *"contractor"* returns the revenue to "*TheDAO*," "*TheDAO*" distributes the profit to the investor [233].

Figure 5.1 below illustrates "*TheDAO*" from a technical point of view. As shown, "*TheDAO*" performs five steps to achieve the business goal: investing funds (child DAO creation), executing the proposal, returning the investment, sharing revenue, and distributing dividends. In the first step, fund investment, an investor, who obtained a voting right by purchasing The DAO Token (TDT) with Ether, will cast a vote on the

proposal for funding. As investors complete the voting, the Ether(s), which are the amount of TDT used for the vote, will be transferred to a main account called the *"DAO main account*." The voting process will create a child DAO for the investor as a form of smart contract and the child DAO is chained to all other child DAOs in a continuous chain all the way up to main DAO [234]. If the investor changes his mind and withdraws the vote, the child DAO that contains the invested funds (TDT) will be split from the *"DAO main account"* and refunded to the investor [235]. In the second step, proposal execution, all of investment funds will be sent from the *"DAO main account"* to the "*contractor*" [236] once the proposal is approved [237]. In the third step, investment return, the result of a proposal will pay back the revenue to the "*DAO Reward Account*" as an investment return. In the fourth step, revenue sharing, Ethers in the "*DAO Reward Account*" will be split from the main DAO for autonomous operation costs and for investment distribution of the child DAOs in proportion to amount of their original investment [238]. In the fifth step, dividend distribution, "*TheDAO*" distributes dividends to their TDT holders. "*TheDAO*" will send the total amount that it wants to be distributed into a "*Reward Account*" for distribution.

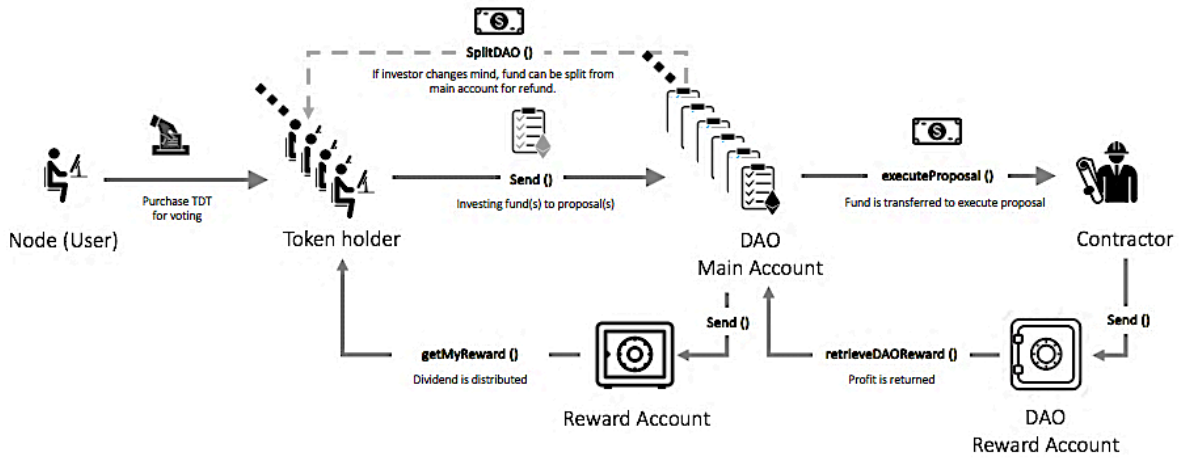


Figure 5. 1 – Normal flux of the fund in "TheDAO" operation . Please note the arrows indicate system operation with associated actual function invocation(s) in source code, such as "Send ()", "SplitDAO ()", "executeProposal ()", "retrieveDAOReward ()", and "getMyReward ()" [239].

In terms of revenue generation, "*TheDAO*" was not significantly different from other existing investment models [240]. However, "*TheDAO*" had received tremendous interest and expectation from the industry at the planning stage due to the many advantages of distributed applications (dApps) based on Blockchain technology, such as transparency of execution, integrity of fulfillment, independency of management, and autonomous operation [241]. As soon as it began crowdfunding on April 30, 2016, the record high of $150 million was invested into the project in just 28 days, the largest

project ever in the history of crowdfunding [242]. At the time commercialization of Blockchain technology was limited to the implementation of the cryptocurrency system, and many experts believed the future of Blockchain depended on the success of "*TheDAO*," the first and most notable dApps (distributed applications).

Step #1: Intrusion and hazard

Unknown attackers exploited the security vulnerability in the code of "*TheDAO*" dApps, known as a recursive bug. The vulnerability allowed the attacker to transfer all funds from the *"DAO main account"* to their own [243]. The hazards in this case were that Ethereum Blockchain allowed unsafe distributed applications (dApps) to operate on its system environment and did not adequately address countermeasures in the event of a cyberattack.

Step #2: Security constraints and requirements [244]

- The Ethereum Blockchain system must allow dApps to execute on the system environment without any censorship due to the principle of "Code is Law."
- "*TheDAO*" solidity program must undergo in-depth secure source review with a trustworthy party in order to minimize the risk of cybersecurity incidents.
- "*TheDAO*" solidity program must remediate all known security issues with sufficient validation of a fix prior to its deployment to the Ethereum Blockchain system.
- "*TheDAO*" solidity application development must develop an incident response plan for any malfunction, incorrect operation or cyberattack.
- "*TheDAO*" solidity application development must be proactive to resolve any encountered issues upon occurrence of those incidents.

Step #3: System security overview

Like other Blockchain-based systems, Ethereum utilized the inherent security features of Blockchain technology as the key and only system protection [245]. As shown in Figure 5.2 below, the node (user) must be authenticated in the Ethereum Blockchain system before proceeding with a data transaction or running dApp within the system environment. However, with the exception of the user authentication process, the Ethereum Blockchain system was structured to fully trust all decisions and executions made by software (dApp) running on each node without further validation and verification. Fortunately, but indeed unfortunately, before this "*TheDAO*" hack, the Ethereum Blockchain system never experienced major security problems like system exploitation, software bugs, and so on [246]. Since its launch in 2015, it has been

operating for about a year without any problems [247].

However, shortly after the successful fundraising of "*TheDAO*," a lot of questions and warnings were raised regarding system security. Especially, computer science professors Gun Emin Turer and Vlad Zamfir of the Ethereum Foundation reported several potential security issues in "*TheDAO*" code to the community. Their paper, "A Call for a Temporary Moratorium on *"TheDAO,"* revealed actual multiple attacks that manipulated "*TheDAO*" processes which led to a theft of investments [248].

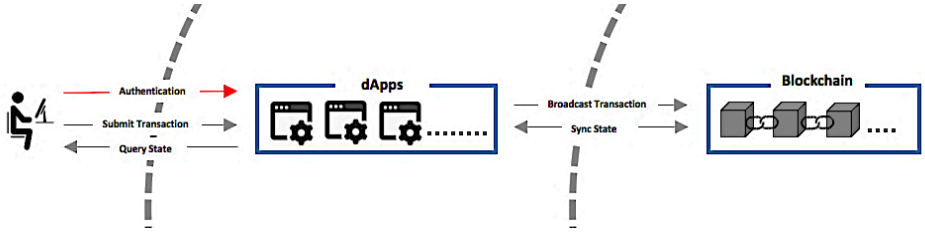


Figure 5. 2 – Simplified view of data communication among node (user), dApps and Blockchain in Ethereum Blockchain system [249]. Please note that the authentication request as colored in red is the only security verification in data transitions among them.

Step #4: Proximate events chain [250]

Step #4 contains key events related to the "*TheDAO*" hack in chronical order, such as pre-cautions and warnings by computer security researchers about potential exploitation, cyberattack preparation and execution phases by malicious users, and incident response efforts of the Ethereum development community. To help better understand the cyberattack, Figure 5.3 illustrates 6 phases of "*TheDAO*" hack (5 preparation procedures plus attack execution) based on Figure 5.1 (*Normal flux of the fund in "TheDAO" operation*).

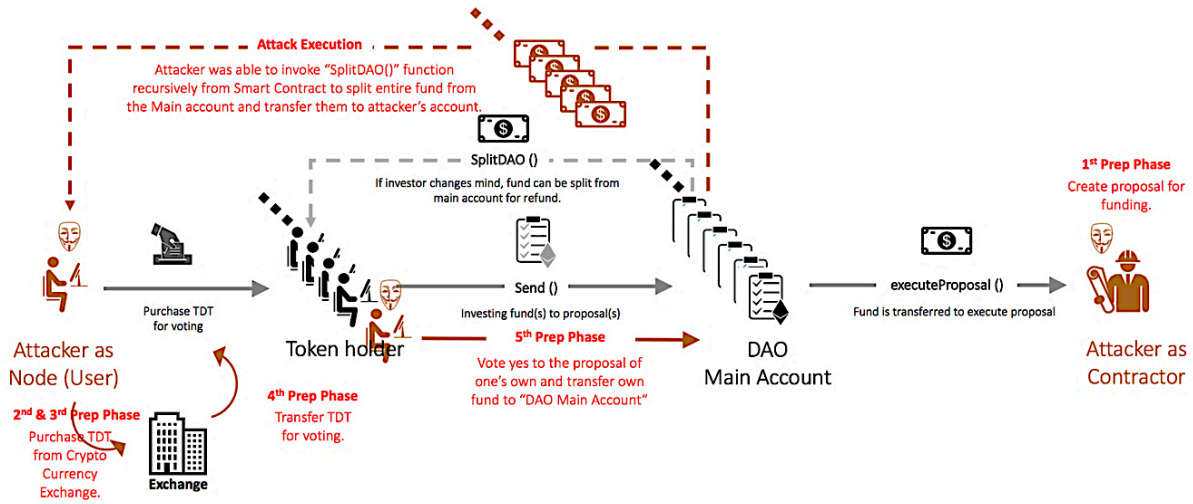


Figure 5. 3 – The red colored lines and description illustrate preparation and execution of "TheDAO" hack in high level view. Details of each phase is described in event chain.

- On May 7, 2016, a "A Call for a Temporary Moratorium on *TheDAO*" became available to the public, which exposed multiple potential security issues. The researchers issued a warning about investing in "*TheDAO*" before the security issues were resolved. However, the investments continued to flow in without any disruption [251].

- On May 27, 2016, the Slock.it team, who launched "*TheDAO*" project, posted their first proposal, "Slock.it UG Proposal #1, DAO Security," on its blog site. This proposal included the plan to remediate security issues and acknowledged the necessity of hiring staff to protect "*TheDAO*" from attack vectors [252].

- On June 8, 2016, as shown in Figure 5.3, an attacker executed the first preparation process for the cyberattack by creating a function proposal, "*proposal 59,*" as *"contractor"*, as shown in Figure 5.3 [253].

- On June 9, 2016, Peter Vessenes posted a blog entitled, "*Race to Empty,*" announcing a bug discovery with detailed analysis and realistic world attack scenarios [254]. At this point the Ethereum developer community became aware of this issue.

- On June 10, 2016, a potential security vulnerability called, "Re-Entrance (recursive) Attack," was discovered by Christian Reitwiessner, the creator of solidity [255]. Some of main solidity developers became aware of the issue and

confirmed that all smart contracts running on the Ethereum Blockchain system were affected by the security vulnerability.

- On June 10, 2016, a few hours after Christian's post, it became known to the public that the first smart contract "*MakerDAO*" was vulnerable to the "Re-Entrance (recursive) Attack" [256].

- On June 12, 2016, Eththrowa announced that the same security vulnerability was discovered within "*withdrawRewardFor()*" function in theDAO [257]. Stephan Tual, one of "*TheDAO*" creators, announced that the "*recursive call bug was identified, but confirmed no theDAO funds at risk*" [258].

- On June 14, 2016, some security fixes were proposed and placed on hold for review by "*TheDAO*" development team. After the review, "*TheDAO*" development team decided to schedule a patch update in the framework's code in subsequent time [259].

- On June 14, 2016, the attacker executed the second preparation process for the cyberattack, as shown in Figure 5.3. The attacker purchased and deposited 305,000 TDT in a Kraken cryptocurrency exchange [260].

- On June 14, 2016, the attacker executed the third preparation process for the cyberattack, as shown in Figure 5.3. The attacker purchased and deposited 306,914 TDT in a Poloniex cryptocurrency exchange [261].

- On June 14, 2016, the attacker executed the fourth preparation process for the cyberattack, as shown in Figure 5.3. For the first time, the attacker transferred TDT to a main account [262].

- On June 15, 2016, the attacker executed the fifth and final preparation process for the cyberattack, as shown in Figure 5.3. The attacker voted yes to "*proposal 59*" and transferred TDT to the *"DAO Main Account"* [263] [264].

- On June 16, 2016, many bloggers began warning investors to stop investing in "*TheDAO*" due to the confirmed critical security vulnerabilities. However, despite the warning about risk, investments continued to increase [265].

- On June 17, 2016, at 03:34 UTC, the attacker conducted the exploitation and executed the attack as shown in Figure 5.3 [266]. The attacker called function

SplitDAO() recursively from a smart contract to transfer others' funds to his own account.

- On June 17, 2016, at 07:10 UTC, the headline, "*I think TheDAO is getting drained right now. Unfortunately, I am on a train to work, so cannot investigate, but looks like recursive call exploit of some kind,*" was posted at "r/Ethereum" on the social news website Reddit [267].

- On June 17, 2016, at 07:29 UTC, Vitalik Buterin, the Ethereum founder, responded to the post on the social news website Reddit, "*Is anyone in the process of splitting from TheDAO right now? It would really help if the person whose split will finish in 2 hours can contact us*" [268].

- On June 17, 2016, at 10:05 UTC, Slock.it finally confirmed the attack and announced on its public website that, "*TheDAO is being attacked. It has been going on for 3-4 hours, it is draining ETH at a rapid rate. This is not a drill. We need to spam the Network so that we can mount a counter attack all the brightest minds in the Ethereum world are in on this*" [269].

- On June 17, 2016, at 11:00 UTC, the attacker suddenly stopped the attack and ended the withdrawal of funds from main account after a theft of 3.5M ETH ($50MM) [270].

- On June 17, 2016, at 11:13 UTC, Ethereum founder Vitalik Buterin announced a major update plan for "*TheDAO*" vulnerability. For the first time, he mentioned the possibility of executing a soft or hard fork as resolution for this situation [271].

- On June 18, 2016, the Ethereum developer community made its first attempt to prevent further attacks by updating the smart contract to split the rest of "*TheDAO*" funds before the entire "*TheDAO*" drained. The attempt required a certain number of consensus votes from the stakeholders, but new blocks were added too quickly to generate enough votes to split. As a result, the attempt failed [272].

- On June 19, 2016, the Ethereum developer community made a second attempt to prevent further attacks by creating minor transactions in an endless loop so as to jam the attacker's traffic. However, this attempt was not successful either [273].

- On June 21, 2016, the Ethereum developer community made a third attempt to prevent further attacks using the same attack method that was performed by an attacker. This time it was successful, and they were able to drain all of the rest of the 6M ETH into a "*ChildDAO*" called "*WhiteHatDAO*" [274].

- On June 22, 2016, the attacker then performed another preparation process to target the *"WhiteHatDAO"* in the same way. The attacker voted "yes" and transferred TDT to the main account of the "WhiteHatDAO" for another recursive split DAO attack. However, the attacker had to wait 24 days to execute the attack, since the whole voting process for the *"WhiteHatDAO"* would take 24 days for completion. Hence, the Ethereum developer community was able to obtain a window of 24 days to recover the damage and restore the system state [275].

- On July 20, 2016, the Ethereum developer community successfully completed the hard fork and this "*TheDAO*" security incident was finally closed [276].

Step #5: Analyzing the hacking incident

The attacker was able to successfully hack using two bugs found in the "*splitDAO*" function in the "*TheDAO*" smart contract. The first exploit was based on a "*Re-entry*" bug that allows calling the "*splitDAO*" function recursively through a code insertion attack. The second exploit was based on a "*Race-to-Empty*" bug that allows updating the account balance of a victim's smart contract after the "withdraw" function call by code insertion.

About one week prior to the occurrence of the attack, Peter Vessenes, one of the Ethereum developer community members, posted a potential security issue identified as "*Race-to-Empty*" on his blog. He discovered the security vulnerability from theDAO smart contract source code, and he provided detailed analysis and proposed solutions in the post. The root cause of the security issue was involved in the "splitDAO" function in "*TheDAO*" smart contract, and this allowed the malicious attacker to execute the function recursively on other user's contracts to drain the funds [277]. Unfortunately, due to the nature of the Ethereum Blockchain system, function(s) of smart contracts can be triggered and executed by external request. The introduction of the "*Race-to-Empty*" issue demonstrated how the default operation rule of Ethereum, which is "*one contract can trigger other contracts' code*," can be abused and turned into a malicious attack [278].

Below, Code 5.2 is the simplified implementation from "*TheDAO*" source code. The "*splitDAO*" function lets token holders place their funds for a particular *_proposalID* [279]. It calculates the amount of funds to move for this particular caller and then calls the "*createTokenProxy*" function to move the fund.

```
function splitDAO (uint _proposalID, address _newCurator) noEther onlyTokenholders returns (bool _success)
{

     .... [snip]

     uint fundsToBeMoved = (balances[msg.sender] * p.splitData[0].splitBalance) /
     p.splitData[0].totalSupply;

     if (p.splitData[0].newDAO.createTokenProxy.value(fundsToBeMoved)(msg.sender) == false)
          throw;

     .... [snip]

     Transfer (msg.sender, 0, balances[msg.sender]);      // LINE 1
     withdrawRewardFor (msg.sender);                      // LINE 2
     totalSupply -= balances[msg.sender];                 // LINE 3
     balances [msg.sender] = 0;                           // LINE 4
     paidOut [msg.sender] = 0;                            // LINE 5
     return true;

}
```

Code 5.1 – SplitDAO function.

The security issue starts from "*Line 2*" which is calling "*withdrawRewardFor*" function as illustrated in Code 5.2. After the function call, the values of "*totalSupply"* at Line 3, "*balances"* at Line 4 and "*paidOut"* at Line 5 are all updated, which will result in withdrawal of the funds [280].

As shown in code snippet 5.2 below, the "*withdrawRewardFor*" function is a feature of "*TheDAO*" smart contract that allows the user to request the investment withdrawal from the total fund, which is called a "*split*." The problem is that the "*withdrawRewardFor*" function allows setting the address for the destination of the split funds by external function call. Moreover, the "*withdrawRewardFor*" function is allowed to be called recursively in all subsequent recipient's "*TheDAO*" contract (so called child DAO). Therefore, if a malicious user calls the "splitDAO" function recursively with setting *_account* address to his own address, then all of subsequent *"TheDAO"* investment funds will be transferred to the attacker's account [281].

```
function withdrawRewardFor(address _account) noEther internal returns (bool _success) {

     .... [snip]

     if (!rewardAccount.payOut(_account, reward))
          throw;
     paidOut[_account] += reward;
     return true;

}
```

Code 5.2 – withdrawRewardFor function.

Figure 5.4 below shows an overview of how the attacker drained all funds from "*TheDAO*" smart contracts. For the preparation step, the attacker created a child

smart contract (child DAO) and transferred funds (DTD) to "*TheDAO*." Then the attacker called the "*splitDAO*" function recursively in all subsequent contracts and transferred funds to the attacker's address [282]. With this attack method, an attacker could simply and quickly transfer all of "*TheDAO*" funds to his address.

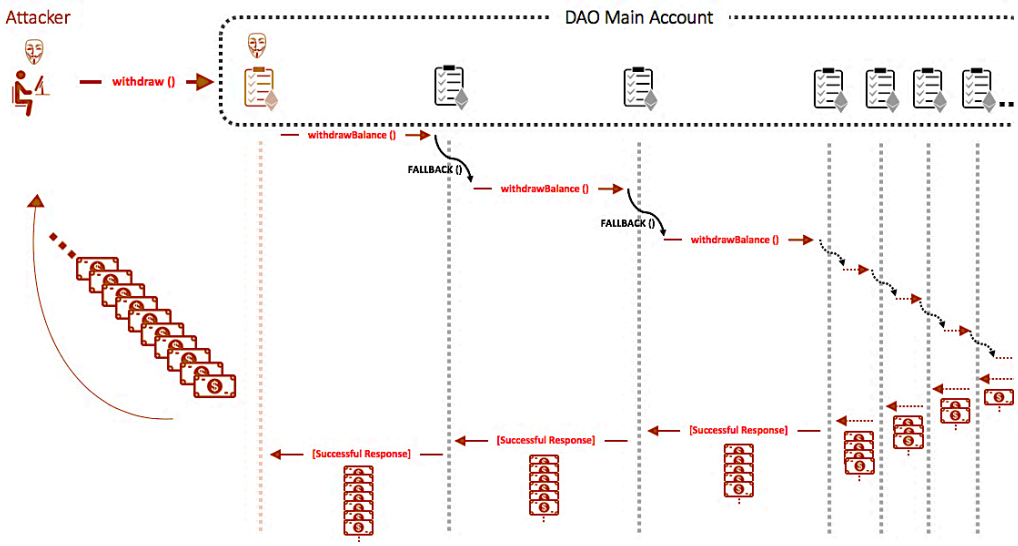


Figure 5. 4 – The simplified view of re-entry attack targeted to "TheDAO" [283].

Step #6: Response to the exploitation and remediation process

Subsequently, in response to the cyberattack, the Ethereum development community held an election for Ether holders to vote on the following 3 options [284] [285]:

Option #1: Nothing - Ethereum Blockchain system runs as is. Nothing would be changed or modified. The attacker will keep the $50MM worth of Ether.

Option #2: Soft fork - The soft fork will rewrite the previous data in Blockchain utilizing its well-known security flaw called "51% attack" (which will be covered in Chapter 6 in detail). When a new tree of blocks spans with 51% of all nodes in agreement, the Blockchain will adapt the new tree span instead of others, as shown in Figure 5.5 below. However, the soft fork plan will result in the complete loss of the stolen Ethers since all the blocks which contained the transaction records will vanish.

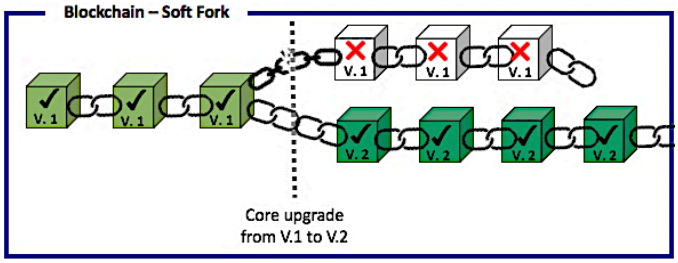


Figure 5. 5 - After the soft fork (core upgrade), version 1 Blockchain (version 1) will accept the new Block (version 2), but will not accept old Block (version 1). Eventually the old Blocks will die out since version 1 block will not be mined any longer.

Option #3: Hard fork - The hard fork will split the path and create two different versions of a Blockchain. One version will have a new software protocol, but the other version will remain the same software as previously. For those remaining as is, Blockchain will roll back transactions that siphoned off the stolen Ethers by invalidating transactions confirmed by nodes. Users who did not experience "*TheDAO*" hack should update to the new software protocol, otherwise all of their transactions during "*TheDAO*" hack will be invalidated. The hard fork will allow for all victims of "*TheDAO*" hack to get their funds back.

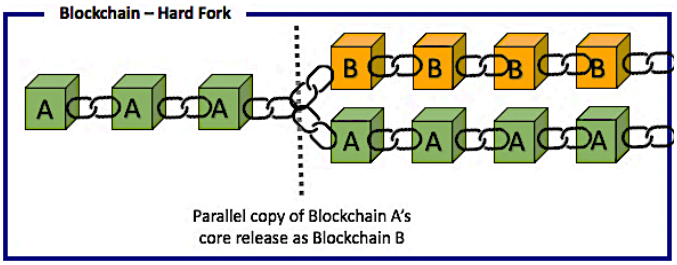


Figure 5. 6 - Blockchain A will not accept Blockchain B's Block, and vice versa, so hard fork is not backwards compatible. Unlike a soft fork, the old Blockchain A does not die out and continue existing and working. The chain splits into two separate chains, that share the same transaction history as before the split.

The initial decision was to use the soft fork option. However, the plan was changed to the hard fork option just before its application since several security researchers found potential threats of DoS (Denial of Service) attacks in the soft fork plan [286]. As a result, two Ethereum Blockchain systems (Ethereum and Ethereum classic) have been isolated and coexist to the current time.

Causal Analysis #2 – first Parity Wallet Hack

The Blockchain system authenticates a user based on providing a public and private key pair. If a user supplies a private key corresponding to a given blockchain address, the user can change data in the address. The problem here is that while the Blockchain system relies heavily on system security for key pair authentication, it is a single point of failure since nothing else protects the system. Also, the irreversibility of Blockchain makes it impossible to recover after a cyber incident occurs. As described in Chapters 3 and 4 previously, key pair authentication of the system was the primary goal of the hacker, and cyberattacks such as identity theft or authentication bypass resulted in breaching of the system.

In order to keep the key safe from theft (especially for cryptocurrency), an application called a wallet was devised. The wallet stores each public and private key pair used for data transactions in Blockchain. The key pair either receives or transfers Bitcoin or Ether in the cryptocurrency Blockchain system. However, the wallet application was not able to make significant improvements in terms of system security. The wallet application still remained a single point of security failure in the system architecture, and the installed wallet file on a PC or workstation could be stolen by hacking, malware or even an offline situation.

In 2012, Bitgo introduced Multi-Sig technology to address single-point error issues. With Multi-Sig, the Blockchain system can implement a more secure authentication process that requires one or more signatures. This technology is based on a new type of address called "Pay to Script Hash" (P2SH). Functions supported by P2SH addresses convert an existing single signature (private key) into multiple signatures, and the signatures are distributed and stored to multiple parties, such as mobile devices or third-party online servers. To perform a data transaction, a user should use a subset of keys (i.e., 2 out of 3 private keys) from multiple parties (servers or devices). Hence, the Multi-Sig allows Blockchain systems to retain secure data transactions (such as Bitcoin or Ether transfer) even if one of the private keys is stolen [287]. After the infamous MT Gox security incident, the adoption of Multi-Sig authentication has been set up as a new security requirement in the Blockchain industry. Parity Technology, founded by Ethereum co-founder Gavin Wood, launched Multi-Sig for the Ethereum Blockchain system in early 2017, which was considered one of the most trusted cryptocurrency wallets in the market before the heist [288].

Step #1: Intrusion and hazard

As unknown attacker exploited an unsecured implementation of the Parity 1.5 Client’s Multi-Sig wallet running on the Ethereum Blockchain system. Through the exploitation, the attacker was able to obtain ownership of a victim’s Ethereum wallet.

Three Ethereum ICO projects were victimized by the heist and lost 153,037 Ethers estimated at about $30 million.

The hazard was that the unsecured dApps runs on Ethereum Blockchain without sufficient security review and verification. The first Parity Wallet Hack was caused by not only exploitation of a security bug in program, but also by the limited of safety control and risk assurance of the Blockchain system.

Step #2: Safety constraints and requirement

- The Ethereum Blockchain system must allow dApps to execute on the system environment without any censorship due to the principle of "Code is Law."
- The Parity Multi-Sig Wallet solidity program must undergo in-depth secure source review with a trustworthy party to minimize the risk of cybersecurity incidents.
- The Parity Multi-Sig Wallet solidity program must remediate all known security issues with sufficient validation of the fix prior to deployment to the Ethereum Blockchain system.
- The Parity Multi-Sig Wallet solidity application development must develop an incident response plan for malfunctions, incorrect operations or cyberattacks.
- The Parity Multi-Sig Wallet solidity application development must be proactive to resolve any encountered issues as soon as they occur.

Step #3: System security structure overview

Adding multi-signature (Multi-Sig) authentication in terms of system security was a sure way of solving a single failure point and ensuring a high level of security [289]. The problem, however, was that the Multi-Sig solution requires more ETHER (ETH) consumption. When a smart contract is deployed and executed, the Ethereum Blockchain system charges a small amount of ETH, known as "gas." Gas refers to the pricing value required to successfully conduct a transaction or execute a contract on the Ethereum Blockchain platform [290].

With Multi-Sig, a smart contract must call for the Multi-Sig function(s) to protect the data transfer whenever the features or methods of the smart contract interact with other smart contracts. As a result, Multi-Sig implementation is more secure but expensive to run for smart contracts. For these additional costs, 97 percent of the smart contracts running on the Ethereum Blockchain system as of November 2014 did not adopt Multi-Sig authentication and only needed single-key authentication due to cost reasons [291].

The Parity Technology resolved the cost issue by utilizing shared libraries [255]. The Parity Technology split the Multi-Sig Wallet into two contracts: (1) the

"*WalletLibrary*" contract that contains Multi-Sig functionalities in the library; and (2) the Wallet contract that calls functions in the library into use. In this case, if a smart contract imports the Multi-Sig functionality from a publicly accessible pre-deployed "*WalletLibrary*," no additional gas is needed for subsequent usage of the Multi-Sig authentication functionality [292].

```
contract WalletLibrary {

     address owner;

     // called by constructor
     function initWallet(address[] _owners, uint _required, uint _daylimit) {
          initDaylimit(_daylimit);
          initMultiowned(_owners, _required);
          .... [snip]

     }

     function changeOwner(address _new_owner) external {
         if (msg.sender == owner) {
             owner = _new_owner;
         }
          .... [snip]

     }

     function () payable {
          if (msg.value > 0)
             Deposit(msg.sender, msg.value);
           else if (msg.data.length > 0)
             _walletLibrary.delegatecall(msg.data);
             .... [snip]

     }

     function withdraw(uint amount) external returns (bool success) {
         if (msg.sender == owner) {
             return owner.send(amount);
         } else {
             return false;
         }
     }

}
```

Code 5.3 – Simplified WalletLibrary.sol

Above, Code 5.4 shows the "*WalletLibrary*" and "*Library*" contract [293]. The library provides a constructor with preset owner and common functionalities to initialize wallet objects and to modify information in the wallet. When performing important functions such as changing the owner, payment and withdrawal, the library can enforce strict authentication for a smart contract.

In Code 5.4 below, please note the heavy usage of "*delegatecall*" functions in the Wallet contract. The "*delegatecall*" function is designed to enable the use of corresponding functions called "forwarding of contracts," in the shared library of the "WalletLibrary" contract. This design is the most important factor that allows the Parity Multi-Sig Wallet to minimize gas consumption through multi-signature authentication on the Ethereum platform. [294]. With the workaround, a developer was able to reduce the transaction cost (gas) by up to 95 percent [295].

```
contract Wallet {

    address constant _walletLibrary;
    address owner;

    .... [snip]

    function Wallet(address _owner) {
        _walletLibrary = 0xa657491c1e7f16adb39b9b60e87bbb8d93988bc3;
        _walletLibrary.delegatecall(bytes4(sha3("initWallet(address)")), _owner);
    }

    function withdraw(uint amount) returns (bool success) {
        return _walletLibrary.delegatecall(bytes4(sha3("withdraw(uint)")), amount);
    }

    function () payable {
          if (msg.value > 0)
                Deposit(msg.sender, msg.value);
          else if (msg.data.length > 0)
                _walletLibrary.delegatecall(msg.data);
    }
    .... [snip]

}
```

Code 5.4 – Simplified Wallet.sol.

Step #4: Proximate chain of events

- On July 18, 2017, at 22:33 UTC, the attacker conducted the first exploitation against Edgeless Casino's Parity Multi-Sig Wallet and transferred 26,793 ETH to the attacker's wallet [296].

- On July 19, 2017, at 12:29 UTC, the attacker conducted the second exploitation against the Parity Multi-Sig Wallet of both Swarm City and Aeternity and transferred 44,055 ETH [297] and 82,189 ETH [298] to the attacker's wallet [299].

- On July 19, 2017, at 17:53 UTC, Gavin Wood, founder of Parity Technology, announced a critical security alert on the Gitter channel, including the loss of 150,000 ETH (about $30MM worth at the time) [300]. In the announcement, Parity Technology claimed that this exploitation only affected Parity Multi-Sig Wallet version 1.5 or above, and that the exploitation could be sufficiently remediated by patch. However, the Ethereum developer community confirmed that the patch plan could not stop the attack, and then started a special task force called the White Hat Group (WHG) to begin analysis of the cyberattack to try to stop the heist [301].

- On July 19, 2017, at 18:34 UTC, The WHG concluded that the cyberattack could be resumed at any time and that there was not enough time to address the security issue. Hence, to protect the remaining ETHs that had not yet been hacked, WHG moved all the ETHs in remaining Parity wallets (about $60MM worth at the time) to its wallet in the same way that the attacker had done [302]. Then, the WHG announced to all Parity Multi-Sig users: “If you hold a Multi-Sig contract that was drained, please be patient. We will be creating another Multi-Sig for you that has the same settings as your old Multi-Sig but with the vulnerability removed and we will return your funds to you there” [303].

- On July 20, 2017, The Parity Technology finally pushed the code patch for remediation of the exploit to Github [304].

- On July 20, 2017, the attacker realized that further theft was not possible and then began to move the stolen ETH to his or her wallets by a quantity of 10,000 ETHs [305].

- On July 24, 2017, the WHG conducted the process of repatriating the seized Ethers to affected users. However, the stolen $30 million ETH was determined to be irreparable [306].

Step #5: Analyzing the hacking incident

The attackers combined the two security issues for this successful exploitation. The first issue was related to a delegate function call within the “*payable*” function of the Wallet contract, as illustrated in Code 5.5 below. The “*payable*” function performs the transfer of Ether(s) in the transaction (*msg*) at lines 1 and 2. However, if the transaction does not contain any Ether but only data in the message payload at line 3, the Wallet contract forwards the function call to the “WalletLibrary” contract at line 4 [307]. Since all functions in the “WalletLibrary” needs to be called from the contract, they all need to be public. Hence, by utilizing the first issue, any smart contract interacting with the Wallet contract is able to call functions in the “WalletLibrary.”

```
contract Wallet {

      .... [snip]

    function () payable {
          if (msg.value > 0)                              // LINE 1
                Deposit(msg.sender, msg.value);           // LINE 2
          else if (msg.data.length > 0)                   // LINE 3
                _walletLibrary.delegatecall(msg.data);    // LINE 4
    }

      .... [snip]

}
```

Code 5.5 – Simplified Wallet.sol which was actually abused for the exploitation.

The second issue was related to the "*initWallet*" function of "WalletLibrary" contract. As seen in Code 5.6 below, the "*initWallet*" function sets the owner of the Wallet contract. The "*initWallet*" function is a constructor that is called upon only once at its creation. However, if the "*initWallet*" function is called by other smart contract interacting with the Wallet contract, the original owner can be modified. Hence, by utilizing the second issue, the Wallet contract can be under control of another user.

```
contract WalletLibrary {

      .... [snip]

     // called by constructor
     function initWallet(address[] _owners, uint _required, uint _daylimit) {         // LINE 5
          initDaylimit(_daylimit);                                                     // LINE 6
          initMultiowned(_owners, _required);                                          // LINE 7
          .... [snip]

     }

      .... [snip]

}
```

Code 5.6 – Simplified WalletLibrary.sol which was actually abused for the exploitation.

The attack itself consisted of two consecutive data transactions. The first data transaction calls up the "*initWallet*" function in the "*WalletLibrary*" contract and changes the owner of the contract to the attacker [308]. Then the second data transaction calls a fund transfer function to move Ethers to the attacker's address [309]. Clearly, the previous functionality within the Wallet contract is coded to identify the owner before execution. However, the attacker already changed the owner information and set himself or herself as the owner of the contract. Consequently, by combining the two issues, the attacker was able to call all public functions from the library and transfer all funds to his or her own address.

Step #6: Response to the exploitation and the remediation process

Due to the nature of decentralized systems, the Ethereum Blockchain system cannot have an organizational hierarchy to respond to cyberattacks already occurring. If such a cyberattack occurs in a centralized system, the system operator or administrator could respond quickly to minimize system damage in several ways, such as

terminating a user session, intervening in the application process, or even shutting down the system.

Fortunately, right after the security incident occurred, some members of the Ethereum Development community volunteered to form an incident response team, later called the White Hack Group (WHG). The team quickly analyzed the security vulnerabilities and then transferred all funds from the remaining vulnerable wallets to their own wallet, the same way the attacker had, to stop the cyberattack. The WHG held the transferred funds safely until Parity Technology pushed the remediation of the security issue to Github [310].

The saved funds were returned to each user at a later date, but ultimately the stolen funds could not be recovered. In the case of the *"TheDAO"* hack, the attacker was forced to wait for 34 days to transfer the stolen funds to his or her own account due to the proposal maturity period requirement. The latency brought the same system security effect as a system operation halt of a centralized system to the Ethereum Blockchain system. Hence, Ethereum developers were able to obtain enough time to safely lock down funds and to execute the fork (hard fork in this case) to restore the Blockchain to its pre-cyberattack state.

However, in the case of the first Parity Wallet hack, it was difficult to consider any type of fork execution because a huge number of active smart contracts were still using Parity wallets in the system environment and because no one could predict the side effects to the Ethereum system. In other words, despite massive stolen funds, the Ethereum developer community determined to not execute any type of fork since it was not realistic to restore the lost funds by exposing the system to additional risks. In conclusion, there was no return of lost funds, and funds were permanently lost [311].

Causal Analysis #3 – second Parity Wallet Hack

According to known facts, this cyber incident was not a case of an intruder hacking or exploiting the system. Nonetheless, this incident is reviewed in this series of analysis because the second Parity Wallet Hack shows how dangerous it is to run dApps on a Blockchain system which cannot have any type of authoritative entity that handles security controls and enforces compliance with security rules and regulations. As the nature of a distributed system, the Ethereum Blockchain system should have relied on the developer (Parity Technology) entirely for the remediation of the discovered security vulnerability (the first Parity Wallet hacking).

Step #1: System and hazard

The developer of Newbie solidity (the programming language used to create smart contract on the Ethereum system environment) developer, known as "devops199,"

unintentionally caused huge damage to the system by accidently triggering a yet-unknown vulnerability from the Parity 1.5 Client's Multi-Sig wallet. As a result, "devops199" destroyed all smart contracts using the Parity Multi-Sig Wallet and had $280 million worth of damage to the Ethereum Blockchain system. The primary hazard is that Ethereum allows execution of any smart contract within the system environment without system security operation hierarchy, such as security issue monitoring, security issue remediation and verification of security issue remediation.

Step #2: Security constraints and requirement

- The Ethereum Blockchain system must allow dApps to execute in the system environment without any censorship due to the principle of "Code is Law."
- Parity Multi-Sig Wallet solidity program must undergo in-depth secure source review with a trustworthy party to minimize the risk of cybersecurity incidents.
- The Parity Multi-Sig Wallet solidity program must remediate all known security issues with sufficient validation of the fix prior to deployment to the Ethereum Blockchain system.
- The Parity Multi-Sig Wallet solidity application development must create an incident response plan for malfunctions, incorrect operations or cyberattacks.
- The Parity Multi-Sig Wallet solidity application development must be proactive to resolve any encountered issue as soon as they occur.

Step #3: Security structure overview

Upon the occurrence of the first Parity Wallet Hack which was about 6 months prior to this incident, Parity Technology, who developed the Parity Wallet, promptly responded with a patch addressing the security vulnerability. The patch was implemented to remediate mainly two different locations in the "*WalletLibrary*" contract [312]. As shown in Code 5.7 below, one remediation was to set a limit on the ability to call the "initWallet" library function only for a wallet which was not initialized. This remediation prevents an attacker from resetting the wallet's critical primitive information such as the wallet address.

```
    216 +
214 217     // constructor - just pass on the owner array to the multiowned and
215 218     // the limit to daylimit
216         - function initWallet(address[] _owners, uint _required, uint _daylimit) {
    219     + function initWallet(address[] _owners, uint _required, uint _daylimit) only_uninitialized {
```

Code 5.7 – The code change can be seen in view of Github. Parity Wallet limits public accessibility of the "initWallet" function in "WalletLibrary".

The other remediation was to add a "*modifier*" attribute. The "*modifier*" will make sure certain conditions are met before the rest of the code in the contract can be executed. As seen in Code 5.8, the "*modifier*" attribute was added to the source code of the Parity Wallet and the value of the variable "*m_numOwners*" will be checked as a security logic condition during smart contract execution. For instance, if the smart contract has not already initialized, then the value of "*m_numOwners*" is less than 0 and rest of the code in the smart contract are allowed to be called and executed. If not, then the value of "*m_numOwners*" is greater than 0 and code execution is stopped immediately at that point [313].

```
214 + // throw unless the contract is not yet initialized.
215 + modifier only_uninitialized { if (m_numOwners > 0) throw; _; }
```

Code 5.8 - The code change can be seen in view of Github. Parity Wallet can now prevent previous exploitation by calling function "only_uninitialized" .

Step #4: Proximate chain of events [314] [315]

- On July 20, 2017, the day after the first hack, the "*WalletLibrary*" smart contract code was deployed with a security bug fix by Parity Technology.

- On August 3, 2017, a user named "*3esmit*" posted critical security vulnerability in the modified code showing that the "*initWallet*" function could be called even prior to "*WalletLibrary*" initiation. However, Parity Technology did not respond to the post and did not make any code fix to remediate the issue either [316].

- On Nov 6, 2017, at 14:33 UTC, a user "*devops199*" attempted to initialize the actual "*WalletLibrary*" by calling "*initWallet*" from his or her smart contract as an experiment (as he or she later explained). The correct usage of the "*WalletLibrary*" is that a smart contract instantiates "*WalletLibrary*" first and then invokes the necessary functions in the Parity Wallet to authenticate any data transitions performed within the smart contract. Due to the code flaw posted by user "3esmit" about 3 months ago, the initialization attempt was allowed and made the smart contract the actual owner of the "WalletLibrary" [317].

- On Nov 6, 2017, at 15:25 UTC, user "*devops199*" sent a "*kill*" function call to the "*WalletLibrary*." Since the user "*devops199*" was the owner of the actual "WalletLibrary," the request was executed and caused the self-destruction of the "WalletLibrary" [318]. As a result of the once unintended mistake of the function

call, all smart contracts using Parity Wallet could no longer use their wallets. In other words, all funds in Parity Wallet had been frozen and nobody was accessible.

- On Nov 6, 2017, at 15:54 UTC, user "*devops199*" realized the "*kill*" function call caused serious consequence and posted an issue (*#6995*) on Github – "anyone can kill your contract?" [319].

- On Nov 6, 2017, at 16:33 UTC, user "*devops199*" posted the same issue in the parity Gitter channel with a question, "is this serious issue?"

- On Nov 6, 2017, at 19:51 UTC, Parity Technologies became aware of the criticality of the issue and released a warning on Twitter, "we are investigating" [320].

- On November 15, 2017, Parity Technologies released the "postmortem" that 513K Ether (about $245 million) had been frozen due to security problems in its code and promising to do its best to return lost funds to its customers in the near future [321].

Step #5: Analyzing the hacking incident [322]

As explained in the causal analysis of the first Parity Wallet Hack, a fixed code was distributed on July 20, 2017, right after the incident. The fixed code did not allow for the modifying of the owner of a Wallet contract any longer. However, despite the prompt remediation, there were still more serious security issues in the code because the "*WalletLibrary*" itself could be initialized into an actual smart contract instance rather than just remaining in the library. In the case of Parity Wallet Multi-Sig, where all smart contracts refer to a single address in the "*WalletLibrary*" and cost savings can be achieved by the public functionality of the "*WalletLibrary*," the presence of this single point of failure had catastrophic results [323].

```
371
372     // FIELDS
373     address constant _walletLibrary = 0xcafecafecafecafecafecafecafecafecafecafe;
374
```

Code 5.9 – "Wallet" contract imports "WalletLibrary" as variable _walletLibrary from single address [324].

In the end, the inexperienced Ethereum developer "*devops199*" mistakenly instantiated "*WalletLibrary*" as an actual smart contract and took ownership of it by

calling the "*initWallet*" function. Then, the user accidentally destroyed the instantiated "WalletLibrary" by calling the "*kill*" method. As a result, Parity Multi-Sig Wallets of 587 smart contracts lost functionality and the wallet's 513,774 ETH were frozen [325].

At the time of the patch update to remediate the first Parity Wallet Hack, Parity Technology claimed that code changes were verified and reviewed. However, it was later confirmed that the code changes were completed within one day. In the context of a typical security remediation process, it is very rare to complete the entire security fix in one day, such as causal analysis, patch development, code validation and deployment. After the incident, Parity Technology stated the code was only reviewed by the its internal developer but never audited by any independent third party who is specialized in secure solidity programming [326].

In addition, a user named "*3esmit*" posted the vulnerability to the public forum and warned of the potential security issue before the incident occurred. However, due to the nature of the decentralized system, no one is responsible for system security monitoring or updates so the post was simply ignored. According to the code change history record in the Github source code repository, neither the Parity Technology developer nor the Ethereum developer community had made any code change at all since the first Parity Wallet hack was patched.

Step #6: Response to the exploitation and the remediation process

In May 2018, "Ethereum Improvement Proposal 999 (EIP-999)" was proposed. The proposal included a code fix and hard fork planning [327]. However, as soon as this proposal was announced, many Ethereum developers in the community had a heated debate as to whether constantly implementing a hard fork on the system was the right thing to do. Many community members believed that a hard fork violates the "Code is Law" principle, which is one of the most important values of Ethereum: "No one has the right to censor the execution of code on the ETC Blockchain" [328]. They claimed that it is not ideal to perform the fork solution to return the lost funds from cyberattacks every time, and that another fork into two different Blockchains would fracture the network and the community. A vote was implemented in July 2018, with 39.4 percent agreeing to change, but 55 percent voted against it [329]. The proposal remained controversial for more than 6 months after the incident when this analysis was under way.

5.3 Bitfinex cryptocurrency exchange heists

Bitfinex (Bitfinex) is a cryptocurrency trading platform that started in Hong Kong in 2012 [330]. By early 2010, cryptocurrency transactions were settled off-Blockchain and were still managed

by a central database. Bitfinex was the first cryptocurrency exchange to offer on-Blockchain transactions, which made cryptocurrency trade more transparent so that users could check their segregated wallet in real-time [331]. With such an innovative system implementation change for Blockchain, Bitfinex became one of the most popular global cryptocurrency exchanges in a very short period of time.

From 2015 to 2016, Bitfinex suffered two cyberattacks. The first exploitation occurred in May 2015, when 1,500 BTC were stolen from its hot storage. The second exploitation occurred in August 2016, when roughly 120,000 BTC, which was worth $72MM at the time, were again stolen from its hot storage. The loss was recorded as the second largest heist in the history of Blockchain system hacking, with $20 million more than *"TheDAO"* hack [332].

Step #1: Intrusion and hazard

An unknown attacker circumvented Bitfinex's multi-signature authentication provided by a third-party company, Bitgo. In this exploitation, the attacker was able to remove the guard from Bitgo's authentication mechanism and transfer funds from the hot storage of Bitfinex to the attacker's own address.

There were two hazards in this incident. First, when making system components and configuration changes for regulation compliance, Bitfinex did not securely realign system components, making the system vulnerable to cyberattack. Second, due to the heavy reliance on a third-party (Bitgo) security solution, Bitfinex was not able to respond promptly and react properly to this cyber incident.

Step #2: Security constraints and requirement [333]

- Bitgo's segregated Multi-Sig implementation in Bitfinex must enforce security policy before co-signing any user transaction.
- Bitgo's segregated Multi-Sig implementation in Bitfinex must protect unauthorized funds transfer requests to the cryptocurrency Blockchain system.
- Bitgo's segregated Multi-Sig implementation in Bitfinex must coordinate with Bitgo and multiple owners to mitigate the risk of stolen private keys.
- Bitfinex and Bitgo must communicate and interact with each other to minimize the security risk.

Step #3: System security structure overview

In May 2015, Bitfinex lost approximately 1,500 BTC (bitcoin) from customers' hot wallets due to cyberattack. Since then, Bitfinex has not disclosed technical details, but the

cause is known to be the usage of unsecured hot and cold proprietary wallets [334]. After the cyber incident, Bitfinex decided to implement an additional layer of security system components with BitGo, which provides a multi-signature wallet solution to prevent cyberattacks.

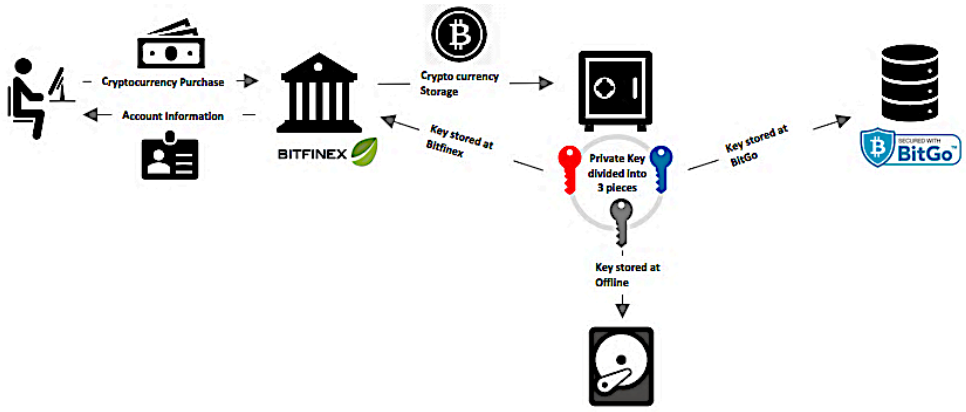


Figure 5. 7 – BitGo generates private key and breaks the private key into 3 pieces. 1st piece is stored in Bitfinex, and 2nd piece is stored at Bitgo, and 3rd piece is stored at offline storage [335].

Typically, in a Blockchain system a user is identified based on two strong cryptographic strings: one is a "public key" and the other is a "private key." The private key is used for authentication and authorization to make a transition, while the public key is used for retrieving transition information. The end user must handle the private key securely, otherwise risk losing ownership of the associated assets in a cryptocurrency Blockchain system.

As illustrated in Figure 5.7 above, unlike private and public key authentication, BitGo's Multi-Sig authentication breaks the private key into three pieces and stores each in different locations [336]. As part of implementation of BitGo's safety control, Bitfinex holds one key in the user's hot wallet and stores the other key in an offline cold wallet. Then, BitGo holds the third key as a means of verifying the user's authorization as well as enforcing spending limits. As illustrated in Figure 5.8 below, to sign off on a data transaction, a user should provide 2 out of 3 pieces of the private key. One key is going to be provided from either the user's offline key storage or from Bitfinex through login. The other key is going to be provided from BitGo through separate login [337].

About a year later, the U.S. Commodity Futures Trading Commission (CFTC) conducted an audit on Bitfinex and fined them $75,000 for illegal off-exchange financial transactions in June 2016 [338]. To resolve the audit findings, Bitfinex had to make modifications on its conservative cryptocurrency hot and cold storage implementation. Previously, Bitfinex allowed only a small portion of the current cryptocurrency to remain

in the hot storage device for security reasons. However, Bitfinex had to move a significant portion of its cryptocurrency to hot storage for regulatory compliance.

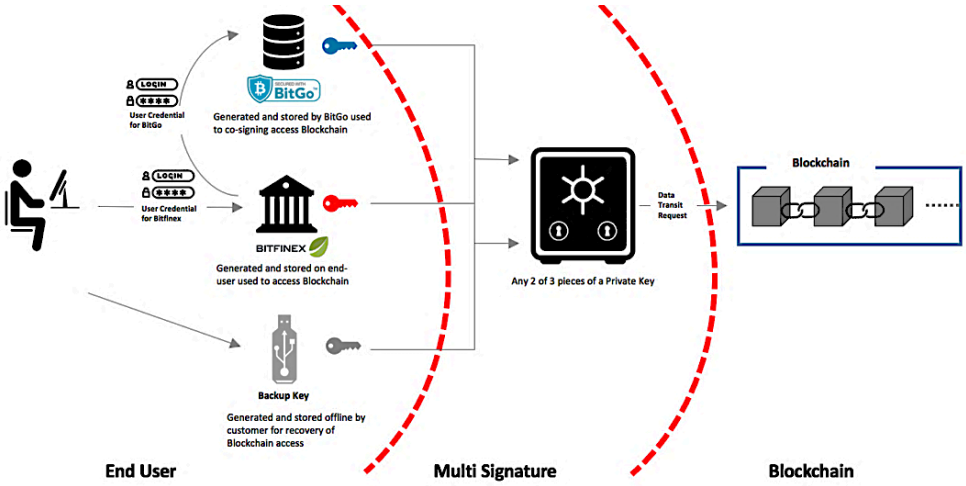


Figure 5. 8 – The BitGo's Multi-Sig solution requires a user at least 2 out of 3 pieces of private key to authorize data transaction. In this implementation of Bitfinex and BitGo, to complete data transaction, a user should provide two pieces of the private key. One key is going to be provided from either user's offline key storage or from Bitfinex through login. The other key is going to be provided from BitGo through separate login [339].

Step #4: Proximate chain of events [340]

- On May 22, 2015, at 05:00 UTC, Bitfinex announced that some hot wallets were compromised and that their funds were stolen [341].

- On July 04, 2015, Bitfinex and Bitgo partnered to create the world's first real-time proof of reserve Bitcoin Exchange by providing individual wallets with Multi-Sig authentication for each customer [342].

- On Sept 18, 2015, the CFTC announced that cryptocurrency is classed as a commodity in the U.S [343].

- On June 02, 2016, the CFTC and Bitfinex settled a fine of $75,000 for illegal off-exchange financial transactions [344].

- On August 02, 2016, at 12:18 UTC, a theft took place.

- On August 02, 2016, at 18:06:28 UTC, Zane Tackett, Director of Community & Product Development at Bitfinex announced on Reddit.com that they "discovered a

security breach that requires to halt all trading on Bitfinex, as well as halt all digital token deposits to and withdrawals from Bitfinex" [345].

- On August 02, 2016, at 20:40:37 UTC, an anonymous Reddit account known as "blahbitcoinredditor" posted P2SH usage statistics related to Bitgo's Multi-Sig authentication process in Bitgo as proof of the occurrence of a cyberattack. The post also indicated that the loss could be over 100,000 BTC, which was worth about $600MM at the time. From that point, the public started to realize that the security breach was related to either an exploitation or circumvention of Bitgo's Multi-Sig authentication [346].

- On August 06, 2016, at 15:51 UTC, Bitfinex posted an interim update announcing that customers would end up losing 119,756 BTC, which was about 36.067 percent of Bitfinex's entire funds [347].

- On August 10, 2016, at 14:01 UTC, Bitfinex announced that the security fix was made successfully on its trading platform and the cryptocurrency trading would resume [348].

Step #5: Analyzing the hacking incident

Figure 5.9 illustrates how an attacker was able to exploit Bitfinex with bypassing the third-party Multi-Sig authentication provided by Bitgo. As a first step, an attacker could break into the Bitfinex trading platform and acquire one piece of a private key for the victims. Since Bitfinex has not yet disclosed its technical details, the way the hacker(s) was able to penetrate the system is not yet known. However, due to the strong security authentication of the Multi-Sig, possessing only one piece of the private keys was not sufficient to obtain BitGo's sign off to commit the data transaction. Although Bitfinex has not disclosed the exact details, the attacker was able to gain access to the source code of Bitfinex somehow and obtain the information for invoking a remote call directly to BitGo's authentication server to sign off on any transaction requests.

Bitgo provides the remote function call capability as form of public library API to its customers. The IT administrator and/or application developer utilizes this functionality with a provided secret Token Key (for authentication) mainly for testing purposes. Hence, as a security best-practice guideline, the final code version should not contain any information of this API Library and the Token Key value. However, this information remained in the source code, so the attacker with only one key was able to obtain the sign-off by simply calling BitGo's public library functions [349]. Figure 5.6 below illustrates how the attacker was able to perform a cryptocurrency transaction on Blockchain without fulfilling the requirement of providing two out of three keys. Due to

this serious security vulnerability, 119,756 Bitcoins were transferred to the attacker's wallets with sign-off from Bitgo [350].

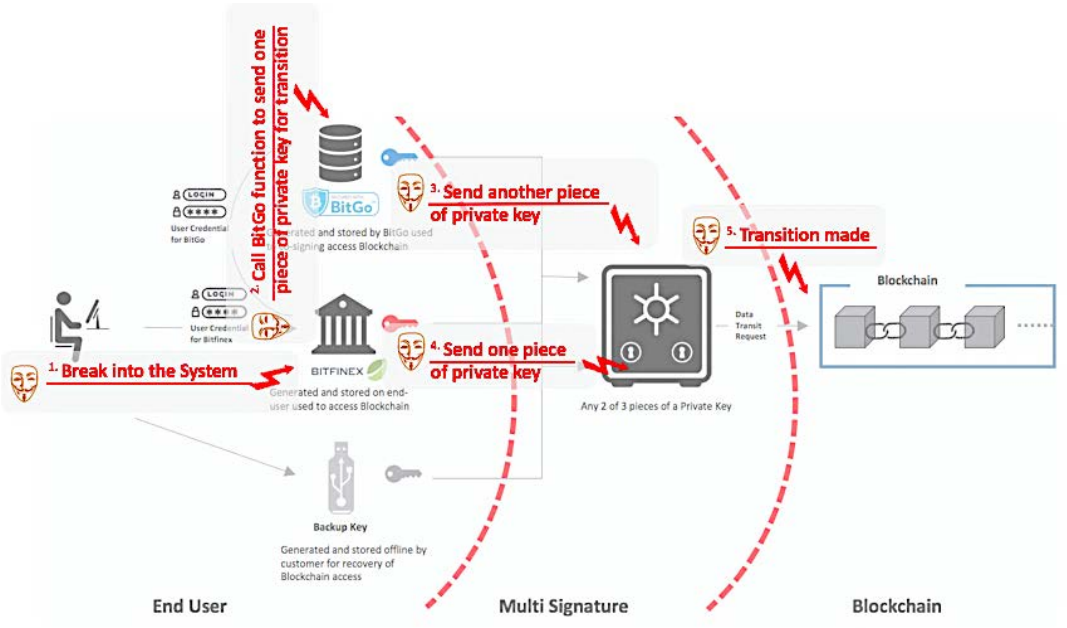


Figure 5. 9 – Brief illustration of how attacker was able to exploit Bitfinex with bypassing the 3rd party multi-sig authentication provided by Bitgo [351].

At first glance, Bitfinex seems to deserve all the criticism about this cyberattack. However, this heist case was actually caused by the intricate entanglement of three parties: (1) Bitfinex who did not securely implement Bitgo's integration and did not conduct a follow-up security review of system changes, (2) Bitgo who failed to verify the insecure implementation and to signal an alarm for an abnormal transaction request, and (3) the CFTC who ordered the system change causing the exploitation.

If BitGo did not adequately communicate with Bitfinex about general security concerns of the integration of BitGo's Multi-Sig safety control or if BitGo did not securely control the remote API method call provided to Bitfinex, then BitGo should also be responsible for selling a false sense of security to the customer. [352]. Also known later, Bitfinex had set alarm on Bitgo server to receive alert notifications when a large number of transactions occur in short period time to minimize the loss of Cyberattacks, but the alarms did not work properly for unknown reason [353].

Apart from all the above causes, many IT security professionals have pointed out that the CFTC was also partially responsible for this heist since the loss due to the cyberattack could have been much smaller if Bitfinex had continued to retain most of its cryptocurrency in segregated cold storage [354].

Step #6: Response to the exploitation and the remediation process

Right after the heist, Bitfinex announced its immediate suspension of the BitGo segregated multi-signature wallet solution. According to a post from Reddit.com, Bitfinex hired Ledger Labs, a private Blockchain security service provider, to conduct a security review, and they discovered vulnerabilities in the system. With assistance and recommendations from the security assessment, Bitfinex was able to remediate the two main causes of the heist: (1) the possibility of remotely invoking BitGo's public library functions and (2) bypassing the alert system for a large fund transition. Bitfinex also announced their plan to re-implement the Multi-Sig procedure and to establish more secure cryptocurrency storage options [355].

5.4 Identified security weakness from causal analysis

As the seventh step of the proposed causal framework of Table 5.1, this section describes major weaknesses contributing to continuous Blockchain system hacking from the previous series of analysis.

System Security Dependency

Most security controls in the Blockchain system heavily depend on inherent security features of Blockchain technology as described in Table 5.2 below. Hence, Blockchain system has been secured only within the area of user authentication and authorization, such as the integration of third-party Multi-Sig (ex. Parity Wallet or Bitgo). From the aspect of "single point of failure," such security improvements within a limited system area would not help to improve overall system security at all. For example, as shown in the series of causal analysis in the previous sections, the only target of all cyberattacks (except for the second Parity Hack) was the user-authentication mechanism. After disabling or bypassing authentication protection, there was no system security component (including Blockchain's inherent security features) to stop the cyberattacks.

Blockchain Safety Feature	Brief Description
Integrity & Immutability	Data record and transit cannot be changed. Write once and then read only. This safety feature prevent any malicious attempt altering data.
Transparency	User (node) operation are all viewable, searchable and traceable to public. This safety feature allows monitoring any suspicious activity to public.

Blockchain Safety Feature	Brief Description
Encryption	Strong cryptographic public and private key access protect from un-authorized usage of the system.
Reliability & Fault Tolerance	As characteristic of decentralized architecture, Blockchain system never stops and ending with fail-safe operation.

Table 5. 2 - Security features inherited from Blockchain technology.

Transparency and Openness

In previous chapters, it was identified that the Blockchain system should disclose information about the operation of Blockchain for autonomous reasons. However, in this chapter it was found that Blockchain systems were disclosing other system information as well, such as a Blockchain's software development process, Blockchain's security issues, and even real-time security incident response actions of the Blockchain system.

In the case of *"TheDAO"* hacking, the security issue was posted to public forums several months before the incident, along with the actual attack scenarios. While the Slock.it developer and the Ethereum developer community were wasted months debating about the patch development, the attacker was collecting vulnerability information and was able to plan attacks accordingly.

Moreover, the attacker was able to control the pace of cyberattacks based on discussions among the Ethereum developer community which were posted in open forums. As shown in Step #4 (Proximate Events Chain), the cyberattacks repeated "stop and continue" actions multiple times throughout the entire process of the cyberattack. Many IT professionals believe that the attacker took such actions since he or she was able to read the posts and obtain information about Ethereum's incident response status and plans. If the system had decided to make a hard fork, the attacker would have had no way to cash out the drained Ethers [356].

The same was true for the first Parity Multi-Sig Wallet Hack case. It was noted that the attacker suddenly started moving the stolen Ethers around from one account to others in the middle of the cyberattack. Initially, many people were wondering about this behavior in the sense that if the attack had been continuous, the attacker could drain and steal more Ethers. It became clear through later investigation that the attacker had started the action immediately after posting the WHG incident response on the public forum. Even in the case of the Bitfinex heist, the cyberattack was able to target only high-balance remaining accounts since all data transition (cryptocurrency transfer, in this case) were transparently open to the public.

Lack of Vulnerability Assessment and Security Review

It was identified that applications running on top of or operating with Blockchain were deployed into production without proper or sufficient security assessment and review. Nowadays, common knowledge in the IT industry says it is impossible to develop code without a single security bug or to change system components without a single security problem. This is why multiple-peer and third-party security review processes have always been considered as mandatory in SDLC (Software Development Life Cycle) and in system operation guidelines. In this sense, it is quite a shock to note that many Blockchain systems have not performed periodic security reviews such as automatic security checks, internal penetration checks, and independent security audits on a regular basis. [357].

Moreover, applications running on the blockchain are in a very different situation from applications running on a centralized system, which can stop operations as soon as problems arise and resume operations after the problem is resolved. Immutability is one of the major security features inherited from Blockchain, as mentioned previously. However, when applied to distributed applications, it becomes a serious weakness that prevents or makes it difficult to do software security processes such as security bug fixes and security upgrades. Therefore, distributed applications running on Blockchain systems should be more secure than applications running on other centralized systems or even near perfect for security [358].

At the time of these security incidents, both Slock.it and Parity Technology claimed that multiple security reviews were performed before the codes were deployed to production. In case of "*TheDAO*" hack, it was revealed later that all peers were from internal development teams. In case of the first Parity Wallet Hacking, it was also revealed later that the vulnerable part of the source code was not even in the scope of their security audits [359] and completely different codes were deployed which had never been under any type of security review [360]. In the case of the Bitfinex hacking, Bitfinex hired a security service after the cyber incident, and they found a lot more security vulnerabilities in the system.

Absence of Management and Monitoring

It was identified that the significant problem lies in the fact that no dedicated party or group manages security control in a decentralized system, even if unsecured implementation and programming were confirmed as the main cause of all the exploitations described above. It is clear that the loss from cyberattacks would have been reduced if proper security management and effective incident response were available.

In the case of "*TheDAO*" hacking, several warnings and alerts about potential threats were posted to the public forum for over a month, but the vulnerable code was still running in the production environment during that period. In addition, there was no

response for 36 hours after the attack occurred. Even though the attack was abruptly stopped, it was not from the system's forced control, but from the hacker himself [361].

On the other hand, at the time of the hack event, developers of MakerDAO, a similar smart contract to "*TheDAO*," confirmed the same vulnerability existed in their own smart contracts, then hacked their smart contracts with the same exploitation technique to transfer all funds to a safe Multi-Sig wallet. Hence, MakerDAO could have avoided the hack because the application developers did play the same role as the system manager or controller in a centralized system [362].

After the heists, Slock.it announced they would build a security team and hire dedicated monitoring personnel for system-wide detection and alert. Bitfinex also decided to empower its internal security team to conduct real-time monitoring.

Decision Hierarchy in Non-Hierarchical (Decentralized) System

From its inception, Blockchain was presented as a decentralized platform for "applications that run exactly as programmed without any chance of fraud, censorship, or third-party interference" [363]. Due to the nature of such, the system cannot have decision hierarchy. In Blockchain, the software that runs on the protocol is written by developers, however, its acceptance is determined by miners and users running it themselves. Hence, it is structured as a democratic "tricameral" system among the three different constituencies (developers, miners and users), and all changes to the Blockchain needs participation by all three constituencies to be implemented.

However, as can be seen from a series of causal analysis in Section 5.2, a security decision hierarchy actually exists in the Ethereum Blockchain system, even though it is not explicit or authoritative, as is the case with centralized systems. The Ethereum developer community, which consists of groups of people, institutions, companies and other organizations for support and maintenance, had been literally acting as a central authority to respond to the security incidents and make decisions for system security matters.

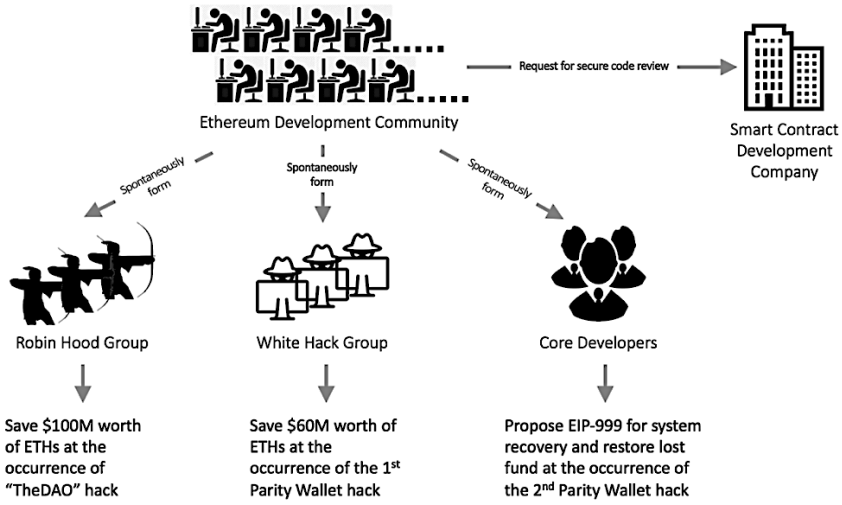


Figure 5. 10 - Ethereum has a form of security decision hierarchy as centralized system. Ethereum development community have been playing like central authority at occurrence of cyber incident.

The Figure 1.1 above illustrates how the Ethereum developer community has gotten involved in the three cyber incidents *("TheDAO"* hack, first Parity Wallet hack, and second Parity Wallet Hack) and communicated with the dApps development vendors to request an independent security assessment. As shown, people from the community spontaneously formed a special task force, such as "Robin Hood Group" or "White Hat Group," to fight back against the exploitation and theft. Also, core developers from the community volunteered to set up a recovery and improvement plan. Moreover, the Ethereum developer community also drove smart contract development companies to have independent security reviews to minimize security risk and vulnerability.

Even if the immediate responses of the Ethereum development community reduced system damage from hacking, as a result, the actions brought a structure of governance processes to Ethereum, which raised multiple concerns and problems. First, no matter how good the intention was, decision making by a person or a group of people basically violates Ethereum's code of principle, which declares decentralization, censorship resistance, and a permission-free environment. Hence, when the Ethereum developer community proposed a fork solution for the first time to restore lost funds due to *"TheDAO"* hack, a number of users worried that the change would ruin integrity of the system and warned about false signals that projects like *"TheDAO"* can influence the immutability of the decentralized system for their own benefits. In fact, after the proposal was announced, the Ethereum developer community was flooded with an enormous number of fork requests to recover the lost ETHs. Furthermore, the *"TheDAO"* attacker sent an open letter to the community claiming his compensation (stolen ETHs) was legal based on the premise of smart contracts and threatened to take legal action against any attempt to invalidate his work (by implementing a fork) [364].

Second, this voluntary participation can lead to a rather opaque and unreasonable centralized decision-making structure without supervision and balance. For example, during *"TheDAO"* hack, most of incident response status and system change decisions made by the Ethereum development community were shared within the community. Although the information later spread across online blog posts and email subscriptions, it seemed insufficient and inappropriate for users and miners in a decentralized system. The process of forming the special task forces was also not transparent at all. No entitlement to participate in the Task Force was explicitly stated, and no one other than the community have ever reviewed or approved the decisions made during the incident response (such as bolstering security by removing ETH from the weak wallet during the first Parity Wallet hack). Hence, many IT specialists expressed great concern about such strong influence of the Ethereum development community and Vitalik Buterine, the founder of Ethereum and core member of the community [365]. In practice, it is good to follow recommendations of such experienced professionals in the technology, however the process then should be more transparent and structured for review and monitoring. For example, at the time of the second Parity Wallet security incident, the Ethereum development community did not explicitly state the reason for missing the vulnerability during the secure code review of the first Parity Wallet hack. There was no information as to who performed the review and who was responsible for the review. Until this writing, no one knows who wrote the review or who was responsible for it.

Third, empowering this informal system hierarchy is difficult. This is how the fork occurred at the time of the *"TheDAO"* hack and why the two Blockchain systems (Ethereum and Ethereum Classic) co-exist. Ethereum community developers were in favor of a hard fork in order to return stolen funds. However, a minority of miners rejected the controversial idea of changing immutable transactions and continued mining the old Blockchain. If a portion of the miners and users agree with a software upgrade, but another portion of the miners and users do not agree, then two different versions of Blockchain with the same root are going co-exist. This divided Ethereum into two co-existing Blockchains: the new one, Ethereum (ETH), and the old one, Ethereum Classic (ETC) [366]. In addition, at the time of the first Parity Wallet hack, core developers requested an independent security review for the issue remediation patch. At that time, Parity Technology and the Parity Wallet dApps development company confirmed the third-party security review was conducted. However, at the time of second Parity Wallet security incident, Parity Technology said it had never done a third-party security review for the remediation patch [367].

CHAPTER 6 – Security Remediation Approach of Blockchain System

"Security is better when it is built in, not bolted on."

— Stephen Yu
(Executive VP of Infoblox)

6.1 The myth of Blockchain system security

Blockchain is Never Changed as Immutability

As described in Chapter 5, despite Blockchain's being known as immutable, the soft or hard fork was able to make changes to the Blockchain network as recovery methods for cyberattacks. In standard software industry parlance, the term *fork* means a "copy of an existing project." However, in Blockchain, *fork* means an existing Blockchain is to be split into two separate chains. Although the fork was explained in detail in Chapter 5, Table 6.1 below summarizes them once again from the aspect of compatibility.

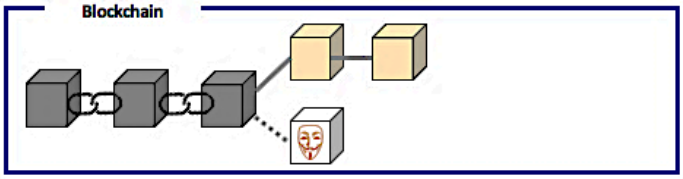
Type of Fork	Compatibility
Soft	Soft fork is compatible software upgrade on Blockchain network that is backwards compatible with older versions. In soft fork, nodes (users) can still participate in Blockchain network without software upgrade, such as data transaction validation and verification. However, soft fork will result in invalidating previously valid blocks, and might cause security risks for non-upgrading nodes.
Hard	Hard fork is in-compatible software upgrade on Blockchain network that is not compatible with older versions. In hard fork, nodes (users) should upgrade to the software to continue participate in Blockchain network. This separation results in a permanent divergence of the Blockchain network. In other words, two Blockchain network will concurrently exist. Hard fork on Blockchain network makes previously invalid blocks valid, and the non-upgrading nodes become incompatible.

Table 6. 1 – Different types of forks in terms of compatibility [368].

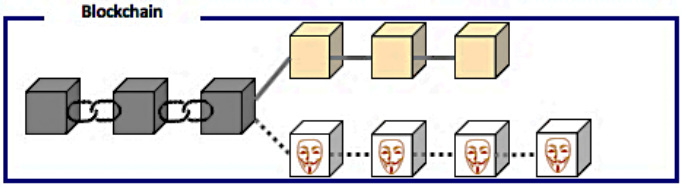
The attack, known as the "51% attack," was designed to take advantage of the fork's technological possibilities in Blockchain: Blockchain data can be altered if one of the attacker groups can achieve 51% of the computer or computing performance of the

entire Blockchain system's nodes. Below, Figure 6.2 illustrates how the "51% attack" is executed and how it makes existing data changes in Blockchain.

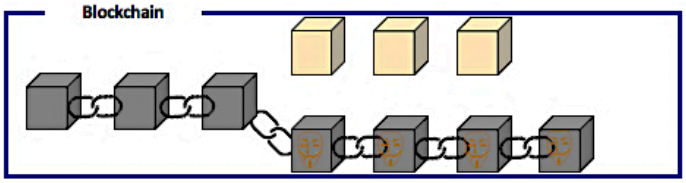
Step 1 shows that while the chain is growing by adding new blocks, multiple branches are created containing conflicting information before determining which branch will be added to the existing chain. Blockchain has a decision policy of selecting the longest branch. The longest branch becomes the main one and adds to the Blockchain, but shorter ones go back to the pool of unconfirmed transactions [369]. Step 2 shows that by abusing the longest chain selection policy, malicious attackers can alter or change data in the system if they can generate blocks faster than the rest of the network. Finally, Step 3 shows attackers can simply persevere with their private fork until it becomes longer than the branch built by the honest network, then publish the altered branch to be accepted as valid one.



1. Honest nodes continue extending the valid chain by putting yellow colored blocks, while the attacker secretly starts mining a fraudulent branch with white colored block(s).



2. The attacker succeeds in making the fraudulent branch longer than the honest one.



3. The attacker's branch is published and is now considered the valid one.

Figure 6. 1 – Simple illustration of 51% attack.

This exploitation technique has been considered for years as only a theory since it would require an attacker to take control of a large number of computers in the network (51% of the entire Blockchain network). However, in June 2017, a Bitcoin Blockchain system announced that 70 percent of all hash rates of its Blockchain network came from

just four Chinese mining pools: F2Pool, Bitmain's AntPool, BTCC Pool and BW.com [370]. This means that the 51% attack becomes literally possible if a couple of major mining pools in the Bitcoin Blockchain system combine their computing power. In 2018, the theoretical threat became real. The Verge, a cryptocurrency exchange, reported that it had experienced three different 51% attacks within the first two quarters of 2018 [371]. In May 2018, Bitcoin Gold (BTG) also announced that it fell victim to the 51% attack and lost $18MM [372].

In June 2018, the website crypto51.app was launched to provide a theoretical estimation in terms of hourly costs of launching a 51% attack against each cryptocurrency [373]. The estimation was calculated mainly based on network hash rates and hashing algorithm of the PoW (Proof-of-Work) for each cryptocurrency Blockchain system. Based on this estimation, launching a 51% attack against Bytecoin, which is one of the top 20 cryptocurrency systems, only costs approximately $167 per hour, as of August 25, 2018.

Furthermore, an attacker can also achieve 51% of attacks with less than 50% of the total system hash power. Of course, the likelihood of success is less than 100% but not 100% failure. Therefore, depending on the situation of the system, a 51% attack can still manipulate data in Blockchain with only a 30-40 percent, or even less, hash power of the entire system environment.

Blockchain Secures User Anonymity

Within a Blockchain system environment, each node (user) will have a unique address that is generated by crypto algorithm. Each node can use the cryptographic value (the public key) to maintain anonymity. The Blockchain algorithm that generates public and private key pairs has proven to be impossible to crack. This anonymity guarantees not only intractability of data transition but also privacy of end users in the Blockchain system.

What should be noted here is that similar levels of user information anonymity are also being used in the current banking industry and stock exchange systems based on a centralized system. Examples of end-user information includes the timestamp of wire transfers, amount of transactions, counterparties to transactions, and account numbers. In that sense, the anonymity of the Blockchain system is nothing new or special from a security perspective, and it should not be considered as a superior endpoint safety control over an existing centralized system [374].

Therefore, it would be a more accurate statement that the Blockchain system provides pseudonymity rather than anonymity. Pseudonymity is a method that is used to obfuscate the actual identity of a person or group [375]. On the other hand, maintaining complete anonymity means that there is, in fact, no way to track the identity of an individual or group. A node (user) in Blockchain systems still needs to provide full or

partial self-identity information to interact outside of the system, such as when a user registers in a cryptocurrency exchange, when a user sends or receives cryptocurrency through an online wallet, or when the cryptocurrency is cashed in or out for purchase or sale. Given this, it would be more appropriate to conclude that a Blockchain system does not provide true anonymity but rather distributes user identifications to the system network in a secure way.

Figure 6.2 illustrates recent research from Princeton University which supports the above conclusion. The research found that 53 out of 130 web merchants which accept cryptocurrency have routinely leaked end users' identifiable data in the form of a cookie (also known as a session ID) [376]. The cookie is usually set on a client web browser by a web application to maintain a user session or to track user activity. The researcher found out that an end user might be tracked or disclosed by using the information inside those cookies. As shown in the Figure, cookies contain various information about the user's purchases, such as the amount spent, time of purchase and name of the user. Since Blockchain systems disclose entire records of data transitions to the public, the information inside cookies might be used to link with data transition records in Blockchain to discover the identity of the node.

This fact can also be interpreted that the Blockchain system defers responsibility of system security to the end user(s), since it does not have a central security authority that can be held to such responsibility.

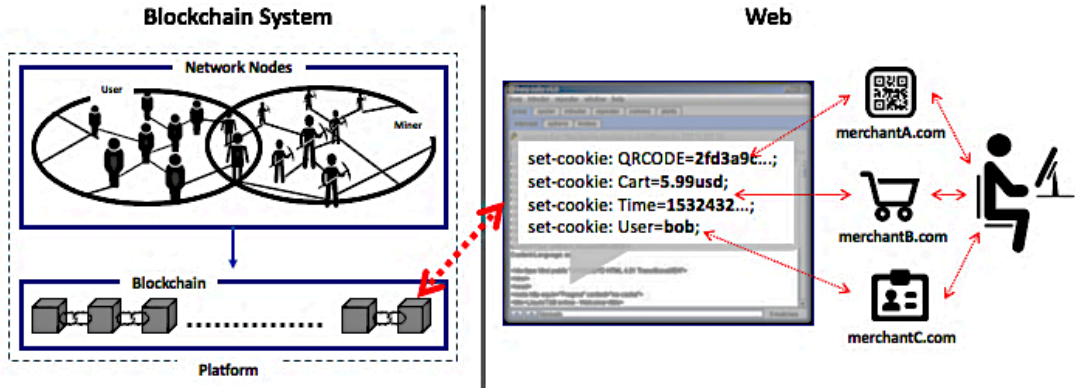


Figure 6. 2 – Purchase information within Session ID or Cookies may be abused to link them with transaction in Blockchain [377].

Blockchain Protects the System via Transparency

The most common misconception about Blockchain security is probably its transparency and traceability. By using public ledger techniques, data in the Blockchain is copied and shared within all nodes of the system network. All data transit information is

transparently open to and traceable by anyone in the public. Such transparency and traceability of Blockchain has been considered as a strong defense against cyberattacks.

In fact, Blockchain can only processes data that does not need to be secure. In other words, data in the Blockchain system is not sensitive and does not need to be protected at all. For example, a cryptocurrency Blockchain system transparently discloses data transit information, such as sender, recipients, transaction amounts and time stamps. The personal bank checks we use in our daily lives also include similar information such as bank routing number, sender's account number, amount of funds to transfer and recipient information. Personal bank checks are freely transferable to others, but for decades they have been used as a secure payment method without fear of personal information leakage.

In this sense, the application of Blockchain technology is limited to systems that contain data that does not need to be protected. For example, Blockchain technology cannot be used to process bid data for active auctions because the data must be unopened until the end of the auction. Hence, it is an incorrect statement that the transparency and traceability of Blockchain safely protects its data.

Moreover, the transparency and the traceability of Blockchain often causes its system to be in more danger in the event of a cyberattack. As shown in previous causal analysis in Chapter 5, attackers were able to target the cyberattack on accounts holding large amount of funds since such information is available and accessible to the public. Table 6.2 below describes the adverse effects caused by transparency and traceability in terms of system security.

	Adversary effects caused by Blockchain's transparency and traceability
Data & Information	Users' (nodes') activities are all viewable, searchable and traceable to public. Hence, attackers can gather information about target (account in case of crypto currency system) without spending much effort.
Architecture & Design	As nature of distributed system, most of Blockchain is open source. System design, architecture and even source code are accessible to public. As shown in causal analysis in chapter 5, attackers were able to exploit known and unknown security flaw in the code.
Operation & Management	Since there is no central authority and governance party, all of communications are occurred at public channel, such as SNS, public form, company web site etc. Hence, all of operation and management activities such as status, update, schedule etc are open to public.

Table 6. 2 – Threats of System Safety due to Transparency in Public Blockchain System.

Blockchain is Hard to Hack or Hack-Proof

Any technology has security weak points and, unfortunately, Blockchain is no exception. As briefly mentioned in Chapter 4, Blockchain is not immune to cyberattacks at all. The

notion of security in Blockchain was found only within a limited system area and within restricted conditions. Furthermore, throughout multiple causal analysis in Chapter 5, it was also discovered that the advantages of this technology (immutability, anonymity, transparency and integrity) ironically became rather a hinderance when responding to a cyberattack.

Figure 6.3 below shows the difference between Blockchain and a centralized system from the aspect of system hacking. In a centralized banking system shown on the right side of Figure 6.3, an attacker must complete several different exploitation steps to obtain financial gain. Also, all the steps should be accomplished as soon as possible. Otherwise, the system can detect the exploitation through intrusion detection or security monitoring to recover the loss and restore the system state immediately. In addition, the attacker has to make a lot of effort to hide his or her identity to avoid discovery.

In the Blockchain system shown on the left side of Figure 6.3, the exploitation step is fairly simple. Once an attacker steals user credentials or bypasses system authentication, he or she can just start transferring funds from the victim's account to his own account at any moment without any concern about detection. The integrity of Blockchain prevents the system from stopping the cyberattack even if it is aware of the attack, and the anonymity of Blockchain lets the attacker keep his or her identity hidden. Then, the attacker has enough time to cash out the stolen cryptocurrency since the immutability of Blockchain prevents any system changes to restore the stolen funds.

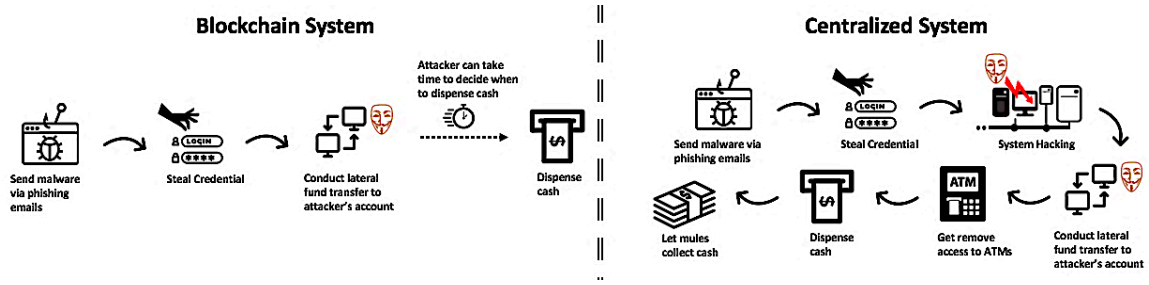


Figure 6. 3 – Typical carry out of network-based ATM malware attack between Blockchain vs. Centralized system [378].

6.2 Difficulties in Blockchain system security

Infinite Running Machine

In an existing centralized system, a contingency plan can minimize damage from cyberattack by disabling parts or even the entire system until issues are fixed or resolved. However, a Blockchain system cannot offer such an option. As explained in Chapter 2, the Blockchain technology was developed as a concept of DAO which operates the

system infinitely and autonomously. This characteristic of the Blockchain system makes it extremely difficult or even impossible to take effective remediation actions in response to security incidents, since the resolution should be applied while the system is operating.

Complexity & Size of System Boundary Increase

As described above, a Blockchain network grows very rapidly, literally without limitation in terms of nodes (users). Such system boundary expansion causes increasing complexity and ambiguity, making it very difficult for developers to understand the system architecture and implement system security controls prior to deployment [330]. These factors make it extremely hard to anticipate any type of emergency during its operation, and also make it very complicated to plan out incident response upon the occurrence of cyberattacks.

Centralization of System Controls

It is widely believed that a Blockchain system is distributed and that there is no single point of security failure. However, as seen in the system architecture analysis in Chapter 3, distribution only occurs within a Blockchain boundary, but a large portion of its system components are still centralized. For instance, wallet service which is currently utilized by most end users, are operating on a traditional centralized web server. All active trading funds are stored at a centralized hot storage in a cryptocurrency exchange. Third-party Multi-Sig authentication solutions also provide users service running on a centralized server. If a system contains centralized controls, it should require a traditional system protection approach, such as fraud prevention, access management and confidentiality requirements. However, the Blockchain system poses a serious dilemma of system security architecture, caused by a mixture of centralization and decentralization, because its security controls have been essentially handed over to end users in a distributed manner.

6.3 Remediation approach of Blockchain system security issues

Below, Table 6.3 is a list of recommended remediations from identified cyberattack(s). The listed remediations are based on the studies about actual hacking incidents targeting Blockchain systems in Chapter 4 and Chapter 5. The recommended security remediations were referenced from well-known public sources, such as Open Web Application Security Project (OWASP), National Institute of Standard and Technology (NIST) and Computer Emergency Response Team (CERT). Each recommended remediation in the left-most column starts with the naming convention RR-N, which means Recommended Security Remediation Number N. The naming convention is used in later chapters of this paper. The second column contains cyberattacks

which would be prevented by the recommended security remediation. The third column contains security domain(s) where the remediation can be applied to work as security resolutions. Hence, some of listed remediations are the same content but associated to different kind of cyberattacks and security domains. For example, both RR-9 and RR-10 contain the same remediation as a requirement of security source review. However, depending on which security domain it is applied to, it remediates different sets of cyberattacks. When it is implemented on D-2, the security domain Front-end Access-Point, the remediation would protect from AV-8 (SQL injection attack) and AV-16 (Cross-Site Scripting attack). When it is implemented on D-3, distributed application, the remediation would protect from AV-11 (reentrancy vulnerability) and AV-14 (self-destruction attack).

Recommended Security Remediation (RR-N)	**Cyberattacks / Security Vulnerability**	**Security Domain #**
(RR-1) User Activity Surveillance or Monitoring required.	AV-1, AV-2, AV-3, AV-15	D-1, D-2, D-3
(RR-2) Review Blockchain protocol implementation with secure source review needed.	AV-1, AV-2, AV-3, AV-5	D-1
(RR-3) Review Blockchain consensus option security review needed.	AV-1, AV-4, AV-5	D-1
(RR-4) Infrastructure security review required.	AV-5, AV-6, AV-9, AV-10	D-1, D-2, D-3
(RR-5) Network security scan needed.	AV-6, AV-7, AV-9, AV-13	D-2, D-3
(RR-6) Network security monitoring required.	AV-6, AV-9, AV-21, AV-22, AV-23	D-2, D-3, D-4
(RR-7) User data input validation source review needed.	AV-8, AV-16, AV-17, AV-18	D-2, D-4
(RR-8) Server data output filtering source review required.	AV-8, AV-17, AV-18	D-2
(RR-9) Application security source review required.	AV-8, AV-10, AV-16, AV-17, AV-18	D-2
(RR-10) Smart contract security source review required.	AV-11, AV-12, AV-13, AV-14, AV-15	D-3
(RR-11) Application security penetration test required.	AV-5, AV-10, AV-16, AV-17	D-2, D-3

Recommended Security Remediation (RR-N)	Cyberattacks / Security Vulnerability	Security Domain #
(RR-12) Analysis of security vulnerabilities in complied software without source code needed.	AV-19,	D-2, D-3
(RR-13) Limit the import library usage in compiled software.	AV-13, AV-19	D-3
(RR-14) Implement host based virus or malware scanner.	AV-19, AV-20	D-1, D-2, D-3, D-4
(RR-15) Implement secure communication channel such as VPN.	AV-19, AV-20, AV-21, AV-22	D-1, D-2, D-3, D-4
(RR-16) Implement secure hardware device on end point such as RSA token.	AV-21, AV-22	D-1, D-2, D-3, D-4
(RR-17) Implement additional secure authentication process such as 2-factor authentication.	AV-15, AV-19	D-2, D-3

Table 6. 3 – List of recommended security resolutions for cyberattacks and security vulnerability in Blockchain system.

CHAPTER 7 – Security Assessment Method for a Blockchain System

"Not only must attempts be made to prevent breaches, there must be efforts to detect and effectively recover from breaches, which are even more poorly addressed."

- Stuart Madnick
(Director of MIT's IC^3, at interview in "Risk Business at IES")

7.1 Needs to detect and address potential security issue

Identifying security issues within a Blockchain system and remediating them prior to a hacking incident would be ideal. Unfortunately, traditional methods are insufficient and ineffective for Blockchain system security analysis. An existing bottom-up approach mainly aims to identify failures of linear systems and single components. However, a Blockchain system includes a mixture of centralized and decentralized system components. Also, their interconnections are quite complicated.

The System-Theoretic Process Analysis (STPA) developed by N. Leveson is a holistic system hazard analysis method designed to address such challenges [379]. As a top-down approach, STPA systematically structures constraints and controls to identify conditions that potentially lead a system to an unsafe state [380]. N. Leveson and William Young then developed the STPA-Sec (System-theoretic Process Analysis for Security). STPA-Sec modifies and improves the safety-focused STPA to perform security analysis based on system theory [381]. STPA-Sec examines each control action under different possible conditions and identifies loss scenarios that contain insufficient or missing controls or security constraints. Following this, SPTA-Sec discovers the most critical system components and highlights the potential system security hazards that can be caused by the malfunctioning of the critical components [382].

In later sections in this chapter, a new security analysis approach for Blockchain systems will be proposed and the approach will be applied to simplified distributed application for a mini case study. The proposed approach is truly inspired by the STPA-Sec and also referenced by other researchers, which expands the STPA-Sec to cover other safety elements, such as safety and security [383] as well as data privacy [384].

7.2 Proposal for a security assessment method for the Blockchain system

Terminology for Blockchain System Security

As a first step, additional terms for the new proposed security assessment method are arranged as shown in Table 7.1. This terminology alignment was proposed to make the security assessment method more useful for cyberattacks and hacking incidents such as reducing misleading exploitation techniques and clarifying the targets of cyberattacks. For example, in most existing security assessment methods, the term *cyberattack* is a vague concept, such as "an external threat for system misuse." However, in the proposed security assessment, each cyberattack will be described in more detail and specifically for Blockchain systems, such as "an attempt to gain unauthorized access by exploiting system security controls to make unauthorized use of system assets."

Terms of the Security Assessment Method for Blockchain System	Description
Adverse Consequence	Unexpected / undesirable consequences to cause risk / loss in system perspective.
Cyberattack	Usage of a system asset / control in un-desirable way or attempt to causes loss of system in unsafe / unsecure way with exploitation of system security control.
Remediation	Migration or treatment of security vulnerability to bring system state to risk-free from threat.
Threat	Potential cause of an unexpected incident in aspect of system security.
Unsecured data flow	Data flow action which may allow attack, cause vulnerability and then may result in adverse sequence in the end.
Vulnerability	Security weakness of system asset and control that can be exploited by attack.

Table 7. 1 – Additional security terminology of proposed security assessment methodology for Blockchain System.

Process for Security Assessment Method

Below, Table 7.2 describe each step of the security assessment method for Blockchain systems in terms of exercise, information and results. In the first step, the target system is generally reviewed and its goal identified. The second step analyzes system architecture and data flow to retrieve system components and its associated controls. Each identified

system component is categorized into the 4 security domains (D-N), and then Table 3.2 is used to identify potential security risks (SR-N) associated with each system component. In the third step, adverse consequences are derived based on discovered potential risks in the second step. The adverse consequence is the impact of each cyber risk and threat on a particular system component. Then, using Table 4.7, each potential cyberattack and security vulnerability (AV-N) for each system component is discovered based on previously identified adverse consequences and security risks. The fourth step, the final phase, discovers recommended security remediation(s) (RR-N) for a particular system component using the associated potential cyberattack and security vulnerability as well as Table 6.3.

Step #		Process	Support
Step 1	1.1	Define goal(s) of target system.	
Step 2	2.1	Identify component(s) and associated data flow(s) of target system. Then categorize them into the 4 Blockchain system security domains from section 3.4.	• 17 security risks (SR-N) identified from table 3.2. • 4 security domains (D-N) identified in section 3.4.
	2.2	Map between Blockchain system security domain(s) (D-N) and target system component(s) to identify potential security risk(s) (SR-N) in table 3.2.	
Step 3	3.1	Derive adverse consequence(s) for each target system component from identified potential security risk(s) from step 2.2.	• 23 cyberattacks and security vulnerabilities (AV-N) from table 4.7.
	3.2	Map the adverse consequence(s) from step 3.1 and security risk(s) from step 2.2 to identify potential cyberattack(s) / security vulnerability (AV-N) in table 4.7.	
Step 4	4.1	Map the table 6.3 with identified system's potential cyberattack(s) & recommended security vulnerability(s) from step 3.2 to identify recommended security remediation(s) (RR-N).	• 17 recommended security remediations (RR-N) from table 6.3.

Table 7. 2 – Overview of the four steps of proposed security assessment methodology for Blockchain System.

Each step requires information and produces artifacts. Most of information about general Blockchain system security is supplied from tables in previous chapters. The artifact is the results of the exercise and is being used for the next exercise and the following step(s). Below, Table 7.3 provides an overview of the proposed Blockchain system security assessment methodology, in terms of produced artifact and supplied information to support the exercise.

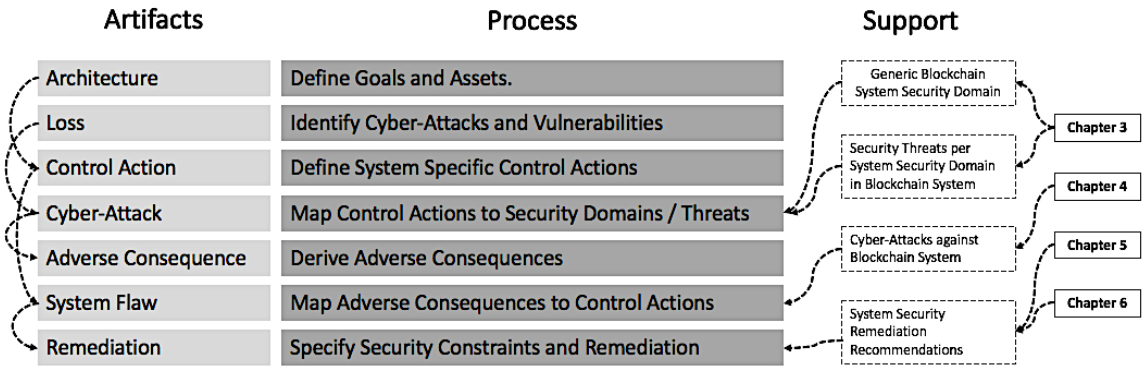


Figure 7. 1 – Flow diagram of the proposed security assessment methodology for Blockchain System.

7.3 Application of the security assessment method to Blockchain systems

To evaluate the proposed methodology, Section 7.3 demonstrates its application to simplified distributed voting application on the Ethereum Blockchain system. The proposed security assessment method will discover potential security issue(s) and will find suggestive resolution to remediate them in the early phase in SDLC.

Step 1: Define System Goal(s)

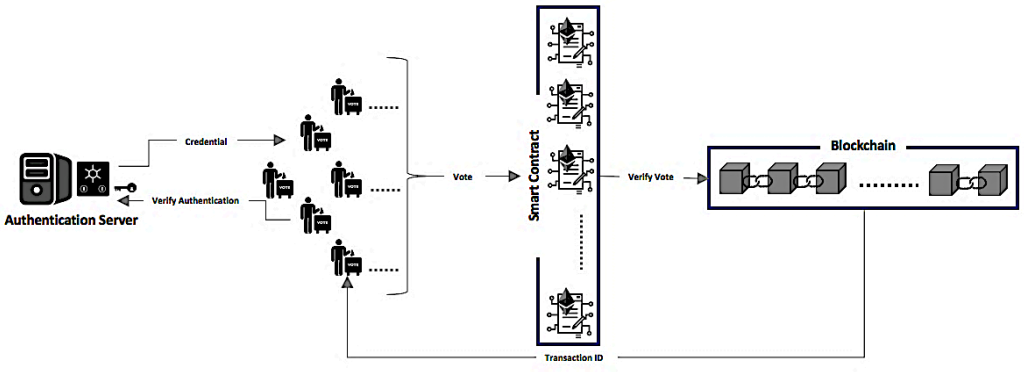


Figure 7. 2 – Overview of simplified distributed voting application based on Ethereum system [385].

Figure 7.2 shows a brief overview of simplified voting for smart contracts on the Ethereum Blockchain system. First, voters must verify their identification through a third-party authentication server. Voters can then cast a vote in the form of a smart contract. Once the smart contract is confirmed and added to the Blockchain, the voting process is completed and the record permanently remains on the Blockchain.

Building a voting application on a Blockchain system can address multiple issues which have been challenging to existing electronic voting systems. First, in terms of integrity, the data transaction (votes and time) is recorded permanently. Second, in regard to the transparency and auditability, the voting results are distributed to entire network nodes (voters) to prevent any forgery. Lastly, with respect to the availability, nodes (users) never reveal their identity. Therefore, the entire system process is carried out transparently and impartially with voter anonymity.

Step 2.1: Categorize System Component(s) into Security Domain(s)

Below, Figure 7.3 shows an interconnected data flow diagram of the smart contract voting system previously shown in Figure 7.2. Eight system components were identified. Based on system security domains established in Chapter 3, Ethereum Blockchain (SC-1) is included in a domain of platforms. Voting creator (SC-2), smart contract (SC-3) and voters (SC-4) are included in a domain of dApps. The rest of the identified system components (SC-5 ~ SC-8) are all included in a domain of Endpoint. The data flow(s) between a domain of platform to other domains are simply based on voting results. However, the data flow(s) between Endpoint and dApps are complex and more likely to become targets of cyberattacks.

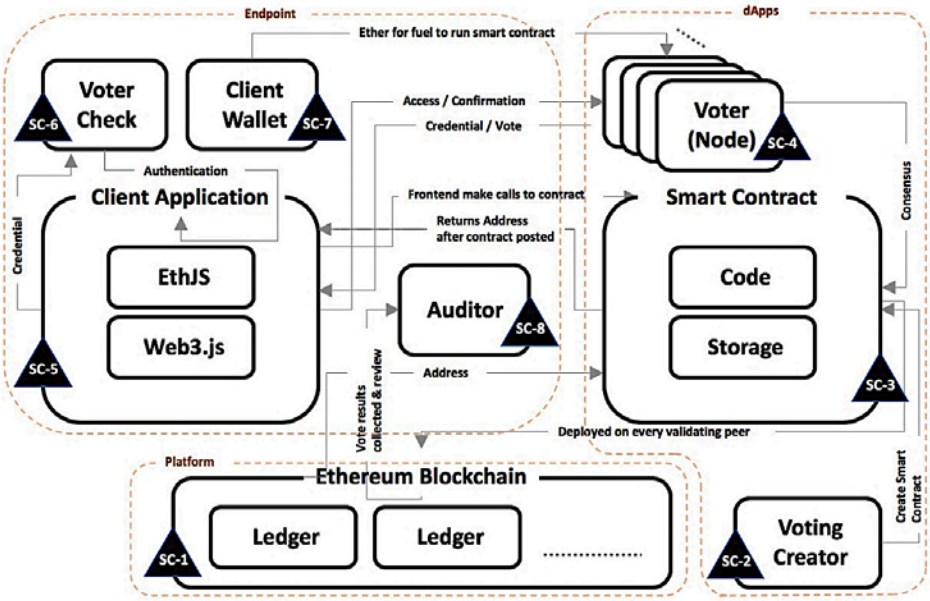


Figure 7. 3 – Simplified system component diagram of smart contract voting system. Squares are system components and attached triangle contains system component number(s) for convention.

Step 2.2: Mapping System Components and Security Domains to Discover Security Risks

Once the domain of each component in the voting system was identified, the potential security risks related to each system component was recorded using Table 3.2. Table 7.3 shows the results of mapping potential system security risks to identified system components per system security domain. With the top-down mapping approach, the system component(s) in the same security domain will have the same or a very similar set of security risks. For instance, SC-5 ~ SC-8 are categorized in D-4 (Endpoint), which all have potential security risks of data manipulation (SR-5), data loss (SR-6) and secure channel broken (SR-7). However, both SC-6 and SC-7 contain the additional security risk of user access broken (SR-8), since SC-6 and SC-7 need to perform an additional data process requiring additional security protection.

		SR-1	SR-2	SR-3	SR-4	SR-5	SR-6	SR-7	SR-8	SR-9	SR-10	SR-11	SR-12	SR-13	SR-14	SR-15	SR-16	SR-17
D-1	SC-1	✓				✓				✓	✓						✓	✓
D-2																		
D-3	SC-2					✓	✓		✓	✓	✓					✓	✓	✓
	SC-3	✓			✓	✓	✓		✓	✓	✓					✓	✓	✓
	SC-4					✓	✓		✓	✓	✓	✓				✓	✓	✓
D-4	SC-5	✓				✓	✓	✓	✓			✓	✓	✓	✓			
	SC-6	✓				✓	✓	✓	✓	✓		✓	✓	✓	✓			
	SC-7	✓				✓	✓	✓	✓	✓		✓	✓	✓	✓			
	SC-8	✓				✓	✓	✓	✓			✓	✓	✓	✓			

Table 7. 3 – Mapping system component(s) to system risk(s) in Blockchain system. Naming convention of Domain (D-N) and system risk (SR-N) are described in chapter 3. Please refer table 3.2 for more information.

Step 3.1 – Define Adversary Consequences

From Step 2.2, adverse consequences can be developed by combining system components with their potential system security risk(s) in the top-down approach. Each adverse consequence is triggered by one or more system security risk types and are also based on placement and implementation within the system architecture. For instance, system components SC-2 and SC-3 are both affected by security risks SR-5 and SR-6, so that smart contracts may be triggered in an unplanned or unexpected voting process by

malicious attacker(s). This is a very important step within the security assessment methodology, which is intended to disclose the system's vulnerable state. This, in turn, will be used as a bridge to find potential cyberattacks and corresponding remediations in subsequent steps. Table 7.4 below lists adverse consequences per system component(s).

System Component(s)	Security Risk(s)	Adverse Consequence(s)
SC-1	SR-1	Un-authorized voting data addition can be occurred.
	SR-5, SR-6, SR-7	Voting timestamp can be manipulated in Block.
	SR-14	Stored Voting data can be changed after addition.
SC-2, SC-3, SC-4	SR-5, SR-6	Smart contract(s) may be trigger un-planned or un-expected process by malicious attacker(s).
	SR-8, SR-9, SR-10	Vote function may be malfunction or out of gas consumption limitation.
	SR-15	Vote function(s) may be called repeatedly, before the first invocation of the function was finished.
	SR-15, SR-16, SR-17	Invocations of the other function may be called than voting to interact in destructive ways.
SC-3	SR-1, SR-4	Voting pool can be altered un-intendedly.
SC-4	SR-11	N/A
SC-5, SC-6, SC-7, SC-8	SR-1	Un-authorized access can be occurred.
	SR-4, SR-5, SR-6	Vote can be completed by malicious attacker prior to valid user.
	SR-7, SR-8	Vote can be dropped or denied.
	SR11, SR12, SR13, SR14	Voting process may be maliciously twisted. For instance, voting question changed or candidate number switched.
SC-6, SC-7	SR-9	Ether(s) in voter(s)'s wallet can be theft.

Table 7. 4 – List of adverse consequence(s) based on identified system security risk(s) and affected system component(s).

Step 3.2 – Mapping Adverse Consequence(s) to Potential Cyberattacks and Security Vulnerabilities

Once adverse consequences are derived from one or a group of the component(s) from the voting system in Table 7.4, cyberattacks and security vulnerabilities can be identified by mapping between Table 4.7 and Table 7.4. Table 4.7 summarizes known attacks and vulnerabilities mainly identified through review of the 78 real-world Blockchain system

security incidents in Section 4.1. The table contains corresponding domain, risk and adverse-consequence information for each identified attack or vulnerability. By matching information about security domains, security risks and adverse consequences between the two tables, potential attacks or vulnerabilities can be found for each system component.

For example, system component SC-2, implemented at domain D-2, may face an adverse consequence of an unintended repetitive function call due to the potential risks of SR-15 ~ 17. With the information of system component's domain, risk and adverse consequence, corresponding AV-11 can be identified as a potential cyberattack target. Table 7.5 summarizes the results of the mapping exercise to identify potential cyberattack(s) per system component by cross-referencing Table 4.7 and Table 7.4.

System Component(s)	Cyberattack(s) / Security Vulnerability(s)
SC-1	**AV-1, AV-3, AV-4**
SC-2	**AV-11, AV-12, AV-14**
SC-3	**AV-12, AV-14**
SC-4	**AV-11, AV-12, AV-13, AV-15**
SC-5	**AV-6, AV-16, AV-19, AV-20, AV-22, AV-23**
SC-6	**AV-17, AV-20, AV-22, AV-23**
SC-7	**AV-6, AV-16, AV-17, AV-18**
SC-8	**AV-19, AV-22, AV-23**

Table 7. 5 – Mapping table 7.4 and table 4.7 to identify potential cyberattack(s) / security vulnerability(s) per each system component in the voting system. Please refer table 4.7 for more information about cyberattacks and security vulnerabilities of Blockchain systems.

Step 4.1 – Identify Security Remediation for each Adverse Scenario

In the fourth step, recommended security remediation(s) for each system component were discovered throughout mapping Table 7.5 and Table 6.3 as shown in Table 7.6. As seen through the above exercises, the proposed methodology can provide system security information such as what types of cyberattacks system components can be subjected to and how to fix them. For example, based on information provided from Table 7.5, we can find system component SC-1 would require consideration of security remediation RR-1, RR-2 and RR-3.

System Component(s)	Recommended Security Remediation
SC-1	RR-1, RR-2, RR-3
SC-2	RR -7, RR -9
SC-3	RR -10
SC-4	RR -7, RR -9, RR -10, RR -13, RR -17
SC-5	RR -6, RR -7, RR -14, RR -15
SC-6	RR -11, RR -14, RR -15
SC-7	RR -6, RR -11, RR -15, RR -16
SC-8	RR -6, RR -12, RR -14, RR -15

Table 7. 6 – Mapping table 7.5 and table 6.3 to identify recommended security remediation(s) per each system component in the voting system. Please refer table 6.3 for more information about security remediation(s) for Blockchain systems.

To make the application of this methodology more realistic, the following two adverse scenarios are given as examples. Let's assume the identification of Adverse Scenarios #1, which is "votes are canceled/revoked in the middle of system running." Once SC-2 and SC-3 are identified as system components related to Adverse Scenario #1, the proposed methodology can find these components have potential security risks SR-5, SR-6, SR-8, SR-9 and SR-10, and have the possibility of becoming victim to cyberattacks AV-11, AV-12 and AV-14. Hence, the methodology recommends performing remediations RR-7, RR-9 and RR-10 to resolve security issues.

Adverse Scenario #1: Votes are canceled or revoked in the middle of system running.	
Affected System Component(s)	SC-2, SC-3
Security Domain(s)	D-2
Security Risk(s)	SR-5, SR-6, SR-8, SR-9, SR-10
Potential Cyberattack(s) / Vulnerability(s)	AV-11, AV-12, AV-14
Security Remediation(s)	RR-7, RR-9, RR-10

For another example, let's assume Adverse Scenario #2 is identified, which is "vote cast is proceeded on client side, but the vote cannot proceed after submission on the server side due to out of token (gas) or the out-of-gas consumption limit." Once SC-2, SC-3, SC-4 and SC-7 are identified as system components related to Adverse Scenario

#2, the proposed methodology discovers that these components are associated to security domains D-2 and D-3, so that confirms the components have potential security risks SR-5, SR-6, SR-8, SR-9, SR-10, R-15, SR-16 and SR-17. Since the confirmed security risks will expose system components to vulnerabilities or cyberattacks AV-6, AV-11, AV-12, AV-13, AV-15, AV-16, AV-17 and AV-18, the methodology recommends remediations RR-4, RR-6, RR-8, RR-9, RR-10 and RR-11 to resolve security issues in advance. Please note that an adverse scenario is supposed to be a textual representation of one specific case where a system operation can lead to a security issue that may subsequently cause an adverse consequence, including a system loss.

Adverse Scenario #2: Vote cast is proceeded on client side, but vote cannot be proceeded after submission on server side due to out of token (gas) or out of gas consumption limit.

Affected System Component(s)	**SC-2, SC-3, SC-4, SC-7**
Security Domain(s)	**D-2, D-3**
Security Risk(s)	**SR-5, SR-6, SR-8, SR-9, SR-10, R-15, SR-16, SR-17**
Potential Cyberattack(s) / Vulnerability(s)	**AV-6, AV-11, AV-12, AV-13, AV-15, AV-16, AV-17, AV-18**
Security Remediation(s)	**RR-4, RR-6, RR-8, RR-9, RR-10, RR-11**

Although it is not comprehensive, exercises in Chapter 7 show that the proposed methodology is useful for discovering potential security issues and remediation(s) from a system-level view using limited and high-level information from a Blockchain system. It is strongly focused on in-depth security analysis of the most critical components. With the top-down approach, the analysis identifies potential security issues from the system architecture and integrates all information to find appropriate security remediation. Since the analysis begins with system architecture information, it can be used to design complex reactive frameworks that ensure system security at the early stages of Blockchain system development.

CHAPTER 8 – Summary and Future Work

"There's no such thing as bad weather, only bad clothes."

- Scandinavian School in Jersey City
(Common Norwegian Phrases)

Blockchain is a relatively new technology of growing importance as its popularity continues to rise. However, misunderstanding and misconception of this new technology has continuously exposed all participants involved in the technology to cyber threats in recent years. Hence, this paper explored and analyzed Blockchain system security incidents to understand Blockchain system security as well as to provide a security evaluation framework for Blockchain systems.

In the beginning, the paper explored Blockchain in terms of technology. Throughout the exploration, it was found that the main purpose of utilizing Blockchain technology is for autonomous system data keeping as a form of decentralization, but it is not the technology for security. Then, as the next study, 78 actual Blockchain system hacking cases and heists were gathered and reviewed. The study summarized information regarding system exploitation and attack surfaces, which was categorized as to their causes as either: Platform Breach, dApps Exploit, Access Point Attack, or Endpoint Hacking. Then, the information was analyzed in various ways, and the following conclusions were drawn.

- *The amount of financial loss due to cyberattacks has significantly increased over the years.*
- *The target of cyberattacks has been moving to core Blockchain technology as hacking techniques evolve.*
- *The incident response and security remediation of Blockchain systems are insufficient. Large numbers of Blockchain systems have been continuously victimized for years by the same or similar types of cyberattacks.*
- *The impact of cyberattacks is quite deadly for Blockchain systems. A number of Blockchain system organizations have been closed due to hacking and heists.*
- *User authentication is the only area to protect an entire Blockchain system due to the characteristics of a decentralized system. Hence, more than half of cyberattacks have targeted the user-authentication process, such as identity theft or authentication bypass.*

For further research to discover the cause of cyber incident(s) in the Blockchain system, two cyberattacks (on the Ethereum Blockchain system and on the Bitfinex cryptocurrency exchange system) were selected, and in-depth analysis performed by using some of the methods in Causal Analysis using System Theory (CAST). Throughout the analysis, the following conclusions were drawn as security weaknesses of the Blockchain system:

- *Large portions of security controls in the Blockchain system heavily depend on inherited security features of Blockchain technology. However, Blockchain technology is designed and operating to protect the entire system from cyberattack(s).*
- *Due to autonomous operation, Blockchain systems have to be transparent and open to the public. However, information disclosure also contains other detail than just Blockchain operation, such as Blockchain's software development process, Blockchain's security issues, and even real-time security incident response actions of a Blockchain system.*
- *No dedicated party or group manages and handles security control in a decentralized system. Hence, in the event of a cyberattack, incident responses are very slow and ineffective so the on-going attack cannot be stopped immediately to minimize the impact. Further, after the incident, security issue remediations are not sufficient, since there is no supervision and/or no review.*

As concatenation of all researches, the paper then discussed common misconceptions about Blockchain system security, such as Blockchain is not immutable, Blockchain does not guarantee the user's anonymity, the transparency of Blockchain does not protect the system, and Blockchain is not hack-proof. Table 8.1 below summarizes the myths of Blockchain from Chapter 6.

Myth of Blockchain		**De-Mystification**
Immutability	Data is never changed.	"Fork" can change data in Blockchain system. "51% attack" is exploitation technic target to Blockchain in the same way of "Soft Fork".
Anonymity	Identity is never disclosed.	Blockchain system provides pseudonymity rather than anonymity. Even the pseudonymity can be assured only within system environment.
Transparency	Transparency secures system.	Blockchain system can only handle non-secure/in-sensitive data due to the transparency. Data can be disclosed not because Blockchain is secure, but because the data does not need protection.
Hack-Proof	Not hack-able.	Blockchain system is hack-able and it was even found that the characteristics of Blockchain technology hinder for system to respond cyberattack.

Table 8. 1 – Myth of Blockchain.

The paper also pointed out difficulties of securing the Blockchain system as follows:

- *The Blockchain system is designed for infinite operation without halt. Hence, once it is deployed and running, security enhancement and issue remediation become extremely difficult.*
- *The Blockchain system keeps increasing its complexity and boundary. Such system boundary expansion causes increasing complexity and ambiguity of the system boundary, and these make it very difficult for a developer to understand the system architecture and implement system security controls prior to deployment.*
- *The Blockchain system still utilizes centralized system components. In a decentralized system environment, system security control is handed over to end users. However, in the Blockchain system, the decentralization occurs within a Blockchain boundary, but a large portion of its system components are still centralized. When a system contains traditional component in centralized architecture, the traditional system security protection approach is still needed.*

Probing deeper, the results in this thesis also provide a strong foundation for future work in the area of Blockchain system security. One area of future work is in combining the knowledge gained about cyberattacks targeting Blockchain systems with knowledge about government policy changes. Another area is in applying the proposed causal analysis framework to the many other real-world cyber incident cases for elaboration and enhancement. Implementing the proposed security assessment method (Chapter 7) as software would also be a good area for future work, because it can generate security recommendations automatically based on Blockchain system architecture.

Appendix A - Yearly Loss of Heist due to Cyber Attack in Blockchain Systems

Year	Organization	Category	Loss Amount
2011	Allinvain	E	$239,250.00
2011	Mtgox - 1st	E	$30,800.00
2011	Bitomal	P	$222,530.00
2011	MyBitcoin	P	$833,792.40
2011	Bitcoin7	A	$25,150.00
2012	Slushi Pool - 1st	A	$14,760.00
2012	Bitcoinca - 1st	A	$214,285.68
2012	Bitcoinca - 2nd	A	$92,735.00
2012	Bitcoinca - 3rd	P	$350,000.00
2012	BTC-E - 1st	P	$35,000.00
2012	Bitfloor	P	$250,000.00
2012	Bitmarket.eu	A	$252,012.50
2013	Bitinstant	A	$12,000.00
2013	Instawallet	A	N/A
2013	Ozcoin	P	$105,000.00
2013	Slushi Pool - 2nd	A	N/A
2013	Bitcoin Central	A	N/A
2013	Vircurex	A	$163,000.00
2013	Bitfunder	A	$775,800.00
2013	Input.io	E	$813,891.00
2013	Bitcash.cz	E	$1,000,000.00
2013	Bidextreme.pl	A	$33,746.70
2013	BIPS	A	$1,226,261.40
2013	Picostocks	E	$5,681,520.00
2014	Silk Road 2	P	$2,700,000.00
2014	MTgox	P	$450,000,000.00
2014	FlexCoin	P	$700,000.00
2014	CoinEx.pw	A	N/A
2014	Poloniex	P	$43,233.22
2014	Dogevault	A	$55,000.00
2014	Cryptsy - 1st	E	$10,000,000.00
2014	BTER - 1st	A	$1,650,000.00
2014	Mintpal	A	$2,000,000.00
2014	Cryptothrift	A	$5,000.00
2014	Justcoin	P	$300,000.00
2014	BTC-E - 2nd	E	$26,693,100.00

Year	Organization	Category	Loss Amount
2014	Bitpay	E	$1,800,000.00
2015	796	E	$313,920.00
2015	Bitstamp	E	$5,200,000.00
2015	LocalBitcoins	E	$5,336.64
2015	BTER - 2nd	A	$1,750,000.00
2015	KipCoin	A	$690,000.00
2015	Carvirtex	A	N/A
2015	Cryptoine	P	N/A
2015	Allcrypt	E	$10,867.08
2015	Coinapult	A	$42,900.00
2015	Bitfinex - 1st	A	$356,000.00
2015	Cloudminr	A	$0.00
2016	BitQuick	A	$0.00
2016	CoinTrader	A	$33,600.00
2016	Coinwallet.co	A	$0.00
2016	ShapeShift.io	A	$230,000.00
2016	Ethereum - 1st	D	$70,000,000.00
2016	CoinKite	A	$0.00
2016	Gatecoin	A	$2,000,000.00
2016	Steemit	A	$85,000.00
2016	Bitfinex - 2nd	P	$72,000,000.00
2016	Bitcurex	A	$1,500,000.00
2017	Zcoin	P	$600,000.00
2017	Yapizon - 1st	A	$5,000,000.00
2017	Jaxx	E	$400,000.00
2017	QuadrigaCX	E	$15,000,000.00
2017	Bithumb - 1st	E	$870,000.00
2017	Coindash	A	$7,000,000.00
2017	Ethereum - 2nd	D	$30,000,000.00
2017	Enigma	E	$500,000.00
2017	Ethereum - 3rd	D	$275,000,000.00
2017	Tether	A	$31,000,000.00
2017	Nicehash	A	$75,000,000.00
2017	youbit - 2nd	A	$15,000,000.00
2018	Blackwallet	A	$400,000.00
2018	Coincheck	E	$600,000,000.00
2018	Bitgrail	P	$195,000,000.00
2018	Bee	A	$1,000,000.00
2018	CoinSecure	A	$3,300,000.00
2018	MyEtherWallet	A	$152,000.00
2018	Coinrail	A	$42,000,000.00
2018	Bithumb - 2nd	E	$30,000,000.00

Bibliography

[1] A. Rosic, "blockgeeks.com," 2016. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed 21 03 2018].

[2] T. R. N. Desk, "Why is Blockchain Gaining Popularity?," 31 May 2017. [Online]. Available: https://www.readitquik.com/articles/digital-transformation/why-is-blockchain-gaining-popularity/. [Accessed 21 12 2017].

[3] N. News, "Nasdaq and Citi Announce Pioneering Blockchain and Global Banking Integration," NASDAQ, 22 5 2017. [Online]. Available: https://www.nasdaq.com/article/nasdaq-and-citi-announce-pioneering-blockchain-and-global-banking-integration-cm792544. [Accessed 30 8 2018].

[4] J. Mathis, "FedEx is Testing Blockchain Tech for Critical Cargo Shipments," CCN, 15 5 2018. [Online]. Available: https://www.ccn.com/tracking-key-shipments-fedex-is-testing-with-blockchain/. [Accessed 31 8 2018].

[5] J. Agrawal, "8 Benefits of Blockchain to Industries Beyond Cryptocurrency," Entrepreneur, 18 1 2018. [Online]. Available: https://www.entrepreneur.com/article/306420. [Accessed 29 8 2018].

[6] C. Insights, "Blockchain Investment Trends In Review," CB Insights, 1 1 2018. [Online]. Available: https://www.cbinsights.com/research/report/blockchain-trends-opportunities/. [Accessed 30 8 2018].

[7] CSIRO, "Risks and Opportunities for Systems using blockchain and Smart Contracts," CSIRO, Australia, 2017.

[8] P. Belagatti, "What Is Blockchain Technology and Why Is It So Popular," 27 05 2017. [Online]. Available: http://www.influencive.com/blockchain-technology-popular/. [Accessed 21 12 2017].

[9] Statista, "Blockchain Market Projection to 2021 in World Wide," Statista, [Online]. Available: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/. [Accessed 20 3 2018].

[10] D. Blog, "Blockchain: Cyber Security Pros and Cons," Dev Blog, 31 10 2017. [Online]. Available: https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons. [Accessed 14 8 2018].

[11] P. Passeri, "2017 Cyber Attacks Statistics," 17 01 2018. [Online]. Available: https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/. [Accessed 25 03 2018].

[12] I. Pro, "Biggest Cryptocurrency Hacks," 29 01 2018. [Online]. Available: https://en.insider.pro/infographics/2018-01-29/chart-day-biggest-cryptocurrency-hacks/. [Accessed 15 03 2018].

[13] L. Mearian, "The top 5 problems with blockchain," 10 11 2017. [Online]. Available: https://www.computerworld.com/article/3236480/emerging-technology/the-top-5-problems-with-blockchain.html. [Accessed 05 02 2018].

[14] W. S. S. Stuart Haber, "How to time-stamp a digital document," *Journal of Cryptology,* vol. 3, no. 2, pp. 99-111, 1991.

[15] S. H. W. S. S. Dave Bayer, "Improving the Efficiency and Reliability of Digital Time-Stamping," *Sequences II,* pp. 329-334, 1992.

[16] S. Ghosh, "Will Blockchain Become the Cyber Security Linchpin for the Digital Future?," 21 07 2017. [Online]. Available: https://www.hcltech.com/blogs/will-blockchain-become-cyber-security-linchpin-digital-future. [Accessed 15 01 2018].

[17] A. Hertig, "What is a DAO?," coindesk, 1 1 2017. [Online]. Available: https://www.coindesk.com/information/what-is-a-dao-ethereum/. [Accessed 15 1 2018].

[18] M. W. N. B. Rituparna Bhattacharya, "A blockchain based peer-to-peer framework for exchanging leftover foreign currency," in *IEEE*, 2017.

[19] Bitcoin.it, "the Bitcoin Wiki," bitcoin.it, 14 4 2010. [Online]. Available: https://en.bitcoin.it/wiki/Main_Page. [Accessed 25 1 2018].

[20] S. B. Rumy, "How the Blockchain Works," Technical Ustad, 7 10 2017. [Online]. Available: https://technicalustad.com/how-the-blockchain-works/. [Accessed 24 1 2018].

[21] Universa, "Decentralized autonomous organization—What is a DAO company?," 28 11 2017. [Online]. Available: https://medium.com/universablockchain/decentralized-autonomous-organization-what-is-a-dao-company-eb99e472f23e. [Accessed 23 1 2018].

[22] B. Wiki, "Mining," Bitcoin Wiki, [Online]. Available: https://en.bitcoin.it/wiki/Mining. [Accessed 1 12 2018].

[23] Unocoin, "Bitcoin miners vs Bitcoin nodes," Unocoin, 6 2 2018. [Online]. Available: https://blog.unocoin.com/bitcoin-miners-vs-bitcoin-nodes-6a4d35be9712. [Accessed 2 12 2018].

[24] G. Greenspan, "The Blockchain Immutability Myth," Coindesk, 09 05 2017. [Online]. Available: https://www.coindesk.com/blockchain-immutability-myth/. [Accessed 24 01 2018].

[25] B. Wiki, "Nonce," Bitcoin Wiki, [Online]. Available: https://en.bitcoin.it/wiki/Nonce. [Accessed 02 12 2018].

[26] R. A. Grimes, "Hacking bitcoin and blockchain," CSO, 12 12 2017. [Online]. Available: https://www.csoonline.com/article/3241121/cyber-attacks-espionage/hacking-bitcoin-and-blockchain.html. [Accessed 27 01 2018].

[27] B. Wiki, "Proof of work," [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_work. [Accessed 25 1 2018].

[28] Investopedia, "Proof of Work," Investopedia, [Online]. Available: https://www.investopedia.com/terms/p/proof-work.asp. [Accessed 2 12 2018].

[29] N. C. Fabien Aepli, "Blockchain simply explained," Mangeat, 2017.

[30] A. G. Karl Wüst, "Do you need a Blockchain?," Department of Computer Science ETH Zurich, Switzerland, 2017.

[31] B. Wiki, "Multisignature," Bitcoin Wiki, [Online]. Available: https://en.bitcoin.it/wiki/Multisignature. [Accessed 2 12 2018].

[32] C. Desk, "What is a Decentralized Application?," Coin Desk, [Online]. Available: https://www.coindesk.com/information/what-is-a-decentralized-application-dapp. [Accessed 2 12 2018].

[33] Wikipedia, "Cryptocurrency wallet," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Cryptocurrency_wallet. [Accessed 02 12 2018].

[34] C. Castiglione, "Hot Wallet vs. Cold Storage," One Month, 11 10 2017. [Online]. Available: https://learn.onemonth.com/hot-wallet-vs-cold-storage/. [Accessed 2 12 2018].

[35] List.io, "Nodes," List.io, [Online]. Available: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/nodes. [Accessed 2 12 2018].

[36] B. Mining, "How Bitcoin Mining Works," Bitcoin Mining, [Online]. Available: https://www.bitcoinmining.com. [Accessed 2 12 2018].

[37] V. Suji, "What Are Dapps? The New Decentralized Future," Block Geeks, 2017. [Online]. Available: https://blockgeeks.com/guides/dapps/. [Accessed 18 02 2018].

[38] L. Turvey, "Blockchain Implementation Security. A hardening how-to," 22 8 2017. [Online]. Available: https://www.pentestpartners.com/security-blog/blockchain-implementation-security-a-hardening-how-to/. [Accessed 14 3 2018].

[39] B. Beyst, "Reasons Why CISOs Need Threat Modeling," Threat Modeler, 15 4 2016. [Online]. Available: https://threatmodeler.com/2016/04/15/4-key-reasons-cisos-need-threat-modeling/. [Accessed 18 5 2018].

[40] OWASP, "Content Spoofing," OWASP, [Online]. Available: https://www.owasp.org/index.php/Content_Spoofing. [Accessed 20 9 2018].

[41] N. Secure, "NRI Secure Launches Japan’s First “Blockchain Assessment” Service," 23 7 2017. [Online]. Available: https://www.nri-secure.com/blog/nri-secure-launches-japans-first-blockchain-assessment-service. [Accessed 28 3 2018].

[42] B. Graveyard, "Blockchain Graveyard," [Online]. Available: https://magoo.github.io/Blockchain-Graveyard/. [Accessed 5 4 2018].

[43] Allinvain, "I just got hacked - any help is welcome! (25,000 BTC stolen)," Bitcoin Forum, 13 6 2011. [Online]. Available: https://bitcointalk.org/index.php?PHPSESSID=fc3f7e84282795804dae8afde402e17d&topic=16457.0. [Accessed 4 7 2018].

[44] R. BRODERICK, "Bitcoin, Used to Purchase Illegal Things, Has Been Illegally Stolen," Motherboard, 15 6 2011. [Online]. Available: https://motherboard.vice.com/en_us/article/gvv8kj/bitcoin-currency-used-for-illegal-things-illegally-stolen. [Accessed 4 7 2018].

[45] A. Norry, "The History of the Mt Gox Hack: Bitcoin’s Biggest Heist," blockonomi, 29 11 2017. [Online]. Available: https://blockonomi.com/mt-gox-hack/. [Accessed 6 4 2018].

[46] L. Eichholz, "MtGox, BTC-e, and the Missing Coins: A living timeline of the greatest cyber crime ever," bravenewcoin, 17 8 2017. [Online]. Available: https://bravenewcoin.com/news/mtgox-btc-e-and-the-missing-coins-a-living-timeline-of-the-greatest-cyber-crime-ever/. [Accessed 5 4 2018].

[47] K. DOTSON, "Third Largest Bitcoin Exchange Bitomat Lost Their Wallet, Over 17,000 Bitcoins Missing," 1 8 2011. [Online]. Available: https://siliconangle.com/blog/2011/08/01/third-largest-bitcoin-exchange-bitomat-lost-their-wallet-over-17000-bitcoins-missing/. [Accessed 6 4 2018].

[48] A. Jeffries, "MyBitcoin.com Is Back: A Week After Vanishing With at Least $250 K. Worth of BTC, Site Claims It Was Hacked," 5 8 2011. [Online]. Available: http://observer.com/2011/08/mybitcoin-disappeared-with-bitcoins/. [Accessed 6 4 2018].

[49] A. Jeffries, "MyBitcoin Spokesman Finally Comes Forward: “What Did You Think We Did After the Hack? We Got Shitfaced”," Observer, 8 8 2011. [Online]. Available: https://observer.com/2011/08/mybitcoin-spokesman-finally-comes-forward-what-did-you-think-we-did-after-the-hack-we-got-shitfaced/. [Accessed 30 6 2018].

[50] J. Redman, "The Bitcoin Exchange Thefts You May Have Forgotten," Bitcoin.com, 3 2 2017. [Online]. Available: https://news.bitcoin.com/bitcoin-exchange-thefts-forgotten/. [Accessed 6 4 2018].

[51] K. DOTSON, "Bitcoin7 Hacked, Funds Recovery Requires Sensitive Personal Information," Silicon Angle, 7 10 2011. [Online]. Available: https://siliconangle.com/blog/2011/10/07/bitcoin7-hacked-funds-recovery-requires-sensitive-personal-information/. [Accessed 8 4 2018].

[52] J. Hind, "bitcoin7.com 'hacked'. Database and wallets 'stolen'," 6 10 2011. [Online]. Available: https://bitcointalk.org/index.php?topic=46982.0. [Accessed 6 4 2018].

[53] V. Buterin, "The Bitcoinica Linode Theft and What it Means for Bitcoin," 3 3 2012. [Online]. Available: https://bitcoinmagazine.com/articles/the-bitcoinica-linode-theft-and-what-it-means-for-bitcoin-1330805009/. [Accessed 5 4 2018].

[54] Sabbetus, "Slash Dot," Slash Dot, 1 3 2012. [Online]. Available: https://slashdot.org/story/12/03/02/0059202/linode-exploit-caused-theft-of-thousands-of-bitcoins. [Accessed 28 6 2018].

[55] Slush, "Hacked Linode & coins stolen to 1NRy8GbX56MymBhDYM...," Bitcoin Forum, 1 3 2012. [Online]. Available: https://bitcointalk.org/index.php?topic=66916.0. [Accessed 28 6 2018].

[56] T. Worstall, "Another Bitcoin Theft at Bitcoinica," Forbes, 15 5 2012. [Online]. Available: https://www.forbes.com/sites/timworstall/2012/05/15/another-bitcoin-theft-at-bitconia/. [Accessed 16 5 2018].

[57] Bitcoinica, "Bitcoinica Hack Post Mortem," Bitcoinica, 15 5 2012. [Online]. Available: http://bitcoinica.blogspot.com. [Accessed 16 5 2018].

[58] D. Goodin, "Unknown hackers broke into Bitcoinica, a site that trades the virtual currency. DAN GOODIN - 5/11/2012, 9:40 PM WordPress is now the most well-known company to accept Bitcoin. redditor freeborn More than $87,000 worth of the virtual currency known as B," Ars Technica, 11 5 2012. [Online]. Available:

https://arstechnica.com/uncategorized/2012/05/bitcoins-worth-87000-plundered/. [Accessed 16 5 2018].

[59] genjix, "Bitcoinica MtGox account compromised," Bitcoin Forum, 13 7 2012. [Online]. Available: https://bitcointalk.org/index.php?topic=93074.0. [Accessed 16 5 2018].

[60] Unknown, "BTC-e post a statement about the hack, and apparently have no idea how it happened," Reddit, 31 7 2012. [Online]. Available: https://www.reddit.com/r/Bitcoin/comments/xg2qf/btce_post_a_statement_about_the_hack_and/. [Accessed 16 5 2018].

[61] repentance, "Bitcoin Forum," Bitcoin Forum, 31 7 2012. [Online]. Available: https://bitcointalk.org/index.php?topic=96831.0. [Accessed 16 5 2018].

[62] localethereum, "Centralised Exchanges Are Terrible At Holding Your Money: A Timeline of Catastrophes," Blog - localethereum, 14 11 2017. [Online]. Available: https://blog.localethereum.com/centralised-exchanges-are-terrible-at-holding-your-money/#btc-e-liberty-reserve-hack-2012. [Accessed 16 5 2018].

[63] V. Buterin, "Bitfloor Hacked, $250,000 Missing," Bitcoin Magazine, 5 9 2012. [Online]. Available: https://bitcoinmagazine.com/articles/bitfloor-hacked-250000-missing-1346821046/. [Accessed 17 5 2018].

[64] J. Biggs, " Hacker Steals $12,000 Worth Of Bitcoins In Brazen DNS-Based Attack," Techcrunch, 8 3 2013. [Online]. Available: https://techcrunch.com/2013/03/08/hacker-steals-12000-worth-of-bitcoins-in-brazen-dns-based-attack/. [Accessed 11 4 2018].

[65] R. MCMILLAN, "HACKERS PULL OFF $12,000 BITCOIN HEIST," Wired, 7 3 2013. [Online]. Available: https://www.wired.com/2013/03/digital-thieves-pull-off-12000-bitcoin-heist/. [Accessed 11 4 2018].

[66] S. Ludwig, "Bitcoin wallet service Instawallet hacked, shuts down ‘indefinitely’," Venture Beat, 3 4 2013. [Online]. Available: https://venturebeat.com/2013/04/03/bitcoin-wallet-instawallet-hacked/. [Accessed 10 4 2018].

[67] K.-M. Cutler, "Another Bitcoin Wallet Service, Instawallet, Suffers Attack, Shuts Down Until Further Notice," Techcrunch, 3 4 2013. [Online]. Available: https://techcrunch.com/2013/04/03/bitcoin-instawallet/. [Accessed 11 4 2018].

[68] dree12, "List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses," Bitcoin Forum, 26 5 2012. [Online]. Available: https://bitcointalk.org/index.php?topic=83794.0#post_toc_47. [Accessed 11 4 2018].

[69] N. Fincham, "Slush's bitcoin mining pool hacked," MineForeman, 24 4 2013. [Online]. Available: https://mineforeman.com/2013/04/24/slushs-bitcoin-mining-pool-hacked/. [Accessed 16 5 2018].

[70] N. D. Bradbury, "Hackers hit Bitcoin Central exchange," Coin Desk, 29 4 2013. [Online]. Available: https://www.coindesk.com/hackers-hit-bitcoin-central-exchange/. [Accessed 12 4 2018].

[71] V. Management, "May 2013 Report," Vircurex, Beijing, 2013.

[72] J. Southurst, "Exchange Vircurex Freezes Withdrawals, Claims Lack of Reserves," Coin Desk, 24 4 2014. [Online]. Available: https://www.coindesk.com/exchange-vircurex-freezes-withdrawals-claims-lack-reserves/. [Accessed 13 4 2018].

[73] L. Vaas, "Bitcoin exchange founder charged with covering up hack," Naked Security, 23 2 2018. [Online]. Available: https://nakedsecurity.sophos.com/2018/02/23/bitcoin-exchange-founder-charged-with-covering-up-hack/. [Accessed 11 4 2018].

[74] C. Hamilton, "Bitcoin Platform Operator Allegedly Lied to SEC Over Hack," Law.com, 21 2 2018. [Online]. Available: https://www.law.com/newyorklawjournal/2018/02/21/bitcoin-platform-operator-allegedly-lied-to-sec-over-hack/?slreturn=20180415025357. [Accessed 14 4 2018].

[75] lbarrow, "Inputs.io hacked – 4100 BTC stolen," ycombinator, 7 11 2013. [Online]. Available: https://news.ycombinator.com/item?id=6687795. [Accessed 14 4 2018].

[76] A. Hern, "Bitcoin site Inputs.io loses £1m after hackers strike twice," The Guardian, 8 11 2013. [Online]. Available: https://www.theguardian.com/technology/2013/nov/08/hackers-steal-1m-from-bitcoin-tradefortress-site. [Accessed 15 4 2018].

[77] Gladoscc, "Inputs.io," Bitcoin Wiki, [Online]. Available: https://en.bitcoin.it/wiki/Inputs.io. [Accessed 11 4 2018].

[78] M. Kumar, "Bitcash.cz Bitcoin Exchange hacked; Money from 4000 Bitcoin wallets Stolen," The Hacker News, 13 11 2013. [Online]. Available: https://thehackernews.com/2013/11/bitcashcz-bitcoin-exchange-hacked-money.html. [Accessed 15 4 2018].

[79] D. Bradbury, "Czech bitcoin exchange Bitcash.cz hacked and up to 4,000 user wallets emptied," Coin Desk, 12 11 2013. [Online]. Available: https://www.coindesk.com/czech-bitcoin-exchange-bitcash-cz-hacked-4000-user-wallets-emptied/. [Accessed 17 4 2018].

[80] J. Adamowski, "Polish Bitcoin Exchange Bidextreme.pl Hacked, Bitcoin and Litecoin Wallets Emptied," Coin Desk, 20 11 2013. [Online]. Available: https://www.coindesk.com/hacker-attack-polands-bitcoin-exchange/. [Accessed 15 4 2018].

[81] S. Państwo, "KOMUNIKAT z dnia 24.11.2013r. - DOTYCZĄCY ŚRODKÓW BTC I LTC SKRADZIONYCH Z PLATFORMY BIDEXTREM," Bidextreme, 14 8 2013. [Online]. Available: http://web.archive.org/web/20140425183423/http://bidextreme.pl/. [Accessed 29 6 2018].

[82] M. Santos, "All Bitcoins and Litecoins gone: Polish Bitcoin exchange Bidextreme.pl hacked From All Bitcoins and Litecoins gone: Polish Bitcoin exchange Bidextreme.pl hacked https://99bitcoins.com/all-bitcoins-and-litecoins-gone-polish-bitcoin-exchange-bidextreme-pl-," 99 Bitcoins, 2 1 2018. [Online]. Available: https://99bitcoins.com/all-bitcoins-and-litecoins-gone-polish-bitcoin-exchange-bidextreme-pl-hacked/. [Accessed 17 4 2018].

[83] S. Khandelwal, "Danish Bitcoin exchange BIPS hacked and 1,295 Bitcoins worth $1 Million Stolen," The Hacker News, 25 11 2013. [Online]. Available: https://thehackernews.com/2013/11/danish-bitcoin-exchange-bips-hacked-and_25.html. [Accessed 17 4 2018].

[84] jimmco, "Three most record-breaking Bitcon hacks and thefts," Busy Beta, 5 8 2016. [Online]. Available: https://busy.org/@jimmco/three-most-record-breaking-bitcon-hacks-and-thefts. [Accessed 17 4 2018].

[85] Forum, "list of major bitcoin heists thefts hacks scams and losses," Bitcointa.IK, [Online]. Available: https://bitcointa.lk/threads/list-of-major-bitcoin-heists-thefts-hacks-scams-and-losses.301464/. [Accessed 16 4 2018].

[86] DEEPDOTWEB, "Silk Road 2 Hacked, All Bitcoins Stolen – $2.7 Miliion," Deep.Dot.Web, 13 2 2014. [Online]. Available: https://www.deepdotweb.com/2014/02/13/silk-road-2-hacked-bitcoins-stolen-unknown-amount/. [Accessed 24 6 2018].

[87] D. Bradbury, "CoinDesk.com," CoinDesk, 13 2 2014. [Online]. Available: Silk Road 2 Loses Over $2.6 Million in Bitcoins in Alleged Hack. [Accessed 23 6 2018].

[88] G. H. Carter Dougherty, "Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss," Bloomberg, 28 2 2014. [Online]. Available: https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy. [Accessed 14 4 2018].

[89] D. Price, "The Worst Cryptocurrency Hacks Everyone Needs to Know About," Make use of dot com, 4 4 2018. [Online]. Available: https://www.makeuseof.com/tag/cryptocurrency-hacks/. [Accessed 17 5 2018].

[90] A. Hern, "Bitcoin bank Flexcoin closes after hack attack," The Guardian, 4 3 2014. [Online]. Available: https://www.theguardian.com/technology/2014/mar/04/bitcoin-bank-flexcoin-closes-after-hack-attack. [Accessed 16 4 2018].

[91] P. Rizzo, "Bitcoin Bank Flexcoin to Close After $600k Bitcoin Theft," Coin Desk, 4 3 2014. [Online]. Available: https://www.coindesk.com/bitcoin-bank-flexcoin-close-600000-bitcoin-theft/. [Accessed 15 4 2018].

[92] J. Brodkin, "How the “world’s first Bitcoin bank” was robbed blind," Ars Technica, 5 3 2014. [Online]. Available: https://arstechnica.com/information-technology/2014/03/how-the-worlds-first-bitcoin-bank-was-robbed-blind/. [Accessed 18 4 2018].

[93] C. Marckx, "CoinEx.pw hacked, all coins stolen," 19 3 2014. [Online]. Available: https://www.ccn.com/coinex-pw-hacked-all-coins-stolen/. [Accessed 19 5 2018].

[94] E. Spaven, "CoinEX.pw: We Were Hacked, But Will Cover All Losses," coindesk.com, 19 5 2014. [Online]. Available: https://www.coindesk.com/coinex-pw-hacked-will-cover-losses/. [Accessed 30 6 2018].

[95] S. Khatwani, "Top 5 Biggest Bitcoin Hacks Ever," Coinsutra, 21 11 2017. [Online]. Available: https://coinsutra.com/biggest-bitcoin-hacks/. [Accessed 18 4 2018].

[96] C. FARIVAR, "Yet another exchange hacked: Poloniex loses around $50,000 in bitcoin," Ars Technica, 6 3 2014. [Online]. Available: https://arstechnica.com/information-technology/2014/03/yet-another-exchange-hacked-poloniex-loses-around-50000-in-bitcoin/. [Accessed 30 6 2018].

[97] P. Rizzo, "Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack," CoinDesk, 5 3 2014. [Online]. Available: https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/. [Accessed 19 4 2018].

[98] C. Osborne, "Doge Vault hack exposes user passwords, wallet data," zdnet, 19 5 2014. [Online]. Available: https://www.zdnet.com/article/doge-vault-hack-exposes-user-passwords-wallet-data/. [Accessed 21 5 2018].

[99] NBCNEWS, "Major Dogecoin Wallet Hacked, Shut Down," nbcnews.com, 13 5 2014. [Online]. Available: https://www.nbcnews.com/tech/security/major-dogecoin-wallet-hacked-shut-down-n104096. [Accessed 30 6 2018].

[100] S. Higgins, "Cryptsy Threatens Bankruptcy, Claims Millions Lost in Bitcoin Heist," Coindesk, 15 1 2016. [Online]. Available: https://www.coindesk.com/cryptsy-bankruptcy-millions-bitcoin-stolen/. [Accessed 30 6 2018].

[101] A. Mizrahi, "Cryptsy Finally Reveals Source of Withdrawal Issues – $6 Million Hacking," Finance Magnates, 17 1 2016. [Online]. Available: https://www.financemagnates.com/cryptocurrency/exchange/cryptsy-finally-reveals-source-of-withdrawal-issues-6-million-hacking/. [Accessed 30 6 2018].

[102] S. Higgins, "8 Million Vericoin Hack Prompts Hard Fork to Recover Funds," 14 07 2014. [Online]. Available: https://www.coindesk.com/bitcoin-protected-vericoin-stolen-mintpal-wallet-breach/. [Accessed 19 06 2018].

[103] P. Rizzo, "Hackers Steal $1.65 Million in NXT from BTER Exchange," Coin Desk, 15 8 2014. [Online]. Available: https://www.coindesk.com/bter-nxt-bitcoin-exchange-hack/. [Accessed 30 6 2018].

[104] I. DeMartino, "EXCLUSIVE: Key Negotiator In Bter NXT Hack Speaks," Coin Telegraph, 25 8 2014. [Online]. Available: https://cointelegraph.com/news/exclusive-key-negotiator-in-bter-nxt-hack-speaks-out. [Accessed 30 6 2018].

[105] I. DeMartino, "CryptoThrift Suffers Security Breach, 15 BTC Stolen, Escrow Service Suspended," Cointelegraph, 7 10 2014. [Online]. Available: https://cointelegraph.com/news/cryptothrift-suffers-security-breach-15-btc-stolen-escrow-service-suspended. [Accessed 21 5 2018].

[106] C. C, "Stellar and Ripple Hacked: Justcoin to the Rescue," 14 10 2014. [Online]. Available: https://cointelegraph.com/news/stellar-and-ripple-hacked-justcoin-to-the-rescue. [Accessed 22 5 2018].

[107] GLOBALCRYPTONEWS, "JUSTCOIN GOXED: EXCHANGE HALTS MARKET AFTER LOSS OF 32 MILLION XRP AND 54 MILLION STELLAR," 12 10 2014. [Online]. Available: http://globalcryptonews.com/2014/10/12/justcoin-goxed-exchange-halts-market-after-loss-of-32-million-xrp-and-54-million-stellar/. [Accessed 22 5 2018].

[108] E. H. News, "Details of BTC-E and BitcoinTalk breach revealed," E Hacking News, 3 9 2016. [Online]. Available: http://www.ehackingnews.com/2016/09/details-of-btc-e-and-bitcointalk-breach.html. [Accessed 18 4 2018].

[109] Thran, "BTC-e suspended accounts and hacked accounts," Bitcoin Forum, 2 11 2014. [Online]. Available: https://bitcointalk.to/index.php?topic=460138.0. [Accessed 18 4 2018].

[110] bitcoinist, "Bitcoin Payment Service BitPay Reports Hack and Loss of 5000 BTC," Inside Bitcoins, 17 9 2015. [Online]. Available: https://insidebitcoins.com/news/bitcoin-payment-service-bitpay-reports-hack-and-loss-of-5000-btc/34877. [Accessed 19 4 2018].

[111] W. Suberg, "Chinese Exchange Gets 'Goxed' for 1,000 bitcoins (UPDATE: Company Responds)," Coin Telegraph, 28 1 2015. [Online]. Available: https://cointelegraph.com/news/chinese-exchange-suffers-1000-btc-loss-in-uncertain-service-compromise. [Accessed 2 7 2018].

[112] D. Ferrin, "796 Theft of 27 Jan," Crypto Crumb, 28 1 2015. [Online]. Available: http://blog.cryptocrumb.com/2015/01/796-theft-of-27-jan.html. [Accessed 2 7 2018].

[113] R. LEMOS, "Bitcoin exchange Bitstamp claims hack siphoned up to $5.2 million," Ars Technica, 6 1 2015. [Online]. Available: https://arstechnica.com/information-technology/2015/01/bitcoin-exchange-bitstamp-claims-hack-siphoned-up-to-5-2-million/. [Accessed 30 6 2018].

[114] R. Reader, "Bitstamp resumes Bitcoin trading after $5M in losses led to shutdown," Venture Beat, 9 1 2015. [Online]. Available: https://venturebeat.com/2015/01/09/bitstamp-resumes-trading-after-5m-in-losses-led-to-shutdown/. [Accessed 13 4 2018].

[115] S. Higgins, "LocalBitcoins User Funds Stolen After Chat Client Hack," Coin Desk, 29 1 2015. [Online]. Available: https://www.coindesk.com/localbitcoins-user-funds-stolen-chat-client-hack/. [Accessed 2 7 2018].

[116] A. Judge, "LocalBitcoins Hack Proves Bitcoin Wallets Need Two-Factor Authentication," Silicon, 29 1 2015. [Online]. Available: https://www.silicon.co.uk/security/cyberwar/localbitcoins-hack-proves-bitcoin-wallets-need-two-factor-authentication-160474. [Accessed 2 7 2018].

[117] S. Higgins, "BTER Claims $1.75 Million in Bitcoin Stolen in Cold Wallet Hack," Coindesk, 15 2 2015. [Online]. Available: https://www.coindesk.com/bter-bitcoin-stolen-cold-wallet-hack/. [Accessed 22 5 2018].

[118] I. Demartino, "Chinese Exchange KipCoin Has Been Hacked," Coin Journal, 17 2 2015. [Online]. Available: https://coinjournal.net/chinese-exchange-kipcoin-hacked/. [Accessed 2 7 2018].

[119] J. BUNTINX, "Chinese Exchange Platform KipCoin Admits To Hackers Stealing Over 3,000 Bitcoin," Digital Money Times, 18 2 2015. [Online]. Available: http://digitalmoneytimes.com/chinese-exchange-platform-kipcoin-admits-to-hackers-stealing-over-3000-bitcoin/. [Accessed 2 7 2018].

[120] L. Munson, "Hackers force closure of Canadian Bitcoin exchange Cavirtex," Naked Security, 19 2 2015. [Online]. Available: https://nakedsecurity.sophos.com/2015/02/19/hackers-force-closure-of-canadian-bitcoin-exchange-cavirtex/. [Accessed 30 6 2018].

[121] N. DOLLENTAS, "BITCOIN EXCHANGE CAVIRTEX SHUT'S DOWN AFTER DATABASE HACK LEAVES USER DATA EXPOSED," 20 2 2015. [Online]. Available: http://bitcoinist.com/bitcoin-exchange-cavirtex-shuts-database-hack-leaves-user-data-exposed/. [Accessed 23 5 2018].

[122] C. Osborne, "Bitcoin exchange Cryptoine hacked," 26 3 2015. [Online]. Available: https://www.zdnet.com/article/bitcoin-exchange-cryptoine-hacked/. [Accessed 23 5 2018].

[123] I. MUSCAT, "Lessons to Learn from the AllCrypt Hack," Acunetix, 25 3 2015. [Online]. Available: https://www.acunetix.com/blog/articles/lessons-to-learn-from-the-allcrypt-hack/. [Accessed 23 5 2018].

[124] P. Rizzo, "Coinapult Claims $40k Lost in Hot Wallet Compromise," Coin Desk, 17 3 2015. [Online]. Available: https://www.coindesk.com/coinapult-loses-40k-hot-wallet-compromise/. [Accessed 2 7 2018].

[125] A. Beikverdi, "150BTC Coinapult Hack Renews Doubts About Security Fundamentals," Coin Telegraph, 19 3 2015. [Online]. Available: https://cointelegraph.com/news/150btc-coinapult-hack-renews-doubts-about-security-fundamentals. [Accessed 30 6 2018].

[126] K. DOTSON, "Bitfinex Bitcoin exchange hot wallet hacked, estimated 1474 BTC stolen," 24 5 2015. [Online]. Available: https://siliconangle.com/blog/2015/05/24/bitfinex-bitcoin-exchange-hot-wallet-hacked-estimated-1474-btc-stolen/. [Accessed 23 5 2018].

[127] W. Amir, "Hackers target Bitcoin Exchange BitFinex' Hot Wallet," Hack Read, 25 5 2015. [Online]. Available: https://www.hackread.com/bitcoin-exchange-bitfinex-hot-wallet-hacked/. [Accessed 2 7 2018].

[128] D. Pauli, "Hackers sell 79,267 Cloudminr accounts for ONE Bitcoin," The Register, 14 7 2015. [Online]. Available: https://www.theregister.co.uk/2015/07/14/cloudminr_hack_80000_bitcoin_miners_exposed/. [Accessed 19 4 2018].

[129] B. N. -. Unknown, "cloudminr io hacked 80000 profiles compromised," Live Bitcoin News, 2015. [Online]. Available: http://www.livebitcoinnews.com/cloudminr-io-hacked-80000-profiles-compromised/. [Accessed 19 4 2018].

[130] D. Shares, "Names, phone numbers, and emails leaked in BitQuick exchange hack," Bitcoin.com, 7 4 2016. [Online]. Available: https://news.bitcoin.com/names-phone-numbers-emails-leaked-bitquick-exchange-hack/. [Accessed 3 7 2018].

[131] S. Higgins, "Bitcoin Exchange Cointrader Shuts Down After Alleged Hack," Coindesk, 30 3 2016. [Online]. Available: https://www.coindesk.com/bitcoin-exchange-cointrader-shuts-down/. [Accessed 2 6 2018].

[132] Traderman, "Coinwallet Announces Shutdown Following Data Breach," 6 4 2016. [Online]. Available: https://themerkle.com/coinwallet-co-announces-shutdown-following-data-breach/. [Accessed 26 5 2018].

[133] D. Shares, "Coinwallet.co bitcoin wallet hacked, is closing down," Bitcoin.com, 8 4 2016. [Online]. Available: https://news.bitcoin.com/coinwallet-co-bitcoin-wallet-hacked-closing/. [Accessed 2 6 2018].

[134] S. Higgins, "ShapeShift Lost $230k in String of Thefts, Report Finds," 18 4 2016. [Online]. Available: https://www.coindesk.com/digital-currency-exchange-shapeshift-says-lost-230k-3-separate-hacks/. [Accessed 3 7 2018].

[135] Emily, "A Timeline: ShapeShift Hacking Incident," Shape Shift, 19 4 2016. [Online]. Available: https://info.shapeshift.io/blog/2016/04/19/timeline-shapeshift-hacking-incident. [Accessed 3 7 2018].

[136] E. Voorhees, "Looting of the Fox: The Story of Sabotage at ShapeShift," Abra, 19 4 2016. [Online]. Available: https://news.bitcoin.com/looting-fox-sabotage-shapeshift/. [Accessed 3 7 2018].

[137] S. Falkon, "The Story of the DAO—Its History and Consequences," Medium, 24 12 2017. [Online]. Available: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee. [Accessed 22 4 2018].

[138] D. Shares, "Coinkite discloses that they leaked a copy of their user database," 6 5 2016. [Online]. Available: https://bitcoinexchangeguide.com/coinkite-coldcard/. [Accessed 25 5 2018].

[139] D. Shares, "Coinkite discloses that they leaked a copy of their user database," Bitcoin.com, 6 5 2016. [Online]. Available: https://news.bitcoin.com/coinkite-discloses-leaked-copy-user-database/. [Accessed 25 5 2018].

[140] A. Mizrahi, "Gatecoin Lost $2m Worth of Bitcoin and Ethereum In Hot Wallet Cyber Hack," Finance Magnates, 15 5 2016. [Online]. Available: https://www.financemagnates.com/cryptocurrency/exchange/gatecoin-lost-2m-worth-bitcoin-ethereum-hot-wallet-cyber-hack/. [Accessed 20 4 2018].

[141] S. Higgins, "Gatecoin Claims $2 Million in Bitcoins and Ethers Lost in Security Breach," Coindesk, 16 5 2016. [Online]. Available: https://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach/. [Accessed 20 4 2018].

[142] S. Higgins, "Digital Currency Exchange Gatecoin Offline After Loss of Funds," Coin Desk, 13 5 2016. [Online]. Available: https://www.coindesk.com/digital-currency-exchange-gatecoin-reportedly-loses-customer-funds-hack/. [Accessed 19 4 2018].

[143] W. Suberg, "Steemit Hacked for ‘$85,000’ as Users Complain of Weak Security," Bitcoin.com, 14 7 2016. [Online]. Available: https://news.bitcoin.com/steemit-hacked-weak-security/. [Accessed 3 7 2018].

[144] Wikipedia, "Bitgo," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/BitGo. [Accessed 19 4 2018].

[145] S. Higgins, "The Bitfinex Bitcoin Hack: What We Know (And Don't Know)," Coin Desk, 3 8 2016. [Online]. Available: https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/. [Accessed 19 4 2018].

[146] D. Shares, "Bitcurex Forced to Shut Down After $1.5 million Theft," Bitcoin.com, 28 10 2016. [Online]. Available: https://news.bitcoin.com/bitcurex-forced-million-theft/. [Accessed 19 4 2018].

[147] B. Exchange, "Polish Bitcoin Exchange Bitcurex Goes Offline After Losing Assets; Questions Loom Over Loss of 2300 BTC," Bitcoin Exchange, 28 10 2016. [Online]. Available: https://www.ccn.com/polish-bitcoin-exchange-bitcurex-goes-offline-losing-assets-questions-loom-loss-2300-btc/. [Accessed 20 4 2018].

[148] W. Suberg, "Bitcurex: Owner ‘Disappears’ After Failing to Return 2,300 BTC," Bitcoinist, 31 1 2017. [Online]. Available: http://bitcoinist.com/bitcurex-owner-disappears-2300-btc/. [Accessed 20 4 2018].

[149] S. Khatwani, "Zcoin (XZC) Cryptocurrency: Everything Beginners Need To Know," Coinstura, 1 2 2018. [Online]. Available: https://coinsutra.com/zcoin-xzc-zercoin/. [Accessed 20 4 2018].

[150] R. Price, "A single typo let hackers steal $400,000 from a bitcoin rival," Business Insider, 20 2 2017. [Online]. Available: http://www.businessinsider.com/typo-bitcoin-rival-zcoin-attacker-steals-400000-2017-2. [Accessed 20 4 2018].

[151] P. Insom, "Zcoin’s Zerocoin bug explained in detail," Zcoin, 21 2 2017. [Online]. Available: https://zcoin.io/zcoins-zerocoin-bug-explained-in-detail/. [Accessed 20 4 2018].

[152] W. Suberg, "Zerocoin Hacker “Creates” and Spends 370,000 Tokens Worth 410 BTC," Coin Telegraph, 21 2 2017. [Online]. Available: https://cointelegraph.com/news/zerocoin-hacker-creates-and-spends-370000-tokens-worth-410-btc. [Accessed 5 7 2018].

[153] W. Amir, "South Korean Bitcoin Exchange Yapizon Hacked; $5 Million Stolen," Hack Read, 29 4 2017. [Online]. Available: https://www.hackread.com/south-korean-bitcoin-exchange-yapizon-hacked. [Accessed 5 7 2018].

[154] A. Sunkara, "Wallet Hacks: How a Person Lost Over $300,000 Due to Simple Mistakes," Coindol, 4 9 2017. [Online]. Available: https://coinidol.com/wallet-hacks-how-person-lost-funds/. [Accessed 22 4 2018].

[155] VxLabs, "Extracting the Jaxx 12-word wallet backup phrase," vxLabs, 10 6 2017. [Online]. Available: https://vxlabs.com/2017/06/10/extracting-the-jaxx-12-word-wallet-backup-phrase/. [Accessed 20 4 2018].

[156] E. Faggart, "Jaxx Wallet Vulnerability Puts Your Bitcoin At Risk: Update From Jaxx," Bitsonline, 10 6 2017. [Online]. Available: https://bitsonline.com/jaxx-vulnerability-bitcoin-risk/. [Accessed 22 4 2018].

[157] B. Security, "Users Report Losing $400,000 Due to Jaxx Wallet Vulnerability," CNN, 12 6 2017. [Online]. Available: https://www.ccn.com/users-report-losing-400000-due-to-jaxx-wallet-vulnerability/. [Accessed 21 4 2018].

[158] b. dutton, "BREAKING: The Biggest Canadian Coin Exchange - QuadrigaCX -- loses 67,000 $ETH !! Due to Coding Error - Funds Locked in an Executable Contract Now!," Steem It, 3 6 2017. [Online]. Available: https://steemit.com/cryptocurrency/@barrydutton/breaking-the-biggest-canadian-coin-exchange-quadrigacx-loses-67-000-usdeth-due-to-coding-error-funds-locked-in-an-executable. [Accessed 8 7 2018].

[159] S. Higgins, "Ethereum Client Update Issue Costs Cryptocurrency Exchange $14 Million," Coin Desk, 2 6 2017. [Online]. Available: https://www.coindesk.com/ethereum-client-exchange-14-million/. [Accessed 8 7 2018].

[160] R. Price, "One of the world's biggest bitcoin exchanges has been hacked," Business Insider, 5 7 2017. [Online]. Available: http://www.businessinsider.com/south-korean-bitcoin-exchange-bithumb-hacked-ethereum-2017-7. [Accessed 20 4 2018].

[161] Y. J. Kim, "Virtual currency exchange 'Bitsum' hacking accidents, withdrawals were made.," Seoul Economy, 13 12 2017. [Online]. Available: http://www.sedaily.com/NewsView/1OOU97FCBA. [Accessed 20 4 2018].

[162] K. S. Park, "Virtual Money Exchange 'Bitsum' staff hacking PC, leakage of customer information "Concerns about second damages ..."," Joong Ang news paper, 3 7 2017. [Online]. Available: http://news.joins.com/article/21720927. [Accessed 6 7 2018].

[163] W. Zhao, "$7 Million Lost in CoinDash ICO Hack," Coin Desk, 17 7 2017. [Online]. Available: https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/. [Accessed 22 4 2018].

[164] N. De, "Hacks, Scams and Attacks: Blockchain's 2017 Disasters," Coin Desk, 29 12 2017. [Online]. Available: https://www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters/. [Accessed 20 4 2018].

[165] W. Zhao, "$30 Million: Ether Reported Stolen Due to Parity Wallet Breach," Coin Desk, 19 7 2017. [Online]. Available: https://www.coindesk.com/30-million-ether-reported-stolen-parity-wallet-breach/. [Accessed 22 4 2018].

[166] H. Qureshi, "A hacker stole $31M of Ether—how it happened, and what it means for Ethereum," Free Code Camp, 20 7 2017. [Online]. Available: https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce. [Accessed 20 4 2018].

[167] P. D. A. J. E. G. S. Lorenz Breidenbach, "An In-Depth Look at the Parity Multisig Bug," Hacking Distributed, 22 7 2017. [Online]. Available: http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/. [Accessed 25 4 2018].

[168] J. Samuel, "Ether Coins Stolen From Enigma," Coin Stocks, 30 8 2017. [Online]. Available: http://coinstocks.com/ether-coins-stolen-from-enigma/. [Accessed 22 4 2018].

[169] J. P. Mullin, "Enigma’s Hack: $500,000 of Ether Stolen, Accounts Compromised," Cointelegraph, 22 8 2017. [Online]. Available: https://cointelegraph.com/news/enigmas-hack-500000-of-ether-stolen-accounts-compromised. [Accessed 25 4 2018].

[170] A. Akentiev, "Parity Multisig Hacked. Again," Medium, 8 11 2017. [Online]. Available: https://medium.com/chain-cloud-company-blog/parity-multisig-hack-again-b46771eaa838. [Accessed 29 4 2014].

[171] T. Ong, "Tether says nearly $31 million worth of its digital tokens have been stolen after hack," The Verge, 21 11 2017. [Online]. Available: https://www.theverge.com/2017/11/21/16684296/tether-cryptocurrency-stolen-30-million-hack. [Accessed 20 4 2018].

[172] L. Nguyen, "NiceHash CEO speaks out after $60m cryptocurrency hack," Wikitribune, 11 12 2017. [Online]. Available: https://www.wikitribune.com/story/2017/12/11/technology/nicehash-ceo-speaks-out-after-60m-cryptocurrency-hack/27212/. [Accessed 22 4 2018].

[173] S. Higgins, "Cryptocurrency Mining Market NiceHash Hacked," Coin Desk, 6 12 2017. [Online]. Available: https://www.coindesk.com/62-million-gone-cryptocurrency-mining-market-nicehash-hacked/. [Accessed 20 4 2018].

[174] R. Browne, "More than $60 million worth of bitcoin potentially stolen after hack on cryptocurrency site," CNBC, 7 12 2017. [Online]. Available: https://www.cnbc.com/2017/12/07/bitcoin-stolen-in-hack-on-nicehash-cryptocurrency-mining-marketplace.html. [Accessed 20 4 2018].

[175] K. o. Security, "Former Botmaster, ‘Darkode’ Founder is CTO of Hacked Bitcoin Mining Firm ‘NiceHash’," Kerbs on Security, 15 12 2017. [Online]. Available: https://krebsonsecurity.com/2017/12/former-botmaster-darkode-founder-is-cto-of-hacked-bitcoin-mining-firm-nicehash/. [Accessed 30 4 2018].

[176] W. R. Kim, "'Youbit bankruptcy' causes poor security consciousness ... other exchange assets 70% offline storage," eToday, 20 12 2017. [Online]. Available:

http://www.etoday.co.kr/news/section/newsview.php?idxno=1576106. [Accessed 29 4 2018].

[177] K. U. L. Ho Chul Sung, "Virtual currency exchange 'Youbit', bankruptcy in hacking," Chosun Daily News, 20 12 2017. [Online]. Available: http://news.chosun.com/site/data/html_dir/2017/12/20/2017122000385.html. [Accessed 20 4 2018].

[178] S. Gordon, "BlackWallet Hacked: Warns Stellar Community Not to Log In to Site," Bitcoin Magazine, 24 3 2018. [Online]. Available: https://bitcoinmagazine.com/articles/blackwallet-hacked-warns-stellar-community-not-log-site/. [Accessed 21 7 2018].

[179] C. Osborne, "$400,000 stolen in Lumens BlackWallet theft," ZDNet, 24 3 2018. [Online]. Available: http://www.zdnet.com/article/400000-stolen-in-lumens-blackwallet-theft/. [Accessed 21 7 2018].

[180] Bloomberg, "How to Steal $500 Million in Cryptocurrency," Fortune, 31 1 2018. [Online]. Available: http://fortune.com/2018/01/31/coincheck-hack-how/. [Accessed 20 4 2018].

[181] L. S. Stephens, "Cold Wallet Vs. Hot Wallet: What’s The Difference?," Medium, 9 4 2017. [Online]. Available: https://medium.com/dash-for-newbies/cold-wallet-vs-hot-wallet-whats-the-difference-a00d872aa6b1. [Accessed 20 4 2018].

[182] H. Partz, "Coincheck: NEM Foundation Stops Tracing Stolen Coins, Hackers’ Account At Zero," cointelegraph, 23 3 2018. [Online]. Available: https://cointelegraph.com/news/coincheck-nem-foundation-stops-tracing-stolen-coins-hackers-account-at-zero. [Accessed 30 4 2018].

[183] G. Rocco, "BITGRAIL CRYPTOCURRENCY EXCHANGE HACKED, $170 MILLION IN NANO ALLEGEDLY STOLEN," Bitcoinist, 11 2 2018. [Online]. Available: https://bitcoinist.com/bitgrail-cryptocurrency-exchange-hacked-170-million-nano-allegedly-stolen/. [Accessed 7 7 2018].

[184] R. McIntosh, "$170 Million Mistake: BitGrail May Have Been Aware of Bug that Led to Hack," Finance Magnates, 14 2 2018. [Online]. Available: https://www.financemagnates.com/cryptocurrency/news/170-million-mistake-bitgrail-may-aware-bug-led-hack/. [Accessed 7 7 2018].

[185] N. De, "Bee Token ICO Stung by $1 Million Phishing Scam," Coin Desk, 1 2 2018. [Online]. Available: https://www.coindesk.com/bee-token-phishing-scam/. [Accessed 7 7 2018].

[186] S. Town, "BEE Token Sale A Honeypot For Hackers," Crypto Briefing, 1 2 2018. [Online]. Available: https://cryptobriefing.com/bee-token-sale-honeypot-hackers/. [Accessed 7 7 2018].

[187] A. Abdel-Qader, "Indian Bitcoin Exchange Coinsecure Claims $3.5 Million Lost in Insider Hack," Finance magnates, 13 4 2018. [Online]. Available: https://www.financemagnates.com/cryptocurrency/news/indian-bitcoin-exchange-coinsecure-claims-%E2%80%8E3-5-million-%E2%80%8Elost-insider-hack/. [Accessed 7 7 2018].

[188] C. Osborne, "Coinsecure, not so secure: Millions in cryptocurrency stolen, CSO blamed," ZDNet, 13 4 2018. [Online]. Available:

https://www.zdnet.com/article/coinsecure-not-so-secure-millions-in-cryptocurrency-stolen-cso-branded-as-thief/. [Accessed 7 7 2018].

[189] T. Fox-Brewster, "A $152,000 Cryptocurrency Theft Just Exploited A Huge 'Blind Spot' In Internet Security," Forbes, 24 4 2018. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2018/04/24/a-160000-ether-theft-just-exploited-a-massive-blind-spot-in-internet-security/#9b8aff5e26bd. [Accessed 7 7 2018].

[190] M. Huillet, "MyEtherWallet Warns That A “Couple” Of Its DNS Servers Have Been Hacked," Coin Telegraph, 24 4 2018. [Online]. Available: https://cointelegraph.com/news/myetherwallet-warns-that-a-couple-of-its-dns-servers-have-been-hacked. [Accessed 7 7 2018].

[191] J. Russell, "Korean crypto exchange Coinrail loses over $40M in tokens following a hack," Tech Crunch, 11 6 2018. [Online]. Available: https://techcrunch.com/2018/06/10/korean-crypto-exchange-coinrail-loses-over-40m-in-tokens-following-a-hack/?guccounter=1. [Accessed 7 7 2018].

[192] J.-y. Lee, "My tokens evaporated 40 billion ... To prevent a second coin rail incident," Blockchain News, 12 6 2018. [Online]. Available: http://www.blockchainnews.co.kr/news/view.php?idx=1366. [Accessed 7 7 2018].

[193] K. Helms, "Report: Suspicious Transactions at Korean Exchange Coinrail Months Before Hack," Bitcoin.com, 12 6 2018. [Online]. Available: https://news.bitcoin.com/suspicious-transactions-korean-exchange-coinrail-hack/. [Accessed 7 7 2018].

[194] J. Wilmoth, "Breaking: South Korean Crypto Exchange Bithumb Hacked, Thieves Steal $30 Million," CCN, 20 6 2018. [Online]. Available: https://www.ccn.com/breaking-south-korean-crypto-exchange-bithumb-hacked-thieves-steal-30-million/. [Accessed 7 7 2017].

[195] W. Zhao, "Bithumb $31 Million Crypto Exchange Hack: What We Know (And Don't)," Coin Desk, 20 6 2018. [Online]. Available: https://www.coindesk.com/bithumb-exchanges-31-million-hack-know-dont-know/. [Accessed 7 7 2018].

[196] M. Nadeau, "State of Cybercrime 2017: Security events decline, but not the impact," CSO, 28 7 2017. [Online]. Available: https://www.csoonline.com/article/3211491/security/state-of-cybercrime-2017-security-events-decline-but-not-the-impact.html#tk.cso_fsb. [Accessed 15 4 2018].

[197] Wikipedia, "Zero-day (computing)," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Zero-day_(computing). [Accessed 15 10 2018].

[198] BullGuard, "What are zero-day attacks?," BullGuard, [Online]. Available: https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-are-zero-day-attacks.aspx. [Accessed 15 10 2018].

[199] G. Chavez-Dreyfuss, "Cyber threat grows for bitcoin exchanges," Reuters, New York, 2016.

[200] N. De, "Hacks, Scams and Attacks: Blockchain's 2017 Disasters," coindesk, 29 12 2017. [Online]. Available: https://www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters/. [Accessed 1 6 2018].

[201] Reuters, "Risk of Bitcoin Hacks and Losses Is Very Real," fortune, 29 08 2016. [Online]. Available: http://fortune.com/2016/08/29/risk-of-bitcoin-hacking-is-real/. [Accessed 31 12 2017].

[202] C. E. Hacker, "The Phases of Ethical Hacking," Certified Ethical Hacker, 8 2011. [Online]. Available: http://certifiedethicalhackerceh.blogspot.com/2011/08/phases-of-ethical-hacking.html. [Accessed 10 8 2018].

[203] Investopedia, "51% Attack," Investopedia, [Online]. Available: https://www.investopedia.com/terms/1/51-attack.asp. [Accessed 10 12 2018].

[204] D. Bradbury, "What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability," Coin Desk, 15 2 2014. [Online]. Available: https://www.coindesk.com/bitcoin-bug-guide-transaction-malleability. [Accessed 18 12 2018].

[205] J. Frankenfield, "Double-Spending," Investopedia, 5 7 2018. [Online]. Available: https://www.investopedia.com/terms/d/doublespending.asp. [Accessed 10 12 2018].

[206] S. Beyer, "Security of blockchain-based smart contracts II – Known Vulnerabilities and Pitfalls," 20 3 2018. [Online]. Available: https://www.securityartwork.es/2018/03/20/security-of-blockchain-based-smart-contracts-ii-known-vulnerabilities-and-pitfalls/. [Accessed 15 12 2018].

[207] Aprorit, "Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology," Aprorit, [Online]. Available: https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors. [Accessed 24 12 2018].

[208] M. Rouse, "DNS attack," Search Security, 9 5 2018. [Online]. Available: https://searchsecurity.techtarget.com/definition/DNS-attack. [Accessed 15 12 2018].

[209] L. Ankney, "Hot Wallets vs Cold Wallets—What to Know," A Medium Corporation, 30 1 2018. [Online]. Available: https://medium.com/@CryptoLeslie/hot-wallets-vs-cold-wallets-what-to-know-2030d858421e. [Accessed 15 12 2018].

[210] OWASP, "SQL Injection," 10 4 2016. [Online]. Available: https://www.owasp.org/index.php/SQL_Injection. [Accessed 28 12 2018].

[211] BlockCAT, "Medium Corporation," Medium Corporation, [Online]. Available: https://medium.com/blockcat/on-the-parity-multi-sig-wallet-attack-83fb5e7f4b8c. [Accessed 15 12 2018].

[212] Reentrancy, "Ethereum Smart Contract Best Practices," Ethereum Smart Contract Best Practices, [Online]. Available: https://consensys.github.io/smart-contract-best-practices/known_attacks/. [Accessed 25 12 2018].

[213] J. Hannan, "Introduction to Smart Contract and DApp Security," Medium Corporation, 20 2 2018. [Online]. Available: https://medium.com/modular-network/introduction-to-smart-contract-and-dapp-security-556502629d54. [Accessed 24 12 2018].

[214] Deloitte, "Prevention of DDoS attacks," Deloitte, [Online]. Available: https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/cyber-security-prevention-of-ddos-attacks-with-blockchain-technology.html. [Accessed 15 12 2018].

[215] A. Manning, "Solidity Security: Comprehensive list of known attack vectors and common anti-patterns," Sigma Prime, 20 10 2018. [Online]. Available: https://blog.sigmaprime.io/solidity-security.html. [Accessed 25 12 2018].

[216] G. Konstantopoulos, "How to Secure Your Smart Contracts: 6 Solidity Vulnerabilities and how to avoid them (Part 1)," Medium Corporation, 8 1 2018. [Online]. Available: https://medium.com/loom-network/how-to-secure-your-smart-contracts-6-solidity-vulnerabilities-and-how-to-avoid-them-part-1-c33048d4d17d. [Accessed 26 12 2018].

[217] OWSP, "Testing for AJAX Vulnerabilities (OWASP-AJ-001)," OWASP, [Online]. Available: https://www.owasp.org/index.php/Testing_for_AJAX_Vulnerabilities_(OWASP-AJ-001)#Cross_Site_Scripting. [Accessed 24 12 2018].

[218] S. Shah, "Top 10 Web 2.0 attack vectors," [Online]. Available: https://infosecwriters.com/text_resources/pdf/SShah_Web20.pdf. [Accessed 24 12 2018].

[219] C. G. Inc., "What is a Malware Attack?," Comodo Group Inc., [Online]. Available: https://enterprise.comodo.com/what-is-a-malware-attack.php. [Accessed 26 12 2018].

[220] OWASP, "Session hijacking attack," OWASP, 14 8 2014. [Online]. Available: https://www.owasp.org/index.php/Session_hijacking_attack. [Accessed 29 12 2018].

[221] Forcepint, "What is a Phishing Attack?," Forcepoint, [Online]. Available: https://www.forcepoint.com/cyber-edu/phishing-attack. [Accessed 29 12 2018].

[222] Noction, "BGP Hijacking overview. Routing incidents prevention and defense mechanisms. (Updated)," Noction, 24 4 2018. [Online]. Available: https://www.noction.com/blog/bgp-hijacking. [Accessed 26 12 2018].

[223] S. M. Hami Salim, "Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks," Sloan School of Management at MIT, Boston, 2014.

[224] N. G. Leveson, Analyzing Accidents and Incidents (CAST) in Engineering a Safer World: Systems Thinking Applied to Safety, Cambridge: The MIT Press, 2011, pp. 350-390.

[225] S. M. Hamid Salim, "Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks," in *Composite Information Systems Laboratory (CISL)*, Boston, 2014.

[226] Wikipedia, "Ethereum," Wikipedia, 2 7 2018. [Online]. Available: https://en.wikipedia.org/wiki/Ethereum. [Accessed 9 7 2018].

[227] M. Araoz, "The Hitchhiker's Guide to Smart Contracts in Ethereum," Zepplin, 29 7 2016. [Online]. Available: https://blog.zeppelin.solutions/the-hitchhikers-guide-to-smart-contracts-in-ethereum-848f08001f05. [Accessed 9 7 2018].

[228] Investopedia, "Decentralized Applications or dApps," Investopedia, [Online]. Available: https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp. [Accessed 9 7 2018].

[229] H. Georgiev, "The hack that changed the blockchain perspective," MWR Information Security, 11 8 2016. [Online]. Available: https://labs.mwrinfosecurity.com/blog/the-hack-that-changed-the-blockchain-perspective/. [Accessed 9 7 2018].

[230] T. K. Sharma, "Details Of The Dao Hacking In Ethereum In 2016," Blockchain Council, 20 8 2017. [Online]. Available: https://www.blockchain-

council.org/blockchain/details-of-the-dao-hacking-in-ethereum-in-2016/. [Accessed 9 7 2018].

[231] M. d. Castillo, "The DAO: Or How A Leaderless Ethereum Project Raised $50 Million," Coin Desk, 12 5 2016. [Online]. Available: https://www.coindesk.com/the-dao-just-raised-50-million-but-what-is-it/. [Accessed 2 10 2018].

[232] S. Bannon, "The Tao of “The DAO” or: How the autonomous corporation is already here," 16 5 2016. [Online]. Available: https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/. [Accessed 4 10 2018].

[233] R. Waters, "Automated company raises equivalent of $120M in digital currency," 17 5 2016. [Online]. Available: https://www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html. [Accessed 2 10 2018].

[234] K. Finley, "A $50 Million Hack Just Showed That The Dao Was All Too Human," Wired, 18 6 2016. [Online]. Available: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human. [Accessed 9 7 2018].

[235] A. Hertig, "What is a DAO?," Coin Desk, [Online]. Available: https://www.coindesk.com/information/what-is-a-dao-ethereum/. [Accessed 8 7 2018].

[236] Kate, "What Is The DAO and Why Is It the Biggest Crowdfunding Project in History?," Medici, 29 5 2016. [Online]. Available: https://gomedici.com/what-is-the-dao-and-why-is-it-the-biggest-crowdfunding-project-in-the-history/. [Accessed 9 7 2018].

[237] C. Jentzsch, "Decentralized autonomous organization to automate governance," Slock.it, 2016.

[238] S. Dingle, "The company of the future: a beginner’s guide to the DAO," Medium, 18 5 2016. [Online]. Available: https://medium.com/@simondingle/the-company-of-the-future-a-beginners-guide-to-the-dao-112b8855d9ca. [Accessed 9 7 2018].

[239] Slock.it, "Understanding the DAO accounting," Slock.it, [Online]. Available: https://github.com/slockit/DAO/wiki/Understanding-the-DAO-accounting. [Accessed 10 12 2018].

[240] T. Simonite, "The “Autonomous Corporation” Called the DAO Is Not a Good Way to Spend $130 Million," 18 5 2016. [Online]. Available: https://www.technologyreview.com/s/601480/the-autonomous-corporation-called-the-dao-is-not-a-good-way-to-spend-130-million/. [Accessed 2 10 2018].

[241] M. E. Peck, "Ethereum’s $150-Million Blockchain-Powered Fund Opens Just as Researchers Call For a Halt," IEEE, 28 5 2016. [Online]. Available: https://spectrum.ieee.org/tech-talk/computing/networks/ethereums-150-million-dollar-dao-opens-for-business-just-as-researchers-call-for-a-moratorium. [Accessed 01 10 2018].

[242] E. Lemmerman, "Lessons Learned from theDAO Project: The Future of Regulating Blockchain," 23 8 2016. [Online]. Available: http://www.nira.or.jp/pdf/20160823theDAO.pdf. [Accessed 8 7 2018].

[243] M. d. Castillo, "Cornell Professor Calls for 'DAO 2.0' Movement," 22 6 2016. [Online]. Available: https://www.coindesk.com/cornell-prof-discovered-dao-vulnerability-reveals-10-exploits/. [Accessed 9 7 2018].

[244] G. Greenspan, "Smart contracts and the DAO implosion," 22 6 2016. [Online]. Available: https://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/. [Accessed 8 7 2018].

[245] L. Mearian, "How blockchain will underpin the new trust economy," 7 12 2017. [Online]. Available: https://www.computerworld.com/article/3240906/security/how-blockchain-will-underpin-the-new-trust-economy.html. [Accessed 8 7 2018].

[246] L. Coleman, "DAO Vulnerability Raises Questions of Trust and the Human Factor," 24 6 2016. [Online]. Available: https://www.ccn.com/dao-vulnerability-trust-human-factor/. [Accessed 9 7 2018].

[247] D. Siegel, "Understanding The DAO Hack for Journalists," 17 6 2016. [Online]. Available: https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993. [Accessed 9 7 2018].

[248] V. Z. E. G. S. Dino Mark, "A Call for a Temporary Moratorium on “The DAO”," 30 5 2016. [Online]. Available: https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWyS-dQ4lsBacR2dUgGTtV98C40/edit#heading=h.exdzp88avpn4. [Accessed 8 7 2018].

[249] S. Palladino, "Designing the architecture for your Ethereum application," Zeppelin, 21 11 2017. [Online]. Available: https://blog.zeppelin.solutions/designing-the-architecture-for-your-ethereum-application-9cec086f8317. [Accessed 21 5 2018].

[250] Sebfor, "The DAO Hack – Recap of What Happened," Sebfor, 28 5 2016. [Online]. Available: http://sebfor.com/the-dao-hack-recap-of-what-happened/. [Accessed 10 7 2018].

[251] V. Z. E. G. S. Dino Mark, "A Call for a Temporary Moratorium on The DAO," Hacking Distributed, 27 5 2016. [Online]. Available: http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/. [Accessed 10 7 2018].

[252] Croocroo, "Slock.it DAO Security Proposal (v1.0 - Revised/Redux)," 7 5 2016. [Online]. Available: https://dao.consider.it/slockit-dao-security-proposal-revisedredux?results=true. [Accessed 9 7 2018].

[253] slacknation, "DAO hack timeline," 21 6 2016. [Online]. Available: https://medium.com/@slacknation/dao-hack-timeline-823e5a18e894. [Accessed 9 7 2018].

[254] P. Vessenes, "More Ethereum Attacks: Race-To-Empty is the Real Deal," 9 6 2016. [Online]. Available: https://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/. [Accessed 9 7 2018].

[255] C. Reitwiessner, "Smart Contract Security," Ethereum Blog, 10 6 2016. [Online]. Available: https://blog.ethereum.org/2016/06/10/smart-contract-security/. [Accessed 9 7 2018].

[256] i3nikolai, "Critical ether token wrapper vulnerability - ETH tokens salvaged from potential attacks," Reddit, 10 6 2016. [Online]. Available: https://www.reddit.com/r/MakerDAO/comments/4niu10/critical_ether_token_wrapper_vulnerability_eth/. [Accessed 9 7 2018].

[257] C. Jentzsch, "The History of the DAO and Lessons Learned," 24 8 2016. [Online]. Available: https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5. [Accessed 24 5 2018].

[258] D. Siegel, "Understanding The DAO Hack for Journalists," Medium, 19 6 2016. [Online]. Available: https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993. [Accessed 23 5 2018].

[259] S. Tual, "No DAO funds at risk following the Ethereum smart contract ‘recursive call’ bug discovery," Slock.it, 12 6 2016. [Online]. Available: https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smartcontract-recursive-call-bug-discovery-29f482d348b.

[260] Etherscan, "Transaction," Etherscan, 14 6 2016. [Online]. Available: https://etherscan.io/tx/0x0b5dfbbce4c4dad6eb92c0790fa9903cd7f27e70d9cadcd6aa30a63c0c11f7d6. [Accessed 12 5 2018].

[261] Transaction, "Etherscan," Etherscan, 14 6 2016. [Online]. Available: https://etherscan.io/tx/0xf0daeb80b0635bc78eb724660d8788c6758ffe7f5ce705c943121c43b388d7f0. [Accessed 22 5 2018].

[262] Etherscan, "Transaction," Etherscan, 14 6 2016. [Online]. Available: https://etherscan.io/tx/0xc017561624884dff6916f1e4e6f450cd1ccefc0c922727eccb8ed791e224c0e2. [Accessed 10 7 2018].

[263] Etherscan, "Transaction," Etherscan, 15 6 2016. [Online]. Available: https://etherscan.io/tx/0xb5ff2d7a165baba4ca8d7bf8223af9dcf956ec6a4f4f85dbdd3ebea0111251ed. [Accessed 10 7 2018].

[264] Etherscan, "Transaction," Etherscan, 15 6 2016. [Online]. Available: https://etherscan.io/tx/0x1de9b7db4d55af395518b83a49dafe0c37cb746e840ce9d4bc367cb050dbe6ac. [Accessed 10 7 2018].

[265] A. M. Zikai Alex Wen, "Scanning Live Ethereum Contracts for the "Unchecked-Send" Bu," Hacking Distributed, 16 6 2016. [Online]. Available: http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/. [Accessed 10 7 2018].

[266] Etherscan, "Transaction," Etherscan, 17 6 2016. [Online]. Available: https://etherscan.io/tx/0x0ec3f2488a93839524add10ea229e773f6bc891b4eb4794c3337d4495263790b. [Accessed 10 7 2018].

[267] ledgerwatch, "I think TheDAO is getting drained right now," Reddit, 17 6 2016. [Online]. Available: https://www.reddit.com/r/ethereum/comments/4oi2ta/i_think_thedao_is_getting_drained_right_now/. [Accessed 22 5 2018].

[268] vbulletin, "I think TheDAO is getting drained right now," Reddit, 17 6 2016. [Online]. Available: https://www.reddit.com/r/ethereum/comments/4oi2ta/i_think_thedao_is_getting_drained_right_now/d4csoa8/. [Accessed 22 5 2018].

[269] A. Quentson, "Ether Price Plumets; Ethereum DAO May Be Hacked," CCN, 17 6 2016. [Online]. Available: https://www.ccn.com/ether-price-plumets-ethereum-dao-may-be-hacked/. [Accessed 11 7 2018].

[270] Etherscan, "Transaction," Etherscan, 17 6 2016. [Online]. Available: https://etherscan.io/tx/0xa348da60799bff3ca804b3e49c96edebea44c5728a97f64bec3e21056d42f6e3. [Accessed 22 5 2018].

[271] V. Buterin, "Critical Update Re:DAO Vulnerability," Ethereum, 17 6 2016. [Online]. Available: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/. [Accessed 11 5 2018].

[272] A. Amsel, "Understanding Proposed Ethereum Forks," Medium, 18 6 2016. [Online]. Available: https://medium.com/ownage/understanding-proposed-ethereum-forks-6abd63a478fc. [Accessed 11 7 2017].

[273] R. H., "The DAO - The story of the second biggest cryptocurrecy heist," 23 6 2016. [Online]. Available: https://docs.google.com/presentation/d/1b78bxx_NNpnD7pCjCbtruwSCS17A0zHWiDoXu3Loo3Y/edit#slide=id.p. [Accessed 7 7 2018].

[274] S. Higgins, "DAO Debacle Escalates: Attacker Counter-Attacks Ethereum Developers," Coin Desk, 23 6 2016. [Online]. Available: https://www.coindesk.com/dao-counter-attack-ethereum/. [Accessed 8 7 2018].

[275] GloomyOak, "It seems attacker just targeted the WhiteHatDAOs," Reddit, 22 6 2016. [Online]. Available: https://www.reddit.com/r/ethereum/comments/4p9z93/it_seems_attacker_just_targeted_the_whitehatdaos/?utm_term=28572302075&utm_medium=comment_embed&utm_source=embed&utm_name=null&utm_content=footer. [Accessed 15 5 2018].

[276] H. Georgiev, "The hack that changed the blockchain perspective," 11 8 2016. [Online]. Available: https://labs.mwrinfosecurity.com/blog/the-hack-that-changed-the-blockchain-perspective/. [Accessed 15 5 2018].

[277] P. Vessenes, "More Ethereum Attacks: Race-To-Empty is the Real Deal," Vessenes Blog, 9 6 2016. [Online]. Available: https://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/. [Accessed 9 7 2018].

[278] M. P. G. Gelvez, "Explaining the DAO exploit for beginners in Solidity," Medium, 16 10 2016. [Online]. Available: https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470. [Accessed 16 4 2018].

[279] K. R, "The Dao Hack And Recursive Calling Vulnerability In Ethereum," What is Ethereum Organization, 5 8 2017. [Online]. Available: https://what-is-ethereum.org/2017/08/05/the-dao-hack-and-recursive-calling-vulnerability-in-ethereum. [Accessed 9 7 2018].

[280] P. Daian, "Analysis of the DAO exploit," Hacking Distributed, 18 6 2016. [Online]. Available: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/. [Accessed 9 7 2018].

[281] R. Graham, "Ethereum/TheDAO hack simplified," Errata Security, 18 6 2016. [Online]. Available: https://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html#.W0QQei2ZPUK. [Accessed 9 7 2018].

[282] Koeppelmann, "The big theDAO heist FAQ," Reddit, 19 6 2016. [Online]. Available: https://www.reddit.com/r/ethereum/comments/4os7l5/the_big_thedao_heist_faq/. [Accessed 13 7 2018].

[283] M. P. G. Gelvez, "Explaining the DAO exploit for beginners in Solidity," Medium, 16 10 2016. [Online]. Available: https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470. [Accessed 25 5 2018].

[284] Investopedia, "Hard Fork," Investopedia, [Online]. Available: https://www.investopedia.com/terms/h/hard-fork.asp#ixzz5E8ZcLqLR. [Accessed 29 4 2018].

[285] CryptoGraphics, "Hard and Soft Fork," [Online]. Available: https://cryptographics.info/cryptographics/blockchain/hard-soft-forks/. [Accessed 10 12 2018].

[286] V. Zamfir, "The DAO Hard Fork, and the Negotiation that Couldn't Happen," Medium, 19 7 2016. [Online]. Available: https://medium.com/@Vlad_Zamfir/the-dao-hard-fork-and-the-negotiation-that-couldnt-happen-bdd2aedefe84. [Accessed 12 7 2018].

[287] C. Aventinus, "Parity Multisig Wallet Hacked, or How Come?," Coin Telegraph, 13 11 2017. [Online]. Available: https://cointelegraph.com/news/parity-multisig-wallet-hacked-or-how-come. [Accessed 14 5 2018].

[288] S. Schroeder, "Not again: Hackers steal $52 million worth of Ethereum," Mashable, 20 7 2017. [Online]. Available: https://mashable.com/2017/07/20/ethereum-hackers-theft-32-million/#JPX2TL5fgZq9. [Accessed 21 5 2018].

[289] B. Chan, "How Ethereum's Wallets Are Evolving," Coin Desk, 17 9 2016. [Online]. Available: https://www.coindesk.com/ethereums-wallets-evolving/. [Accessed 15 5 2018].

[290] Investopedia, "Gas (Ethereum)," Investopedia, [Online]. Available: https://www.investopedia.com/terms/g/gas-ethereum.asp. [Accessed 20 12 2018].

[291] B. Davenport, "What is Multi-Sig, and What Can It Do?," Coin Center, 1 1 2015. [Online]. Available: https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do. [Accessed 21 5 2018].

[292] H. Qureshi, "A hacker stole $31M of Ether—how it happened, and what it means for Ethereum," 20 7 2017. [Online]. Available: https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce. [Accessed 15 5 2018].

[293] P. D. A. J. a. E. G. S. Lorenz Breidenbach, "An In-Depth Look at the Parity Multisig Bug," Hacking Distributed, 22 7 2017. [Online]. Available: http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/. [Accessed 15 7 2018].

[294] . D. J. a. G. S. Lorenz Breidenbach, "An In-Depth Look at the Parity Multisig Bug," Hacking Distributed, 22 7 2017. [Online]. Available: http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/. [Accessed 11 5 2018].

[295] Etheraveum, "Parity Wallet Hack Explained," Steemit, 19 7 2017. [Online]. Available: https://steemit.com/cryptocurrency/@etheraveum/parity-wallet-hack-explained. [Accessed 15 7 2018].

[296] Etherscan, "Transactions::Address 0x0e0d16475d2ac6a4802437a35a21776e5c9b681a77fef1693b0badbb6afdb083," Etherscan, 18 7 2017. [Online]. Available:

https://etherscan.io/tx/0x0e0d16475d2ac6a4802437a35a21776e5c9b681a77fef1693b0badbb6afdb083. [Accessed 15 5 2018].

[297] Etherscan, "Transactions::Address 0x97f7662322d56e1c54bd1bab39bccf98bc736fcb9c7e61640e6ff1f633637d38," Etherscan, 19 7 2017. [Online]. Available: https://etherscan.io/tx/0x97f7662322d56e1c54bd1bab39bccf98bc736fcb9c7e61640e6ff1f633637d38. [Accessed 14 5 2018].

[298] Etherscan, "Transactions::Address 0xeef10fc5170f669b86c4cd0444882a96087221325f8bf2f55d6188633aa7be7c," Etherscan, 19 7 2017. [Online]. Available: https://etherscan.io/tx/0xeef10fc5170f669b86c4cd0444882a96087221325f8bf2f55d6188633aa7be7c. [Accessed 1 5 2018].

[299] S. Palladino, "The Parity Wallet Hack Explained," Zeppelin, 19 7 2017. [Online]. Available: https://blog.zeppelin.solutions/on-the-parity-wallet-multisig-hack-405a8c12e8f7. [Accessed 2 5 2018].

[300] G. Wood, "Security Alert," Parity Technology, 18 7 2017. [Online]. Available: https://gitter.im/paritytech/parity. [Accessed 14 7 2018].

[301] W. Suberg, "Parity Hack: White Hat Group Drains $85 Mln As Company Fills Holes," Coin Telegraph, 20 7 2017. [Online]. Available: https://cointelegraph.com/news/parity-hack-white-hat-group-drains-85-mln-as-company-fills-holes. [Accessed 14 7 2018].

[302] Etherscan, "Transactions::Address 0x1dba1131000664b884a1ba238464159892252d3a," Ethereum, 19 7 2017. [Online]. Available: https://etherscan.io/txs?a=0x1dba1131000664b884a1ba238464159892252d3a&p=79. [Accessed 14 7 2018].

[303] J. Morse, " Hackers just stole $85 million in Ether to save it from *the real crooks*," Mashable, 20 7 2017. [Online]. Available: https://mashable.com/2017/07/20/ethereum-stolen-white-hat-group/#5Hu8F9JsHOqT. [Accessed 14 7 2018].

[304] P. Technology, "update wallet library modifiers #6103," Parity Technology, 19 7 2017. [Online]. Available: https://github.com/paritytech/parity/pull/6103. [Accessed 2 5 2018].

[305] Etherscan, "Transactions," Ethereum, 20 7 2017. [Online]. Available: https://etherscan.io/txs?a=0xb3764761e297d6f121e79c32a65829cd1ddb4d32. [Accessed 15 7 2018].

[306] W. H. Group, "Contract 0x3abe5285ED57c8b028D62D30c456cA9eb3E74105," White Hack Group, 24 7 2017. [Online]. Available: https://etherscan.io/address/0x3abe5285ED57c8b028D62D30c456cA9eb3E74105#code. [Accessed 15 7 2018].

[307] Solidity, "Visibility and Getters," Solidity, [Online]. Available: https://solidity.readthedocs.io/en/develop/contracts.html#visibility-and-getters. [Accessed 2 5 2018].

[308] Etherscan, "Transactions::Address 0x9dbf0326a03a2a3719c27be4fa69aacc9857fd231a8d9dcaede4bb083def75ec," Etherscan, 19 7 2017. [Online]. Available:

https://etherscan.io/tx/0x9dbf0326a03a2a3719c27be4fa69aacc9857fd231a8d9dcaede4bb083def75ec. [Accessed 2 5 2018].

[309] Etherscan, "Transactions::Address 0xeef10fc5170f669b86c4cd0444882a96087221325f8bf2f55d6188633aa7be7c," Etherscan, 19 7 2017. [Online]. Available: https://etherscan.io/tx/0xeef10fc5170f669b86c4cd0444882a96087221325f8bf2f55d6188633aa7be7c. [Accessed 2 5 2018].

[310] Gavofyork, "Fix initialisation bug. (#6102)," Parity Technology, 19 7 2017. [Online]. Available: https://github.com/paritytech/parity-ethereum/commit/b640df8fbb964da7538eef268dffc125b081a82f. [Accessed 14 7 2018].

[311] C. Masters, "Ethereum Hard Fork Explained," Cryptovest, 11 8 2017. [Online]. Available: https://cryptovest.com/education/ethereum-hard-fork-explained/. [Accessed 14 7 2018].

[312] Gavofyork, "Fix initialisation bug (#6102)," 19 7 2017. [Online]. Available: https://github.com/paritytech/parity/commit/b640df8fbb964da7538eef268dffc125b081a82f. [Accessed 14 7 2018].

[313] S. Palladino, "The Parity Wallet Hack Reloaded," Zeppelinos, 7 11 2017. [Online]. Available: https://blog.zeppelinos.org/parity-wallet-hack-reloaded/. [Accessed 14 7 2018].

[314] M. Condon, "Parity Wallet Hack 2: Electric Boogaloo," Hacker Noon, 7 11 2017. [Online]. Available: https://hackernoon.com/parity-wallet-hack-2-electric-boogaloo-e493f2365303. [Accessed 6 5 2018].

[315] C. Durr, "Parity Hack: How It Happened, And Its Aftermath," Medium, 17 11 2017. [Online]. Available: https://medium.com/solidified/parity-hack-how-it-happened-and-its-aftermath-9bffb2105c0. [Accessed 4 7 2018].

[316] 3eamit, "Add the Wallet Library #74," Github, 3 8 2017. [Online]. Available: https://github.com/paritytech/contracts/pull/74#%20issuecomment-319892715. [Accessed 1 7 2018].

[317] Etherscan, "Transaction 0x05f71e1b2cb4f03e547739db15d080fd30c989eda04d37ce6264c5686e0722c9," Etherscan, 6 11 2017. [Online]. Available: https://etherscan.io/tx/0x05f71e1b2cb4f03e547739db15d080fd30c989eda04d37ce6264c5686e0722c9. [Accessed 16 5 2018].

[318] Etherscan, "Transactions Address 0x47f7cff7a5e671884629c93b368cb18f58a993f4b19c2a53a8662e3f1482f690," Etherscan, 6 11 2017. [Online]. Available: https://etherscan.io/tx/0x47f7cff7a5e671884629c93b368cb18f58a993f4b19c2a53a8662e3f1482f690. [Accessed 6 5 2018].

[319] Devops199, "anyone can kill your contract," Github, 6 11 2017. [Online]. Available: https://github.com/paritytech/parity/issues/6995. [Accessed 11 5 2018].

[320] P. Technologies, "UPDATE: A user exploited an issue and thus removed the library code, as it seems unaware of the consequences," Twitter, 7 11 2017. [Online].

Available: https://twitter.com/ParityTech/status/927850992145719296. [Accessed 11 5 2018].

[321] P. Technologies, "A Postmortem on the Parity Multi-Sig Library Self-Destruct," Parity Technologies, 15 11 2017. [Online]. Available: https://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/. [Accessed 11 5 2018].

[322] A. Akentiev, "Parity Multisig Hacked. Again," Medium, 8 11 2017. [Online]. Available: https://medium.com/chain-cloud-company-blog/parity-multisig-hack-again-b46771eaa838. [Accessed 8 5 2018].

[323] neno13, "How it happened: A hacker stole $31M of Ethereum," Busy.org, 31 7 2017. [Online]. Available: https://busy.org/@neno13/how-it-happened-a-hacker-stole-usd31m-of-ethereum. [Accessed 11 5 2018].

[324] Etherscan, "Contract 0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4," [Online]. Available: https://etherscan.io/address/0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4#code. [Accessed 6 5 2018].

[325] C. Pauw, Coin Telegraph, 3 5 2018. [Online]. Available: https://cointelegraph.com/news/eip-999-why-a-vote-to-release-parity-locked-funds-evoked-so-much-controversy. [Accessed 4 10 2018].

[326] P. Technologies, "A Postmortem on the Parity Multi-Sig Library Self-Destruct," Parity Technologies, 15 11 2017. [Online]. Available: https://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/. [Accessed 11 5 2018].

[327] H. Lam, "Against EIP-999 (Restore Parity Wallet Funds)," Coin Monk, 21 4 2018. [Online]. Available: https://medium.com/coinmonks/against-eip-999-restore-parity-wallet-funds-633368125165. [Accessed 4 8 2018].

[328] Ethereum, "Ethereum Classic Technical Reference," Ethereum, [Online]. Available: https://etc-tech-ref.readthedocs.io/en/latest/docs/appendices/code_is_law_principle.html. [Accessed 10 5 2018].

[329] S. Dexter, "EIP-999 & Parity Drama Explained Simply," Mango Research, 19 7 2018. [Online]. Available: https://www.mangoresearch.co/eip-999-parity-drama-explained-simply/. [Accessed 10 8 2018].

[330] Wikipedia, "Bitfinex," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Bitfinex. [Accessed 5 5 2018].

[331] Y. B. Perez, "Bitfinex First Bitcoin Exchange to Offer On-Blockchain Transactions," Coin Desk, 4 6 2015. [Online]. Available: https://www.coindesk.com/bitfinex-bitcoin-exchange-on-blockchain-transactions/. [Accessed 11 5 2018].

[332] B. B. Exchange, "Bitfinex.com Review – Scam or Not?," Best Bitcoin Exchange, [Online]. Available: http://www.bestbitcoinexchange.net/en/bitfinex-com/. [Accessed 13 5 2018].

[333] J. I. Wong, "Bitcoin exchanges can’t stop getting hacked, no matter what security system they use," QZ, 4 8 2016. [Online]. Available: https://qz.com/749789/bitcoin-exchanges-cant-stop-getting-hacked-no-matter-what-security-system-they-use/. [Accessed 11 5 2018].

[334] J. Maxim, "Bitfinex Hot Wallets Hacked, More Than 1,400 Bitcoin May Be Stolen," Bitcoin Magazine, 22 5 2015. [Online]. Available: https://bitcoinmagazine.com/articles/bitfinex-hot-wallets-hacked-1400-bitcoin-may-stolen-1432326539/. [Accessed 11 5 2018].

[335] Sotnd1996, "Overview of BitFinex Hack - The problem with redundant controls," 16 8 2016. [Online]. Available: https://busy.org/@sotnd1996/overview-of-bitfinex-hack-the-problem-with-redundant-controls. [Accessed 21 7 2018].

[336] S. Higgins, "The Bitfinex Bitcoin Hack: What We Know (And Don't Know)," Coin Desk, 3 8 2016. [Online]. Available: https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/. [Accessed 14 5 2018].

[337] A. Hayes, "You've been Buttfinessed," Bitmex, 6 8 2016. [Online]. Available: https://blog.bitmex.com/youve-been-buttfinessed/. [Accessed 16 5 2018].

[338] D. Shares, "CFTC fines bitcoin exchange Bitfinex $75,000 for illegal off-exchange financial transactions," Bitcoin.com, 2 6 2016. [Online]. Available: https://news.bitcoin.com/cftc-fines-bitcoin-exchange-bitfinex-75000-illegal-off-exchange-financial-transactions/. [Accessed 12 5 2018].

[339] B. News, "Bitcoin traders made 700% returns before losing millions in hack attack," Bloomberg News, 15 8 2016. [Online]. Available: https://www.bloomberg.com/professional/blog/bitcoin-traders-made-700-returns-losing-millions-hack-attack/. [Accessed 11 5 2018].

[340] M. Bevand, "Timeline of Bitfinex Exchange Theft," ZoriniAQ, 3 8 2016. [Online]. Available: http://blog.zorinaq.com/bitfinex-hack-2016/. [Accessed 11 5 2018].

[341] B. Exchange, "BREAKING: Bitcoin Exchange BitFinex' Hot Wallet Hacked," CCN, 22 5 2015. [Online]. Available: https://www.ccn.com/breaking-bitcoin-exchange-bitfinex-hot-wallet-hacked/. [Accessed 11 5 2018].

[342] Bitfinex, "Bitfinex and BitGo Partner to Create World's First Real-Time Proof of Reserve Bitcoin Exchange," Bitfinex, 4 6 2015. [Online]. Available: https://www.bitfinex.com/posts/39. [Accessed 14 5 2018].

[343] M. Clinch, "Bitcoin now classed as a commodity in the US," CNBC, 18 9 2015. [Online]. Available: https://www.cnbc.com/2015/09/18/bitcoin-now-classed-as-a-commodity-in-the-us.html. [Accessed 14 5 2018].

[344] D. Shares, "CFTC fines bitcoin exchange Bitfinex $75,000 for illegal off-exchange financial transactions," Bitcoin.com, 2 6 2016. [Online]. Available: https://news.bitcoin.com/cftc-fines-bitcoin-exchange-bitfinex-75000-illegal-off-exchange-financial-transactions/. [Accessed 14 5 2018].

[345] Z. Tackett, "Bitfinex security breach: Trading will be halted as well as all crypto deposits/withdrawals," Reddit, 2 8 2016. [Online]. Available: https://www.reddit.com/r/Bitcoin/comments/4vtuxo/bitfinex_security_breach_trading_will_be_halted/. [Accessed 15 5 2018].

[346] Blahbitcoin, "P2SH.INFO shows movement out of multisig wallets... gives indication of bfx breach size!," Reddit, 2 8 2016. [Online]. Available: https://www.reddit.com/r/Bitcoin/comments/4vupa6/p2shinfo_shows_movement_out_of_multisig_wallets/. [Accessed 15 5 2018].

[347] Bitfinex, "Bitfinex Interim Update," Bitfinex, 6 8 2016. [Online]. Available: http://blog.bitfinex.com/announcements/bitfinex-interim-update/. [Accessed 11 5 2018].

[348] Bitfinex, "Site Update," Bitfinex, 10 8 2016. [Online]. Available: http://blog.bitfinex.com/announcements/site-update/. [Accessed 16 5 2018].

[349] L. P. Adrian Shedden, "The impact of the Bitfinex hack on cryptocurrencies," *Cyber Security Law & Practice,* no. Sept, pp. 7-9, 2016.

[350] K. Torpey, "After the Bitfinex Hack, Here's Why Bitstamp Is Sticking with BitGo," Bitcoin Magazine, 8 8 2016. [Online]. Available: https://bitcoinmagazine.com/articles/after-the-bitfinex-hack-here-s-why-bitstamp-is-sticking-with-bitgo-1470669567/. [Accessed 14 5 2018].

[351] T. O'Donnell, "BitFinex Hack Overview," 27 8 2016. [Online]. Available: https://www.slideshare.net/ODonnellThomas/bit-finex-hack-overview-65412293. [Accessed 11 5 2018].

[352] L. Brus, "Bitfinex hack raises concerns over multisig technology," Coin Fox, 3 8 2016. [Online]. Available: http://www.coinfox.info/news/reviews/6096-bitfinex-confirms-bitgo-signing-theft-transactions. [Accessed 16 5 2018].

[353] pitchbend, "How was Bitfinex hacked!? Users need to know," Reddit, 19 11 2017. [Online]. Available: https://www.reddit.com/r/BitcoinMarkets/comments/5dn784/how_was_bitfinex_hacked_users_need_to_know/. [Accessed 15 5 2018].

[354] D. Roberts, "Biggest bitcoin hack since Mt. Gox revolves around "cold storage"," Yahoo, 3 8 2016. [Online]. Available: https://finance.yahoo.com/news/bitcoin-hack-bitfinex-cold-storage-bitgo-cftc-225434534.html. [Accessed 17 5 2018].

[355] Z. Tackett, "Bitfinex: Update Regarding Security Audit, Financial Audit, And More," Bitfinex, 17 8 2016. [Online]. Available: https://www.reddit.com/r/BitcoinMarkets/comments/4y4uwl/bitfinex_update_regarding_security_audit/. [Accessed 14 7 2018].

[356] Sebfor, "The DAO Hack – Recap of What Happened," Sebfor, [Online]. Available: http://sebfor.com/the-dao-hack-recap-of-what-happened/. [Accessed 30 4 2018].

[357] M. Araoz, "Onward with Ethereum Smart Contract Security," Zeppelin, 16 8 2016. [Online]. Available: https://blog.zeppelin.solutions/onward-with-ethereum-smart-contract-security-97a827e47702. [Accessed 19 5 2018].

[358] L. Abegg, "Code is Law? Not Quite Yet," Coin Desk, 27 8 2016. [Online]. Available: https://www.coindesk.com/code-is-law-not-quite-yet/. [Accessed 20 10 2018].

[359] P. F. Burgeuno, "the Dao Attack," 27 6 2016. [Online]. Available: https://www.slideshare.net/abanlex/the-dao-attack-ethereum. [Accessed 9 7 2018].

[360] P. Vessenes, "Deconstructing theDAO Attack: A Brief Code Tour," 18 6 2016. [Online]. Available: https://vessenes.com/deconstructing-thedao-attack-a-brief-code-tour/. [Accessed 9 7 2018].

[361] D. Siegel, "Understanding The DAO Hack for Journalists," Medium, 19 6 2016. [Online]. Available: https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993. [Accessed 19 5 2018].

[362] C. Jentzsch, "The History of the DAO and Lessons Learned," Slock.it, 24 8 2016. [Online]. Available: https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5. [Accessed 19 5 2018].

[363] Ethereum, "The Ethereum Classic Declaration Of Independence," Ethereum, [Online]. Available: https://etc-tech-ref.readthedocs.io/en/latest/docs/appendices/dec_of_ind.html. [Accessed 4 1 2019].

[364] T. Attacker, "An Open Letter," 18 6 2016. [Online]. Available: https://pastebin.com/CcGUBgDG. [Accessed 5 1 2019].

[365] N. Tomaino, "The Governance of Blockchains," Medium, 28 2 2017. [Online]. Available: https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6. [Accessed 5 1 2019].

[366] T. Friebe, "Ethereum: Governed by a benevolent dictator?," Medium, 31 10 2017. [Online]. Available: https://medium.com/blockchainspace/ethereum-governed-by-a-benevolent-dictator-2a2be8aa331a. [Accessed 6 1 2019].

[367] J. Pearson, "Ethereum Wallet Company Knew About Critical Flaw That Let a User Lock Up Millions," Motherboard, 15 11 2017. [Online]. Available: https://motherboard.vice.com/en_us/article/d3djwj/ethereum-wallet-parity-knew-about-critical-flaw-that-let-user-devops199-lock-up-millions. [Accessed 4 10 2018].

[368] B. Academy, "Byte Academy," Byte Academy, 1 2 2018. [Online]. Available: https://byteacademy.co/blog/faq-blockchain-forks. [Accessed 4 10 2018].

[369] I. B. Yusta, "12 Myths about Blockchain Technology," Open Mind, 22 8 2017. [Online]. Available: https://www.bbvaopenmind.com/en/12-myths-about-blockchain-technology/. [Accessed 4 5 2018].

[370] F. Reese, "As Bitcoin Halving Approaches, 51% Attack Question Resurfaces," Coin Desk, 16 7 2016. [Online]. Available: https://www.coindesk.com/ahead-bitcoin-halving-51-attack-risks-reappear/. [Accessed 6 5 2018].

[371] T. Spilotro, "Third Time’s a Charm: Verge Suffers 51% Attack Yet Again," Block Explorer, 29 5 2018. [Online]. Available: https://blockexplorer.com/news/third-times-a-charm-verge-suffers-51-attack-yet-again/. [Accessed 27 12 2018].

[372] R. Sharma, "Bitcoin Gold Hack Shows 51% Attack Is Real," Investopedia, 30 5 2018. [Online]. Available: https://www.investopedia.com/news/bitcoin-gold-hack-shows-51-attack-real/. [Accessed 23 8 2018].

[373] C. 51, "PoW 51% Attack Cost," Crypto 51, [Online]. Available: https://www.crypto51.app. [Accessed 23 8 2018].

[374] T. K. Sharma, "How Is Blockchain Verifiable By Public And Yet Anonymous?," Blockchain Council, 10 7 2018. [Online]. Available: https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/. [Accessed 26 8 2018].

[375] M. Taylor, "Bitcoin Isn’t Anonymous, and That’s Ok," Coin Central, 25 6 2018. [Online]. Available: https://coincentral.com/bitcoin-isnt-anonymous-and-thats-ok/. [Accessed 25 8 2018].

[376] M. T. Review, "Bitcoin Transactions Aren’t as Anonymous as Everyone Hoped," MIT Technology Review, 23 8 2017. [Online]. Available:

https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/. [Accessed 5 5 2018].

[377] "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," Princeton University, Princeton University, 2017.

[378] P. Paganini, "Europol report – Cyber attacks against ATM networks on the rise," Security Affaires, 26 9 2017. [Online]. Available: https://securityaffairs.co/wordpress/63476/cyber-crime/atm-networks-hacking.html. [Accessed 22 8 2018].

[379] N. Levinson, "A new accident model for engineering safer systems," *Saf Sci*, vol. 4, no. 42, pp. 237-270, 2004.

[380] N. G. Leveson, "Engineering a Safer World: Systems Thinking Applied to Safety.," MIT Press, Cambridge, MA, 2011.

[381] N. L. William Young, "System thinking for safety and security.," in *Annual Computer Security Applications Conference - ACSAC 13*, New York, 2013.

[382] N. L. William Young, "Systems thinking for Safer Systems," *ACM Press*, no. Safety Science ACSAC '13, pp. 1-8, 2013.

[383] K. M. P. S. D. L. S. S. Ivo Friedberg, "STPA-SafeSec: Safety and security analysis for cyber-physical systems.," *Journal of Information Security and Applications*, no. 34, pp. 183-196, 2016.

[384] F. R. A. A. C. S. S. W. Kai Mindermann, "Exploratory Study of the Privacy Extended for System Theoric Process Analysis (STPA-Priv) to elicit Privacy Risk in eHealth," University of Stuttgart, Stuttgart, 2017.

[385] K. Ciesielski, "Event sourcing on blockchain with Ethereum, TypeScript and React," Software Mill, 1 8 2017. [Online]. Available: https://softwaremill.com/event-sourcing-on-blockchain/. [Accessed 1 9 2018].

[386] statista, "Size of the blockchain technology market worldwide from 2016 to 2021 (in million U.S. dollars)," statista.com, 2018. [Online]. Available: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/. [Accessed 15 1 2018].

[387] R. Fletcher, "Causal Analysis using System Theory Accident Analysis," Robert Fletcher System Safety, Inc., 2014.

[388] A. Hertig, "What is a DAO?," Coindesk, 2017. [Online]. Available: https://www.coindesk.com/information/what-is-a-dao-ethereum/. [Accessed 15 1 2018].

[389] M. W. N. B. Rituparna Bhattacharya, "A Blockchain based Peer-to-Peer Framework for Exchanging Leftover Foreign Currency," in *IEEE*, 2017.

[390] A. Collins, "Four reasons to question the hype around blockchain," World Economic Forum, 10 07 2017. [Online]. Available: https://www.weforum.org/agenda/2017/07/four-reasons-to-question-the-hype-around-blockchain/. [Accessed 2 3 2018].

[391] P. Crosman, "Does Blockchain Tech Solve Security Problems or Cause New Ones?," 16 8 2016. [Online]. Available: https://www.americanbanker.com/news/does-blockchain-tech-solve-security-problems-or-cause-new-ones. [Accessed 29 3 2018].

[392] R. ASSESSMENT, "The Ultra-Secure Network Architecture," [Online].

[393] R. Assessment, "The Ultra-Secure Network Architecture," RSM, [Online]. Available: https://rsmus.com/what-we-do/services/risk-advisory/the-ultra-secure-network-architecture.html. [Accessed 30 3 2018].

[394] B. Peterson, "Thieves stole potentially millions of dollars in bitcoin in a hacking attack on a cryptocurrency company," Business Insider, 6 12 2017. [Online]. Available: http://www.businessinsider.com/nicehash-bitcoin-wallet-hacked-contents-stolen-in-security-breach-2017-12. [Accessed 5 4 2018].

[395] T. Worstall, "Another Bitcoin Theft at Bitcoinica," Forbes, 15 5 2012. [Online]. Available: https://www.forbes.com/sites/timworstall/2012/05/15/another-bitcoin-theft-at-bitconia. [Accessed 3 4 2018].

[396] Bitcoinica, "Bitcoinica Hack Post Mortem," Bitcoinica, 12 5 2012. [Online]. Available: http://bitcoinica.blogspot.com. [Accessed 5 4 2018].

[397] D. GOODIN, "Bitcoins worth $87,000 plundered in brazen server breach," ars technica, 11 5 2012. [Online]. Available: https://arstechnica.com/uncategorized/2012/05/bitcoins-worth-87000-plundered/. [Accessed 5 4 2018].

[398] genjix, "Bitcoinica MtGox account compromised," Bitcoin Forum, 13 7 2012. [Online]. Available: https://bitcointalk.org/index.php?topic=93074.0. [Accessed 5 4 2018].

[399] Forum, "BTC-e post a statement about the hack, and apparently have no idea how it happened," reddit, 31 7 2012. [Online]. Available: https://www.reddit.com/r/Bitcoin/comments/xg2qf/btce_post_a_statement_about_the_hack_and/. [Accessed 5 4 2018].

[400] Forum, "BTC-E hacked - still unfolding," Bitcoin Forum, 31 7 2012. [Online]. Available: https://bitcointalk.org/index.php?topic=96831.0. [Accessed 6 4 2018].

[401] Ethereum, "Centralised Exchanges Are Terrible At Holding Your Money: A Timeline of Catastrophes," localethereum, 14 11 2017. [Online]. Available: https://blog.localethereum.com/centralised-exchanges-are-terrible-at-holding-your-money/. [Accessed 7 4 2018].

[402] V. Buterin, "Bitfloor Hacked, $250,000 Missing," Bitcoin Magazine, 5 9 2012. [Online]. Available: https://bitcoinmagazine.com/articles/bitfloor-hacked-250000-missing-1346821046/. [Accessed 9 4 2018].

[403] J. Biggs, " Hacker Steals $12,000 Worth Of Bitcoins In Brazen DNS-Based Attack," Techcrunch, 8 3 2013. [Online]. Available: https://techcrunch.com/2013/03/08/hacker-steals-12000-worth-of-bitcoins-in-brazen-dns-based-attack/. [Accessed 10 4 2018].

[404] R. MCMILLAN, "HACKERS PULL OFF $12,000 BITCOIN HEIST," Wired, 7 3 2013. [Online]. Available: https://www.wired.com/2013/03/digital-thieves-pull-off-12000-bitcoin-heist/. [Accessed 10 4 2018].

[405] A. Robertson, "Bitcoin service Instawallet 'suspended indefinitely' after hack," The Verge, 3 4 2013. [Online]. Available: https://www.theverge.com/2013/4/3/4180020/bitcoin-service-instawallet-suspended-indefinitely-after-hack. [Accessed 11 4 2018].

[406] E. Smart, "BitPay CEO Scammed for Over $1.8 Million in Bitcoin," cointelegraph, 17 9 2015. [Online]. Available: https://cointelegraph.com/news/bitpay-hacked-for-over-18-million-in-bitcoins. [Accessed 15 4 2018].

[407] S. Morgan, "Gartner: Worldwide information security spending to hit $93B in 2018," CSO, 23 8 2017. [Online]. Available: https://www.csoonline.com/article/3219165/it-careers/gartner-worldwide-information-security-spending-to-hit-93b-in-2018.html. [Accessed 31 4 2018].

[408] D. Houlding, "Healthcare Blockchain: Does Your Chain Have any Weak Links?," IT Peer Network Intel, 14 11 2017. [Online]. Available: https://itpeernetwork.intel.com/healthcare-blockchain-chain-weak-links/. [Accessed 1 5 2018].

[409] S. Wilson, "Blockchain: Almost everything you read is wrong," CIO, 6 5 2016. [Online]. Available: https://www.cio.co.nz/article/599399/blockchain-almost-everything-read-wrong/. [Accessed 1 5 2018].

[410] H. Kuchler, "Cyber attacks raise questions about blockchain security," Financial Times, 12 9 2016. [Online]. Available: https://www.ft.com/content/05b5efa4-7382-11e6-bf48-b372cdb1043a. [Accessed 4 5 2018].

[411] Y. Women, "Debunking Blockchain Myths (And How They Will Impact The Future Of Business)," Forbes, 4 5 2017. [Online]. Available: https://www.forbes.com/sites/yec/2017/05/04/debunking-blockchain-myths-and-how-they-will-impact-the-future-of-business/#77a31cd65609. [Accessed 6 5 2018].

[412] N. Bauerle, "What are Blockchain's Issues and Limitations?," Coin Desk, 1 5 2017. [Online]. Available: https://www.coindesk.com/information/blockchains-issues-limitations/. [Accessed 1 5 2018].

[413] M. Haber, "Securing Your Blockchain Servers," Beyond Trust, 12 1 2018. [Online]. Available: https://www.beyondtrust.com/blog/securing-blockchain-servers/. [Accessed 6 5 2018].

[414] A. Greenberg, "Silk Road 2.0 'Hack' Blamed On Bitcoin Bug, All Funds Stolen," Forbes, 13 2 2014. [Online]. Available: https://www.forbes.com/sites/andygreenberg/2014/02/13/silk-road-2-0-hacked-using-bitcoin-bug-all-its-funds-stolen/#68ce66bc2025. [Accessed 17 5 2018].

[415] A. NEWS, "Breaking: CryptoRush loses millions of Blackcoins," CCN, 25 3 2014. [Online]. Available: https://www.ccn.com/cryptorush-loses-millions-of-blackcoins/. [Accessed 30 6 2018].

[416] J. BUNTINX, "Chinese Exchange Platform KipCoin Admits To Hackers Stealing Over 3,000 Bitcoin," Digital Money Times, 18 2 2015. [Online]. Available: http://digitalmoneytimes.com/chinese-exchange-platform-kipcoin-admits-to-hackers-stealing-over-3000-bitcoin/. [Accessed 2 7 2018].

[417] A. Rosic, "Smart Contracts: The Blockchain Technology That Will Replace Lawyers," Block Geeks, 1 1 2016. [Online]. Available: https://blockgeeks.com/guides/smart-contracts/. [Accessed 9 7 2018].

[418] R. Graham, "Ethereum/TheDAO hack simplified," Errata Security, 18 6 2016. [Online]. Available: https://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html#.W0P9Xy2ZPUJ. [Accessed 9 7 2018].

[419] Slockit, "Understanding the DAO accounting," Slockit, 17 8 2017. [Online]. Available: https://github.com/slockit/DAO/wiki/Understanding-the-DAO-accounting. [Accessed 9 7 2018].

[420] D. Siegel, "Understanding The DAO Attack," 25 6 2016. [Online]. Available: https://www.coindesk.com/understanding-dao-hack-journalists/. [Accessed 9 7 2018].

[421] B. Chan, "How Ethereum's Wallets Are Evolving," Coin Desk, 17 9 2016. [Online]. Available: https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/. [Accessed 14 7 2018].

[422] S. Falkon, "The Story of the DAO—Its History and Consequences," Medium, 24 12 2017. [Online]. Available: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee. [Accessed 18 5 2018].

[423] A. Kohn, "The Failure of The DAO: Should We Regulate Cryptocurrency?," Futurism, 24 10 2016. [Online]. Available: https://futurism.com/the-failure-of-the-dao-should-we-regulate-cryptocurrency/. [Accessed 25 5 2018].

[424] J. Blalock, "What is Blockchain, and how does it benefit security?," Hummingbird Networks, 1 3 2017. [Online]. Available: https://info.hummingbirdnetworks.com/blog/what-is-blockchain-and-how-does-it-benefit-security. [Accessed 14 8 2018].

[425] E. S. C. B. Practices, "Ethereum Smart Contract Best Practices," Ethereum Smart Contract Best Practices, [Online]. Available: https://consensys.github.io/smart-contract-best-practices/known_attacks/. [Accessed 1 9 2018].

[426] W. Young, "STPA-SEC for Cyber Security / Mission Assurance," 24 3 2014. [Online]. Available: http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Young_STAMP_2014_As-delivered.pdf. [Accessed 29 8 2018].

[427] P. H. N. M. a. R. M. Éric Dubois, A Systematic Approach to Define the Domain of Information System Security Risk Management, Berlin, Heidelberg: Springer, 2010.

[428] u/PoRco1x, "EIP-999 Drama Explained Simply --- Catch Up & Discuss," Reddit, 19 7 2018. [Online]. Available: https://www.reddit.com/r/ethereum/comments/9083sn/eip999_drama_explained_simply_catch_up_discuss/. [Accessed 4 8 2018].

[429] phyro, "The DAO is History… or is it?," Medium, 13 5 2018. [Online]. Available: https://medium.com/coinmonks/the-dao-is-history-or-is-it-47a6f457338a. [Accessed 4 10 2018].

[430] T. A. (. c. yet), Pastebin, 18 6 2016. [Online]. Available: https://pastebin.com/CcGUBgDG. [Accessed 4 10 2018].

[431] Wikipedia, "Avalanche effect," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Avalanche_effect. [Accessed 2 12 2018].

[432] Norton, "Zero-day vulnerability: What it is, and how it works," Norton, [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html. [Accessed 8 12 2018].

[433] D. Siegel, "Understanding The DAO Attack," Coin Desk, 25 6 2016. [Online]. Available: https://www.coindesk.com/understanding-dao-hack-journalists. [Accessed 5 1 2019].

THIS PAGE INTENTIONALLY LEFT BLANK