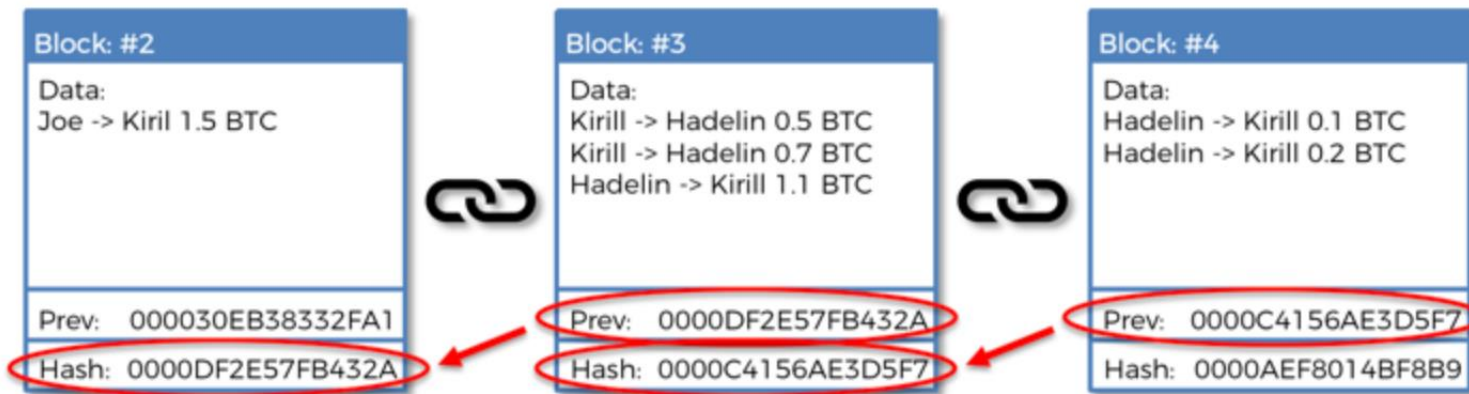**Kellerhals Carrard**

BITCOIN BEYOND SPECULATION

Avv. Lars Schlichting, LL.M., Partner

23.03.2021

What is Blockchain?

HOW DOES BLOCKCHAIN MINING WORK?

SHA256(Block Number, Data, Previous Block's Hash) -> Hash

Block: #2
Data:
Joe -> Kiril 1.5 BTC

Prev: 000030EB38332FA1
Hash: 0000DF2E57FB432A

Block: #3
Data:
Kirill -> Hadelin 0.5 BTC
Kirill -> Hadelin 0.7 BTC
Hadelin -> Kirill 1.1 BTC

Prev: 0000DF2E57FB432A
Hash: 0000C4156AE3D5F7

Block: #4
Data:
Hadelin -> Kirill 0.1 BTC
Hadelin -> Kirill 0.2 BTC

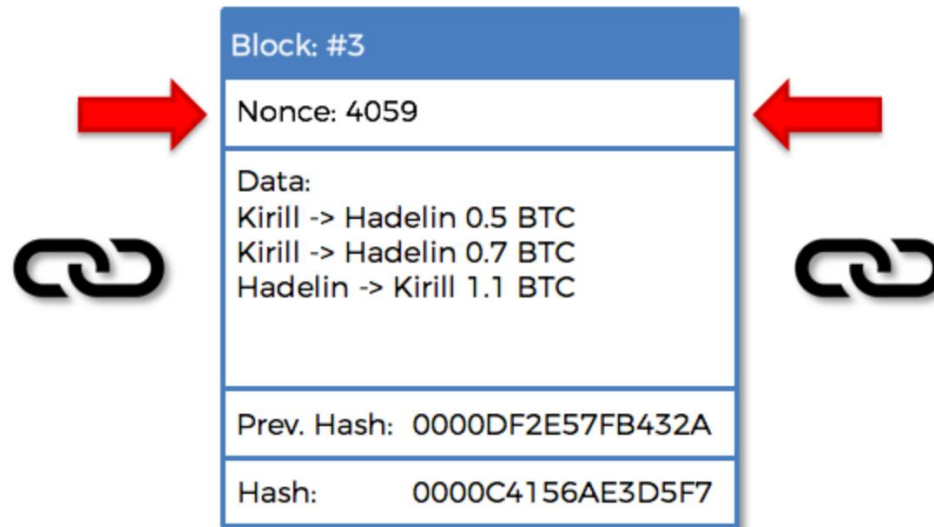Prev: 0000C4156AE3D5F7
Hash: 0000AEF8014BF8B9

The cryptographic puzzle requires miners to find a hash smaller than the set target for it to be valid

Source: Medium, How does Bitcoin/blockchain mining works?

HOW DOES BLOCKCHAIN MINING WORK?

SHA256(Block Number, **Nonce**, Data, Previous Block's Hash) -> Hash

Block: #3

Nonce: 4059

Data:
Kirill -> Hadelin 0.5 BTC
Kirill -> Hadelin 0.7 BTC
Hadelin -> Kirill 1.1 BTC

Prev. Hash: 0000DF2E57FB432A
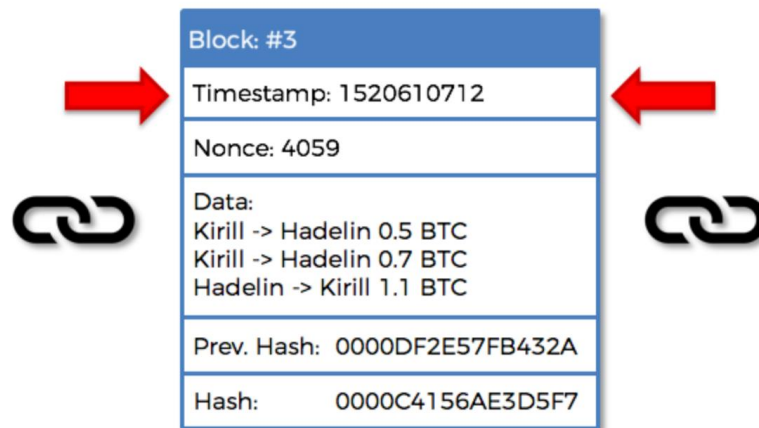
Hash: 0000C4156AE3D5F7

Source: Medium, How does Bitcoin/blockchain mining works?

- There is a total of 16^{64} possible SHA256 cryptographic hash values
- Every leading zero reduces the number's magnitude by a factor of 16
- There is a limited range of around 4 Billion values of nonces
- Average miner takes 40 seconds to do 4 Billion passes.

HOW DOES BLOCKCHAIN MINING WORK?

SHA256(Block Number, **Timestamp**, Nonce, Data, Previous Block's Hash) -> Hash

timestamp representing the current Unix time (number of seconds elapsed since 1st January 1970), that means timestamp is constantly refreshing !

Block: #3

Timestamp: 1520610712

Nonce: 4059

Data:
Kirill -> Hadelin 0.5 BTC
Kirill -> Hadelin 0.7 BTC
Hadelin -> Kirill 1.1 BTC

Prev. Hash: 0000DF2E57FB432A

Hash: 0000C4156AE3D5F7

Source: Medium, How does Bitcoin/blockchain mining works?

HOW DIFFICULT IT IS TO FIND A PRIVATE KEY?

The odds of guessing winning Powerball numbers vs. guessing one Bitcoin private key.
YOU WOULD HAVE TO WIN POWERBALL ~9 TIMES IN A ROW

Bits	Size of Space	
1	2	
10	1,024	
20	1,048,576	
28.121	292,000,000	Winning PowerBall
30	1,073,741,824	
40	1,099,511,627,776	
50	1,125,899,906,842,620	
60	1,152,921,504,606,850,000	
70	1,180,591,620,717,410,000,000	
80	1,208,925,819,614,630,000,000,000	
90	1,237,940,039,285,380,000,000,000,000	
100	1,267,650,600,228,230,000,000,000,000,000	
110	1,298,074,214,633,710,000,000,000,000,000,000	
120	1,329,227,995,784,920,000,000,000,000,000,000,000	
130	1,361,129,467,683,750,000,000,000,000,000,000,000,000	
140	1,393,796,574,908,160,000,000,000,000,000,000,000,000,000	
150	1,427,247,692,705,960,000,000,000,000,000,000,000,000,000,000	
160	1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000,000	
170	1,496,577,676,626,840,000,000,000,000,000,000,000,000,000,000,000,000	
180	1,532,495,540,865,890,000,000,000,000,000,000,000,000,000,000,000,000,000	
190	1,569,275,433,846,670,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
200	1,606,938,044,258,990,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
210	1,645,504,557,321,210,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
220	1,684,996,666,696,920,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
230	1,725,436,586,697,640,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
230.186	1,962,577,783,683,320,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000.00	Guessing any Bitcoin Private Key with a Balance
240	1,766,847,064,778,380,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
256	115,792,089,237,316,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	Guessing a Specific Bitcoin Private Key

What is Bitcoin

WHAT IS BITCOIN?

Some elements to understand bitcoin:

- The inventor of bitcoin (and of Bitcoin blockchain) is an anonymous person identified with the name of Sathoshi Nakamoto.

- Bitcoin is the accounting token on the Bitcoin blockchain, was created after the economical crisis of 2008 as a store of value (digital gold).

- There is no central parts controlling bitcoins (no central bank).

- Allows peers to peers transaction. The holder of the keys can move the bitcoin which are registered on the blockchain. Wallets facilitate the use of the keys.

- Is limited in numbers (21 Mio pieces), every miner solving the mathematical problem which put in security the blockchain is receiving btc. The reward started with 50 btc per block and is halved every 210'000 blocks (more ar less 4 years). Today reward amount to 12.5 btc. Last btc to be mined around year 2140.

WHAT IS BITCOIN?

Some elements to understand bitcoin:

- Has a deflationary effect and therefore is used as store of value in heavily inflationary countries (Venezuela, Zimbabwe).

- Is pseudonymous, but traceable, which allows authorities to create a pattern of the use and discover criminals (eg. Silk road, Mt. Gox case); very difficult to do Money Laundering with traceable crypto like bitcoin today, but easy using non traceable ones (Monero).

- Each BTC is divisible up to 8 decimal places (0.00000001 BTC or 1/100,000,000th). 0.00000001 BTC = 1 satoshi. The Bitcoin protocol could be subdivided further to offer greater divisibility if needed.

- Since blockchain is decentralized, every Bitcoin node in the network would have to be destroyed in order to eliminate the currency.

CAN BLOCKCHAIN EXIST WITHOUT TOKEN/CRYPTO?

Blockchain without token/crypto is like:

- Street without cars

- Cars without gas

- A paper ledger without a pen

A TOKEN ON THE BLOCKCHAIN...

… is representing an accounting value

… can act as a private mean of payment, a right, an asset, or any other material concept

… can allow peer to peer transactions, without intermediation

… is programmable (smart contracts) and can execute autonomous transactions.

… can be used as currency for Internet of Things

WHAT IS BITCOIN

Bitcoin's Asymptotic Money Supply Targeting

Source: https://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-policy/

THE GENESIS BLOCK

THE GENESIS BLOCK

TODOA...

KELLERHALS Carrard

NEWS > MARKETS NEWS

EU Leaders Reach Deal on €750 Billion COVID Recovery Fund

By **DEBORAH D'SOUZA** | Updated Jul 21, 2020

KEY TAKEAWAYS

- EU leaders agree to €750 billion ($860 billion) coronavirus recovery fund
- Includes €390 billion in grants and €360 billion in low interest loans for countries badly affected by the COVID-19 outbreak
- European leaders also finalized the €1.07 trillion budget for 2021-2027 to

European Council
Council of the European Union

The European Council   The Council of the EU   Policies   Meeting calendar   Documents & Publications   Press

Contact

Home > Policies > COVID-19 coronavirus pandemic: the EU's response

> Overview
> Timeline - Council actions on COVID-19
> COVID-19: public health
> COVID-19: economy
> COVID-19: travel and transport
> COVID-19: research and vaccines
> Fighting disinformation
> European solidarity

COVID-19: the EU's response to the economic fallout

The EU and its member states have taken action to minimise the fallout on the economy of the COVID-19 pandemic.

A recovery plan for Europe

On 23 April 2020, EU leaders decided to work towards establishing a EU recovery fund aimed at mitigating the effects of the crisis. They tasked the European Commission to urgently come up with a proposal, which would also clarify the link between the fund and the EU's long term budget. The proposal, a recovery plan for Europe, was presented by the European Commission on 27 May 2020.

On 21 July, EU leaders agreed on a **€750 billion recovery effort**, **Next Generation EU**, to help the EU tackle the crisis caused by the pandemic. The recovery package is now going through the legislative steps to be ready in 2021.

Infographic - EU budget 2021-2027 and recovery plan

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HOW TO SPEND IT

Become an FT subscriber to read:

"US Congress approves $900bn stimulus package"

REUTERS

World Business Markets Breakingviews Video More

BUSINESS NEWS   DECEMBER 8, 2020 / 1:36 AM / UPDATED A MONTH AGO

Japan unveils $708 billion in fresh stimulus with eye on post-COVID growth

By Leika Kihara, Tetsushi Kajimoto   3 MIN READ

TOKYO (Reuters) - Japan announced a fresh $708 billion economic stimulus package on Tuesday to speed up the recovery from the country's deep coronavirus-driven slump, while targeting investment in new growth areas such as green and digital innovation.

BBC   Sign in   Home   News   Sport   Reel   Worklife   Travel   Futu

NEWS

Home | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health

World Africa Asia Australia Europe Latin America Middle East US & Canada

Canada unveils largest economic relief package since WW2

1 December 2020

BITCOIN FAKE MYTHS: ENERGY CONSUMING

Comparing Energy Expenditure Across Monetary and Banking Systems

Source: ARK Investment Management LLC, 2020. Data Source: https://medium.com/@danhedl/pow-is-effic ient-aa3d442754d3
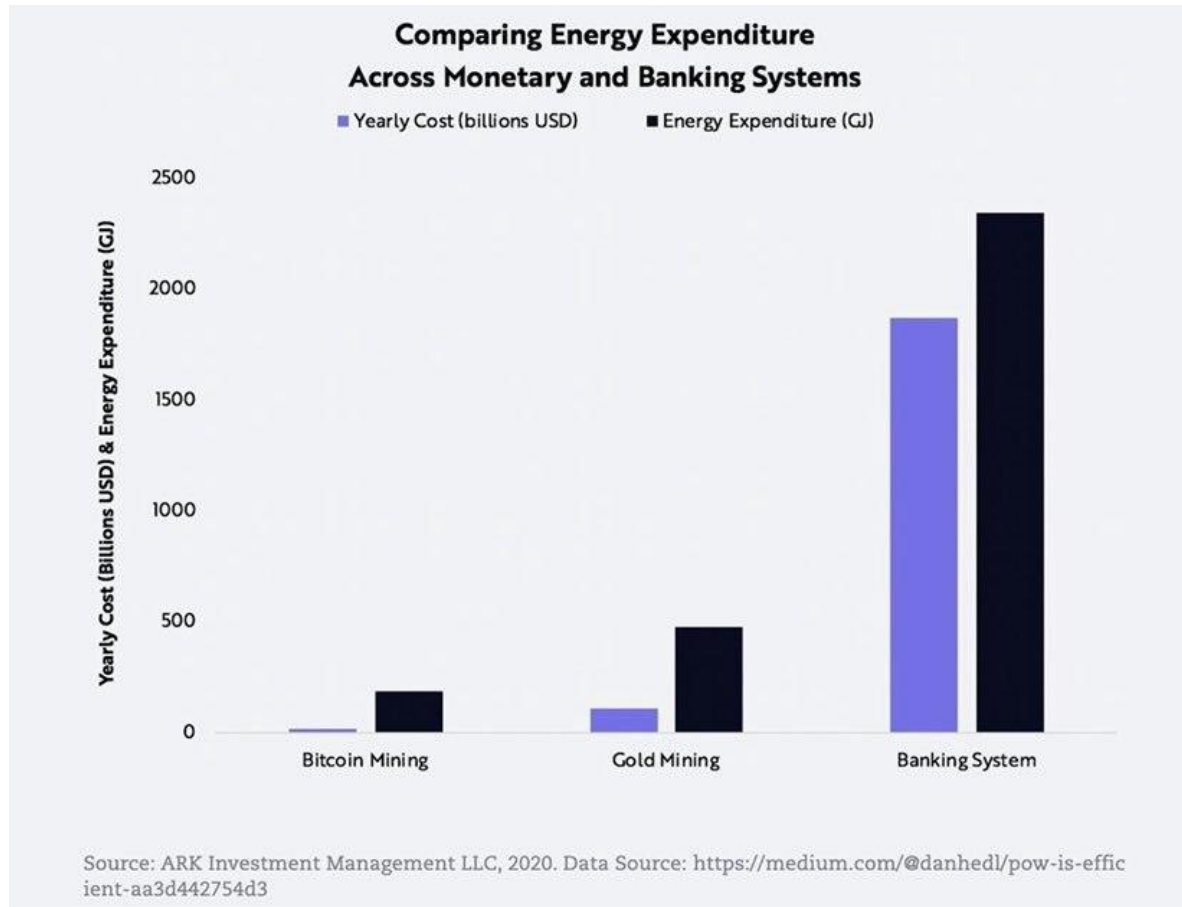
BITCOIN FAKE MYTHS: ENERGY CONSUMING

Letter to the shareholders of Ater Solution ASA, Energy Norwegian company, justifing the establishment of Seetee ASA
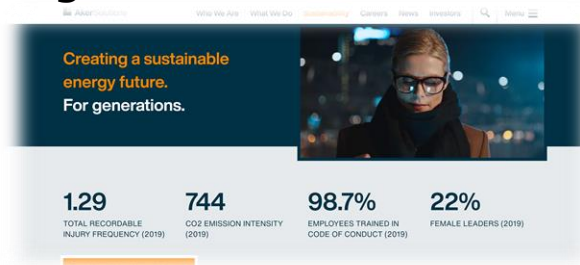
Second, Seetee will establish mining operations that transfer stranded or intermittent electricity without stable demand locally—wind, solar, hydro power— to economic assets that can be used anywhere. Bitcoin is, in our eyes, a load-balancing economic battery, and batteries are essential to the energy transition required to reach the targets of the Paris Agreement. Our ambition is to be a valuable partner in new renewable projects.

Source: https://www.seetee.io/static/shareholder_letter-6ae7e85717c28831bf1c0eca1d632722.pdf

BITCOIN FAKE MYTHS: MONEY LAUNDERING

■ **Bitcoin's Use for Criminal Enterprise:** Authorities took down an illegal online drug marketplace called Silk Road in October 2013. Its founder was charged with engaging in a money laundering and narcotics trafficking conspiracy as well as computer hacking. The U.S. Department of Justice seized Silk Road's website as well as somewhere between $3.5 and $4 million in Bitcoin used to buy drugs on the site.[24] This incident left a lingering perception for Bitcoin as being associated with criminal enterprises, despite the fact that in 2020 less than 0.5% of transactions were deemed as being utilized in illicit activities.[25]

Source: https://www.citivelocity.com/citigps/bitcoin/

BITCOIN FAKE MYTHS: MONEY LAUNDERING

Source: https://www.citivelocity.com/citigps/bitcoin/
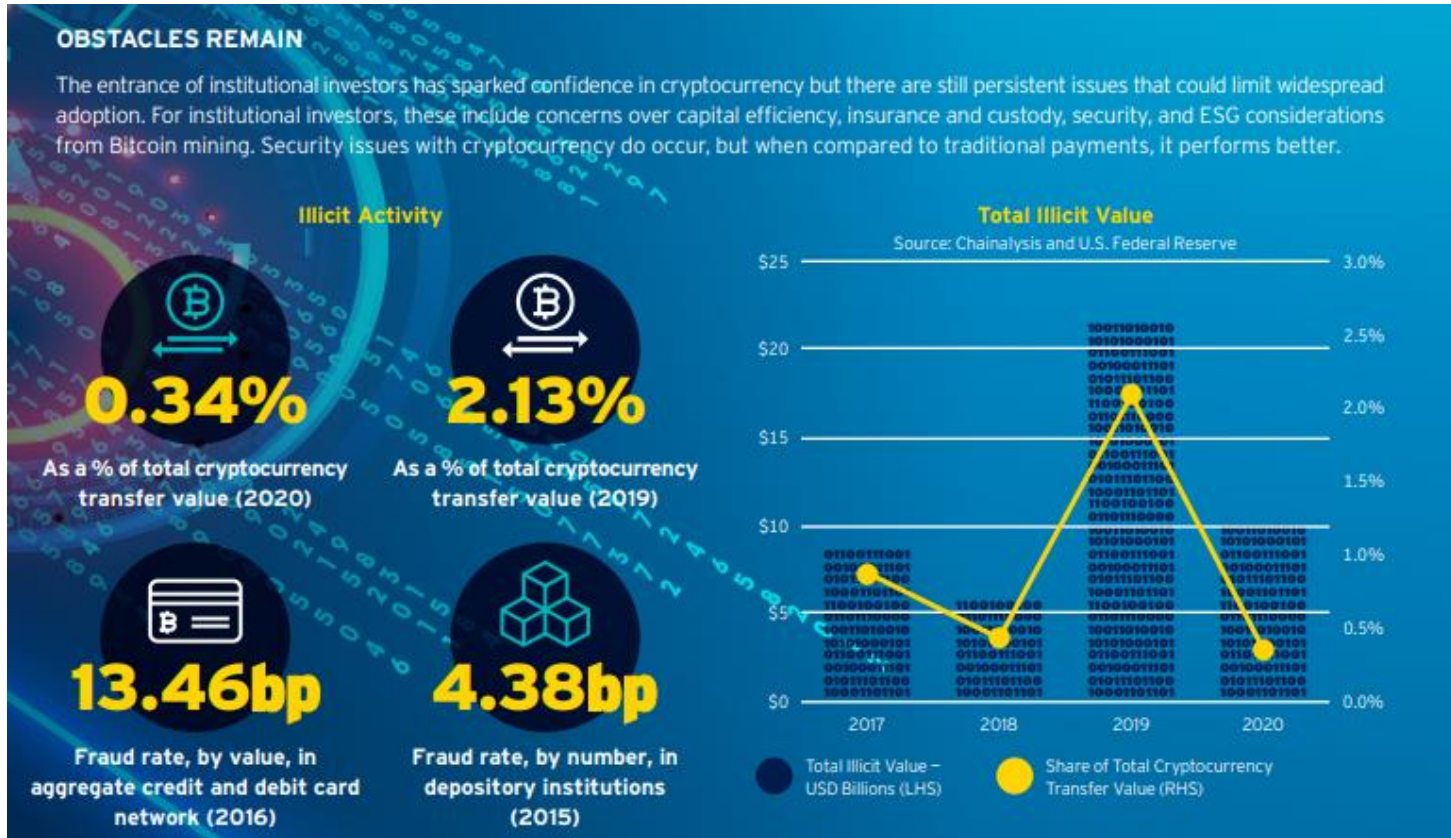
Why regulate?

REASON TO REGULATE

Some reasons to regulate cryptocurrencies:

- Money Fungibility.

- Avoid market manipulation and create trust in the market.

- Combatting money laundering and terrorism financing.

- Protection of investors

- Financial stability

- Tax

Those are the same reason while also the traditional markets are regulated

GEOGRAPHIC DISTRIBUTION OF THE CRYPTOASSET INDUSTRY

Number of identified entities

■ 1-2   ■ 3-5   ■ 6-10   ■ 11-20   ■ 21-50   ■ >50   ▨ Countries covered by survey sample
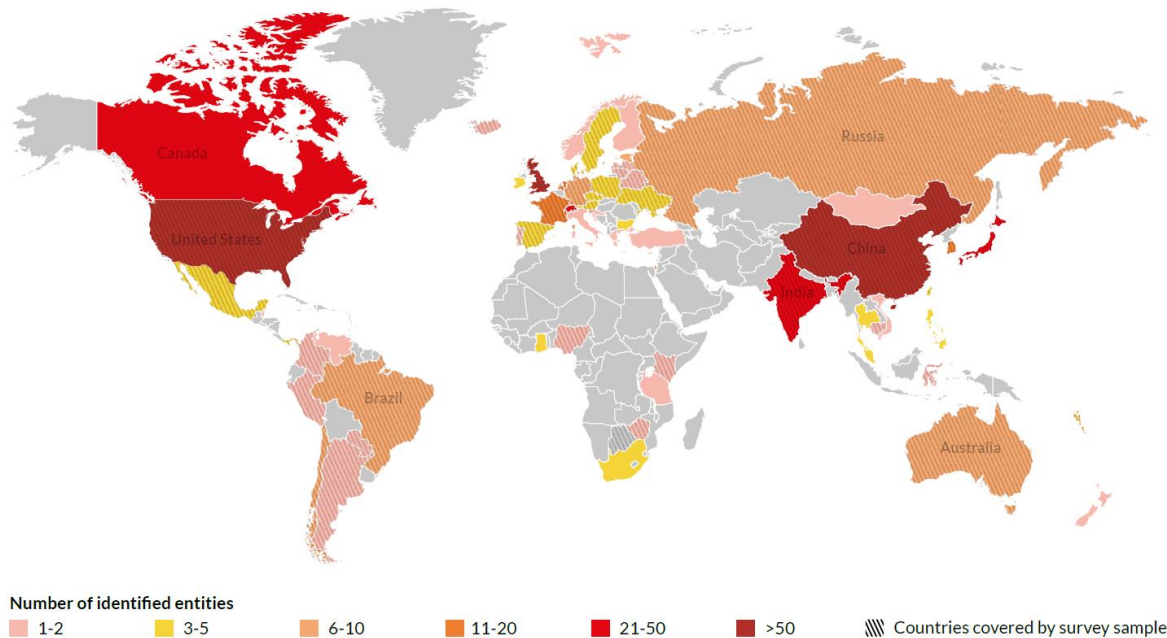
Note: this map is based on operational HQ data from 561 companies active in at least one of the four major cryptoasset industry segments. Colours represent the total number of identified entities from each country; stripes indicate when a country is also covered by our study sample.

Source: University of Cambridge 2nd Global Cryptoasset Benchmarking Study
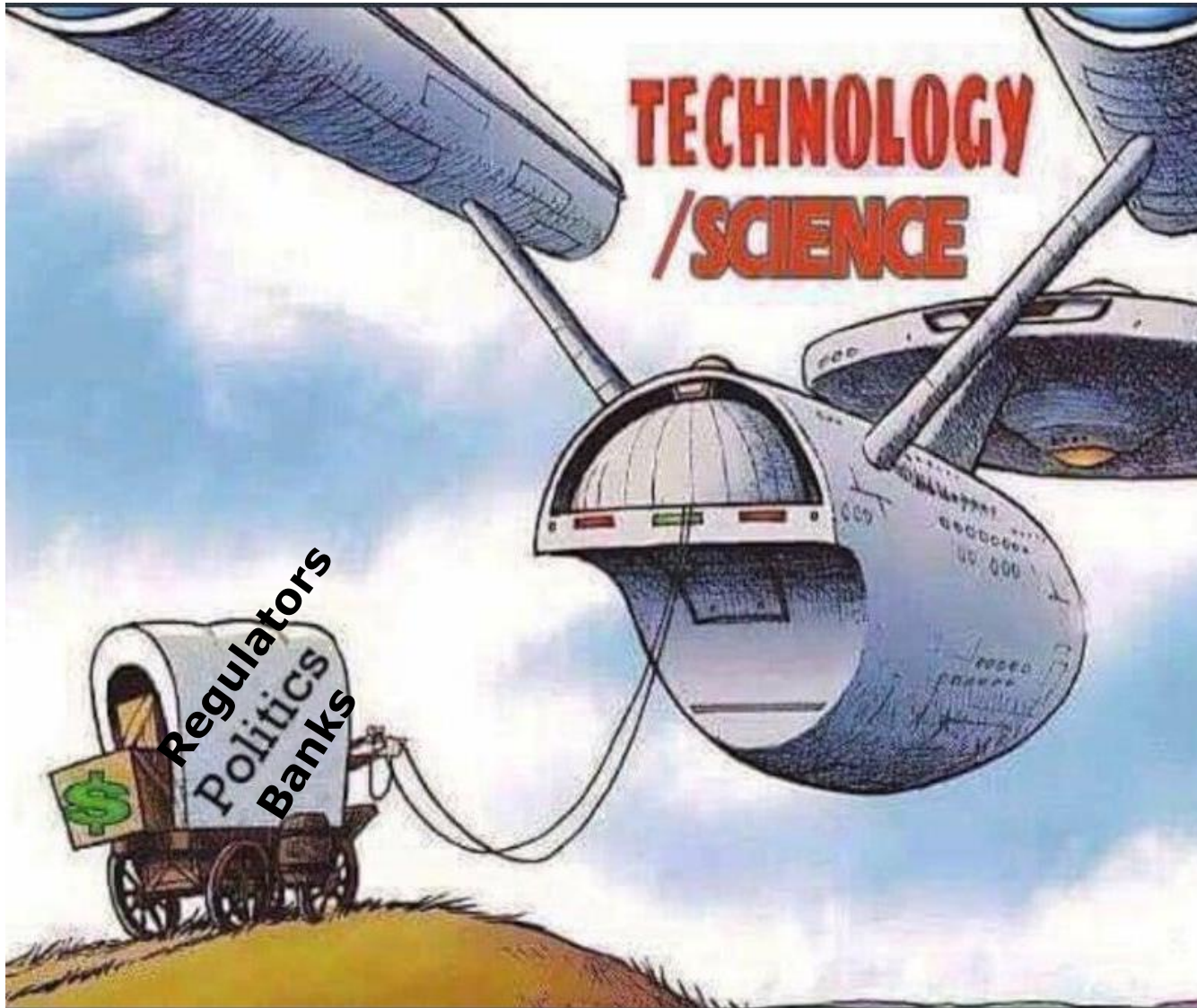
Blockchain and Law (Switzerland)

THE BIRTH OF BLOCKCHAIN AND CRYPTO REGULATION

– In 2014 the Swiss Federal Council published a report on cryptocurrencies

– cryptocurrencies carry substantial risks of loss and abuse but they are not in a legal vacuum: contracts with virtual currencies are enforceable in principle and penalties can be imposed for criminal offences.

– Bitcoin is qualified as a commodity, commerce through bitcoin is not subject to AML, but the offer of trading with cryptos requires such authorization.

– Given that virtual currencies are a marginal phenomenon (reminder, report dated 2014) and are not in a legal vacuum, the Federal Council sees no need for legislative measures at the moment.

The Federal Council
The portal of the Swiss government

...partments	Federal Chancellery	Federal law	Documentation	

...s > Federal Council publishes report on virtual currencies such as bitcoin

‹ Back to overview

Federal Council publishes report on virtual currencies such as bitcoin

Bern, 25.06.2014 - During its meeting today, the Federal Council adopted a report on the use of virtual currencies. It decided not to propose new statutory provisions, as virtual currencies like bitcoin are of only marginal economic significance and are not in a legal vacuum. Nevertheless, the competent authorities and consumer protection organisations should urge users to exercise caution when using bitcoins.

THE BIRTH OF BLOCKCHAIN AND CRYPTO REGULATION

– In February 2017 the Swiss Federal Council started a consultation on FinTech regulations

– aim to regulate fintech and other firms that provide services outside normal banking business according to their risk potential

– Simplified authorization until CHF 100 Mio with no lending business

  o Simplified operating requirements relative to the current banking license in the areas of accounting, auditing and deposit protection. Less stringent requirements particularly in the areas of minimum capital, own funds and liquidity would have to be regulated within the scope of implementing regulations to be issued later.

– Normal authorization if more than CHF 100 Mio

  o But with a case by case study that could allow simplified requirements if justified.

Federal Council initiates consultation on new Fintech regulations

Bern, 01.02.2017 - During its meeting on 1 February 2017, the Federal Council initiated the consultation on amendments to the Banking Act and Banking Ordinance in the fintech area. The revision should ensure that barriers to market entry for fintech firms are reduced and that the competitiveness of the Swiss financial centre is enhanced. The consultation will last until 8 May 2017.

The proposed amendments to the Banking Act (BankA) and Banking Ordinance (BankO) aim to regulate fintech and other firms which provide services outside normal banking business according to their risk potential. A form of deregulation with three supplementary elements is being proposed:

- First, the exception provided for in the Banking Ordinance for the acceptance of funds for settlement purposes (Art. 5 para. 3 lit. c of the BankO) should apply explicitly for settlements within 60 days (instead of only for settlements within seven days as was the practice up to now). For securities dealers, what should remain crucial is that the planned main transaction is organised and directly foreseeable. This change requires an amendment to the BankO.
- Furthermore, an innovation area should be created: the acceptance of public funds up to CHF 1 million should not be classified as operating on a commercial basis and can be exempt from authorisation. This change should allow firms to try out a business model before they are finally required to obtain authorisation in the case of public funds of over CHF 1 million. This change also requires an amendment to the BankO.

THE BIRTH OF BLOCKCHAIN AND CRYPTO REGULATION

– First rules entered in force on 1.8.17 (amendment in the banking ordinance) and FINMA Circular 08/3 on public deposits

– With this amendments a form of deregulation in relation with the accepted deposits is being proposed:

  o No authorization until CHF 1 Mio or 60 days settlement with no interest and information to users that company is not supervised by FINMA and deposits are not protected

  o Max 20 deposits of more of CHF 1 Mio for a maximum of 60 days are allowed.

– This change should allow firms to try out a business model before they are finally required to obtain authorization in the case of public funds of over CHF 1 million.

Federal Council puts new fintech rules into force

Bern, 05.07.2017 - During its meeting on 5 July 2017, the Federal Council adopted an amendment of the Banking Ordinance. It will enter into force on 1 August 2017. The revision should ensure that barriers to market entry for fintech firms are reduced and that the competitiveness of the Swiss financial centre is enhanced.

The amendment to the Banking Ordinance (BankO) aims to regulate fintech firms which provide services outside normal banking business according to their risk potential. The following simplifications are envisaged:

▪ First, the exception provided for in the Banking Ordinance for the acceptance of funds for settlement purposes will apply explicitly for settlements within 60 days – in accordance with the practice up to now, a period of seven days applies.

▪ Furthermore, an innovation area will be created: the acceptance of public funds up to CHF 1 million will no longer be classified as operating on a commercial basis in the future and will be exempt from authorisation. This change should allow firms to try out a business model before they are finally required to obtain authorisation in the case of public funds of over CHF 1 million. It should also be clearly stated to depositors that their deposits are not protected by deposit protection.

NEW SAND BOX LEGISLATION

– Second novation rule introduced with amendments of the Banking Act that will be in force on 01.01.2019

– Introduction of FinTech license:
  • deposits up to CHF 100 Mio
  • No interests
  • No asset management
  • Capital requirement: CHF 300'000
  • Reduced application of banking rules

Financial Services Act and Financial Institutions Act

19.06.2018 - The Financial Services Act (FinSA) and Financial Institutions Act (FinIA) are part of the new financial market architecture. Both acts will create uniform competitive conditions for financial intermediaries and improve client protection.

The FinSA contains rules for offering financial services and distributing financial instruments. The FinIA sets the authorisation conditions and organisational requirements for financial institutions subject to prudential (official) supervision.

Parliament adopted both bills in the final votes on 15 June 2018. The FinSA was accepted by 138 votes to 57 (National Council) and 41 votes to 0 (Council of States); the FinIA passed with 139 votes to 56 (National Council) and 44 votes to 0 (Council of States).

REGULATOR ACTIVITY DURING THE LEGAL SET UP

–   Issue of guidelines

–   Setup of a FinTech Department within FINMA

–   Clear statement that laws will be applied in a techno neutral way:

   o   AML applicable to financial intermediaries (no need to action against AML, no special rules like 4th EU AML directive required since this rules are already in place)

   o   Authorization to be requested if the activity fall under the application of the banking act, the collective investment scheme act or the financial infrastructure act.

   o   Opening enforcement procedures against illegal behaviours

---

19 September 2017   Press release

FINMA closes down coin providers and issues warning about fake cryptocurrencies

The Financial Market Supervisory Authority FINMA has closed down the unauthorised providers of the fake cryptocurrency "E-Coin". The developers of E-Coin had accepted some million Swiss francs in public deposits without holding the required banking licence. FINMA has also launched bankruptcy proceedings against the legal entities involved.

For over a year since 2016, the QUID PRO QUO Association had been issuing so-called "E-Coins", a fake cryptocurrency developed by the association itself. Working together with DIGITAL TRADING AG and Marcelco Group AG, the association gave interested parties access to an online platform on which E-Coins could be traded and transferred. Via this platform, these three legal entities accepted funds amounting to at least four million Swiss francs from several hundred users and operated virtual accounts for them in both legal tender and E-Coins. This activity is similar to the deposit-taking business of a bank and is illegal unless the company in question holds the relevant financial market licence.

FINMA liquidates the companies

FINMA GUIDELINES

February 2018 first FINMA ICOs guidelines

– Clarification on the qualification of the token, introducing legal certitude on utility, payment and asset tokens

– Evaluation of the application of financial laws on the use of tokens

September 2019

– Supplement to the ICO guidelines

– Qualification of stable coins

Guidelines

for enquiries regarding the regulatory framework for initial coin offerings (ICOs)

Published 16 February 2018

1 Purpose

BANKING SOFT REGULATION

–   Non binding rules for opening of corporate accounts for blockchain companies, including ICO

–   In case of utility token, no KYC up to CHF 15'000

–   In case of payment token, simplified KYC (only simple ID copy) up to CHF 3'000

–   Detailed AML analysis in case of transactions above CHF 100'000

–   However, KYC required also for utility token, even if according to FINMA those are not subject to AML

•SwissBanking

Press release | Basel, 20. September 2018

Opening corporate accounts for blockchain companies
Swiss Bankers Association publishes guidelines for its members

- The guidelines issued by the Swiss Bankers Association (SBA) support banks in opening corporate accounts for companies with a connection to blockchain.
- The guidelines are intended to reduce risk in business between banks and companies involved in blockchain technology.
- They build on the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB) and cover questions regarding blockchain.

DISPATHC ON THE FURTHER IMPROVEMENT OF THE FRAMEWORK CONDITION FOR DLT

– November 2019

– dispatch on the further improvement of the framework conditions for DLT/blockchain

– Implementing the amendments required in order to have DLT/blockchain as a legal register

– Main Amendments:
  – civil law, for the transfer of rights
  – insolvency law, segregation of cryptoassets
  – financial market law, new authorization
  – anti-money laundering law, about decentralized trading platforms

Federal Council wants to further improve framework conditions for DLT/blockchain

Bern, 27.11.2019 - During its meeting on 27 November 2019, the Federal Council adopted the dispatch on the further improvement of the framework conditions for DLT/blockchain. The proposal is aimed at increasing legal certainty, removing barriers for applications based on distributed ledger technology (DLT) and reducing the risk of abuse.

In December 2018, the Federal Council published a report on the legal framework for blockchain and DLT in the financial sector. It emphasised that it wants to create the best possible framework conditions so that Switzerland can establish itself and evolve as a leading, innovative and sustainable location for fintech and DLT companies. Moreover, it wants to consistently combat abuses and ensure the integrity and good reputation of Switzerland as a financial centre and business location.

Among other things, the report showed that Switzerland's current legal framework is already well suited to dealing with new technologies, including DLT. Nevertheless, it also pointed out the need for action in certain areas, which is why the Federal Council already submitted a series of amendments to existing legislation for consultation in March 2019. However, it refrained from drawing up a specific technology act. Some 80 responses were received during the consultation process. All the participants welcomed the Federal Council's proposal in principle.

LAW ON THE AMENDMENT OF FEDERAL LAWS TO THE DEVELOPMENTS OF THE DLT TECHNOLOGY

– Approuved on 25.09.2020, probably entering in force on 1.7.2021

– Not a single vote against the law!

– Main Amendments:
  – civil law, for the transfer of rights
  – insolvency law, segregation of cryptoassets
  – financial market law, new authorization
  – anti-money laundering law, about decentralized trading platforms

– A description of the single amendments will be done in the next slides
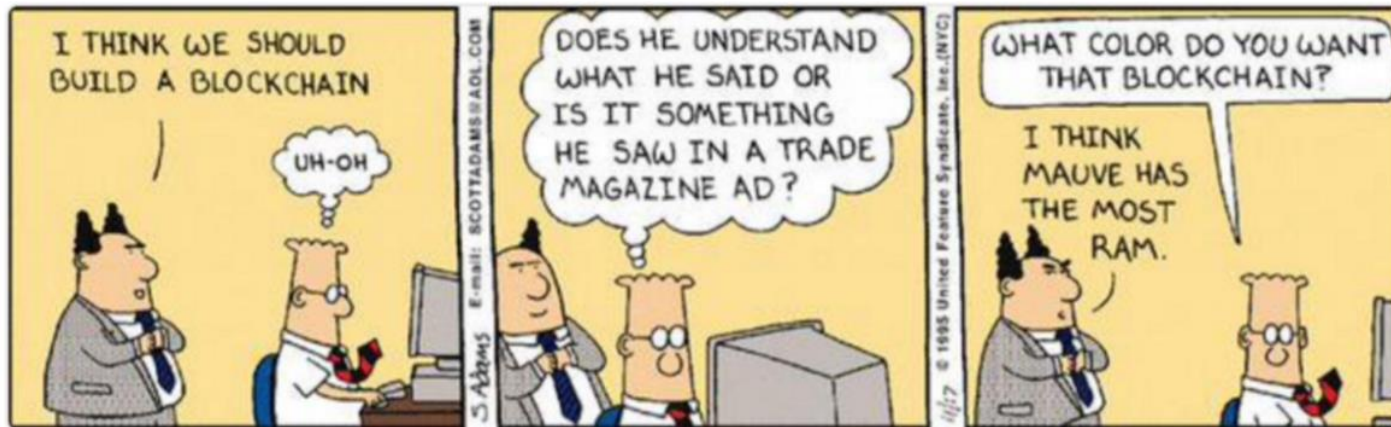
Termine di referendum: 14 gennaio 2021

Legge federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito

del 25 settembre 2020

L'Assemblea federale della Confederazione Svizzera,
visto il messaggio del Consiglio federale del 27 novembre 2019[1],
decreta:

CONCLUSION

READY FOR THE BLOCKCHAIN?

WHO IS SATOSHI NAKAMOTO?

– Check this:

https://cryptonomist.ch/en/blockchain-en/the-white-paper/

Lars Schlichting

Partner
Attorney at Law
LLM

Via Canova 15
6901 Lugano

lars.schlichting@kellerhals-carrard.ch
+41 79 391 91 70