CENTRO
DI STUDI BANCARI
VILLA NEGRONI
ASSOCIAZIONE BANCARIA TICINESE

Organismo di Autodisciplina OAD FCT dei Fiduciari del Cantone Ticino

# WORKSHOP SUL TRADING DELLE CRIPTOVALUTE: FONDAMENTI, OPPORTUNITÀ E RISCHI DEL TRADING ATTIVO E PASSIVO

**5 giugno 2019**

Relatori

**Roberto Gorini**, *CEO Noku SA, Zugo/Lugano*
**Filippo Moor**, *CEO, BitIncubator & Venture SA, Lugano*
**Lars Schlichting**, *Avvocato, Kellerhals Carrard Lugano SA, Lugano*

# Indice

CENTRO
DI STUDI BANCARI
VILLA NEGRONI
ASSOCIAZIONE BANCARIA TICINESE

# What is bitcoin?
# basi di conoscenza per operare con le criptovalute

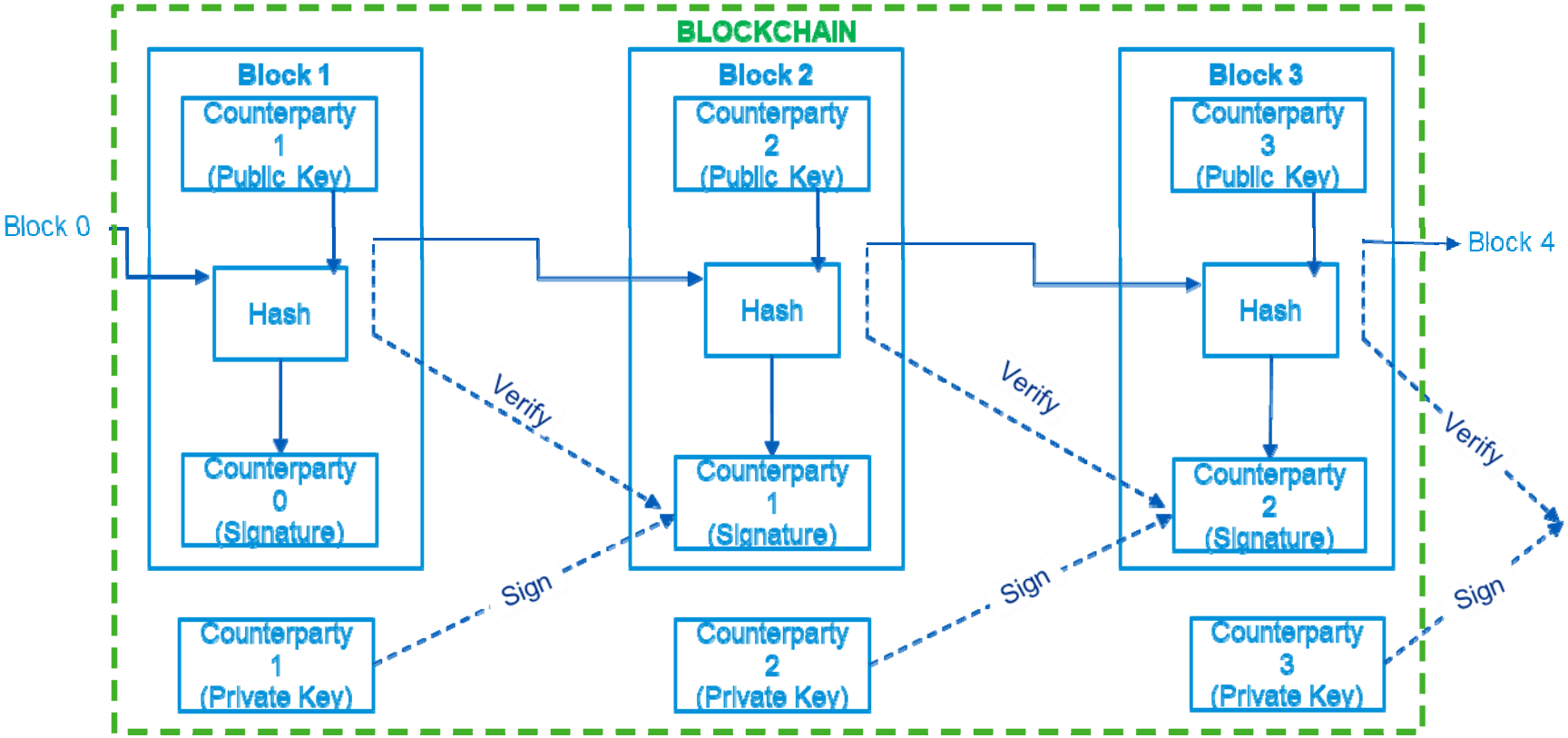


Kellerhals Carrard

# What is Blockchain?

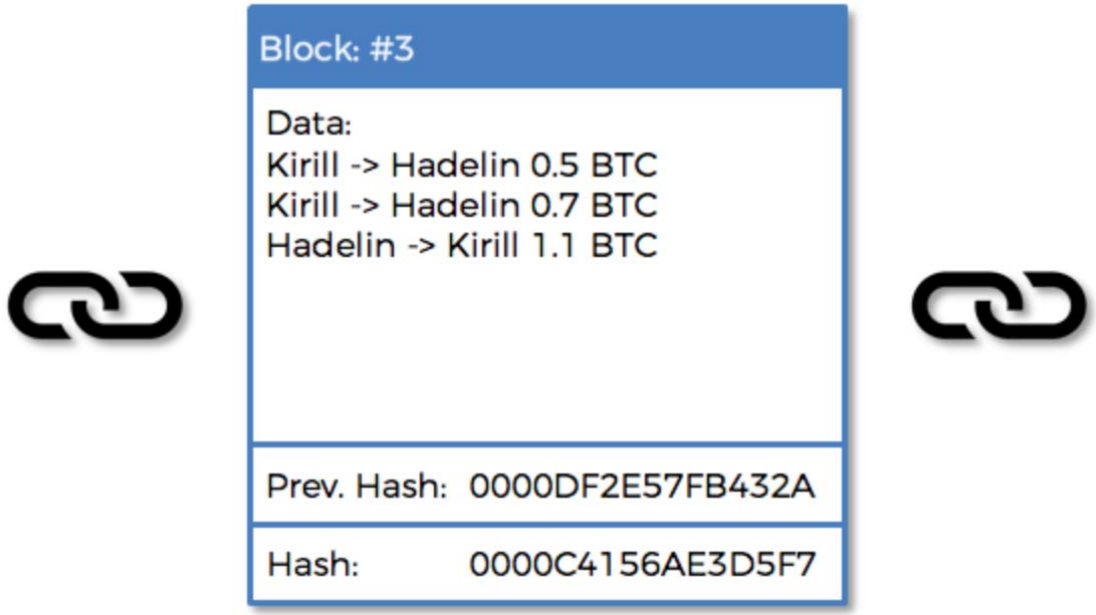
# BLOCKCHAIN

A **Blockchain is a permanent record of transactions** in a network. The system is protected by using a reference to the previous block («hash»), which is encrypted. Thus, a break-in in the system would be so evident that it could immediately be detected and ultimately cancelled.



# HOW DOES BLOCKCHAIN MINING WORK?

Cryptographic hash




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

# HOW DOES BLOCKCHAIN MINING WORK?

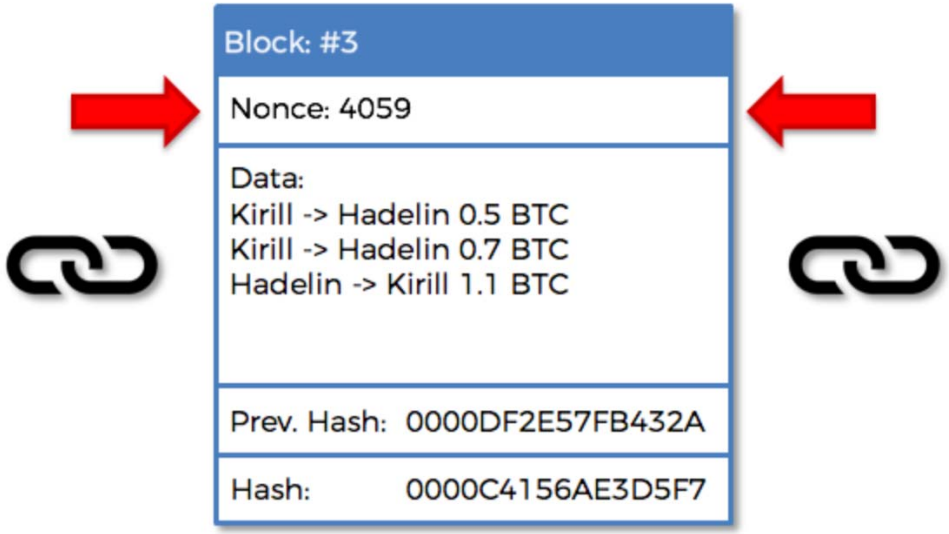
SHA256(Block Number, Data, Previous Block's Hash) -> Hash


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




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.

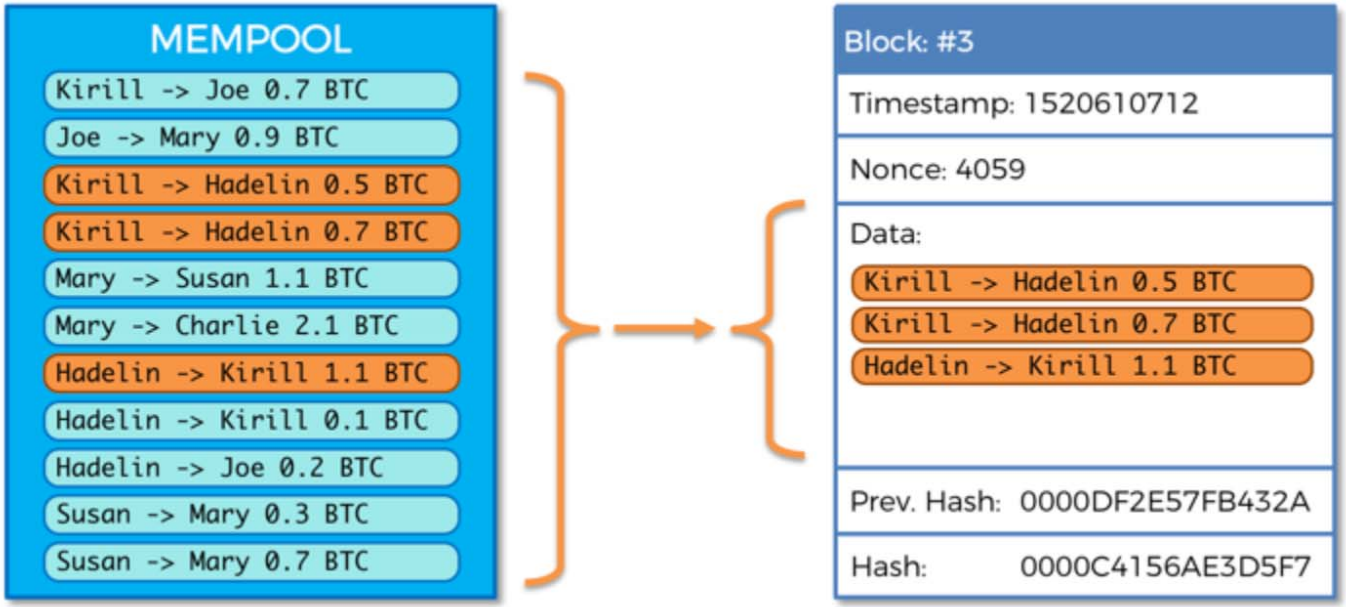
# HOW DOES BLOCKCHAIN MINING WORK?

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 !

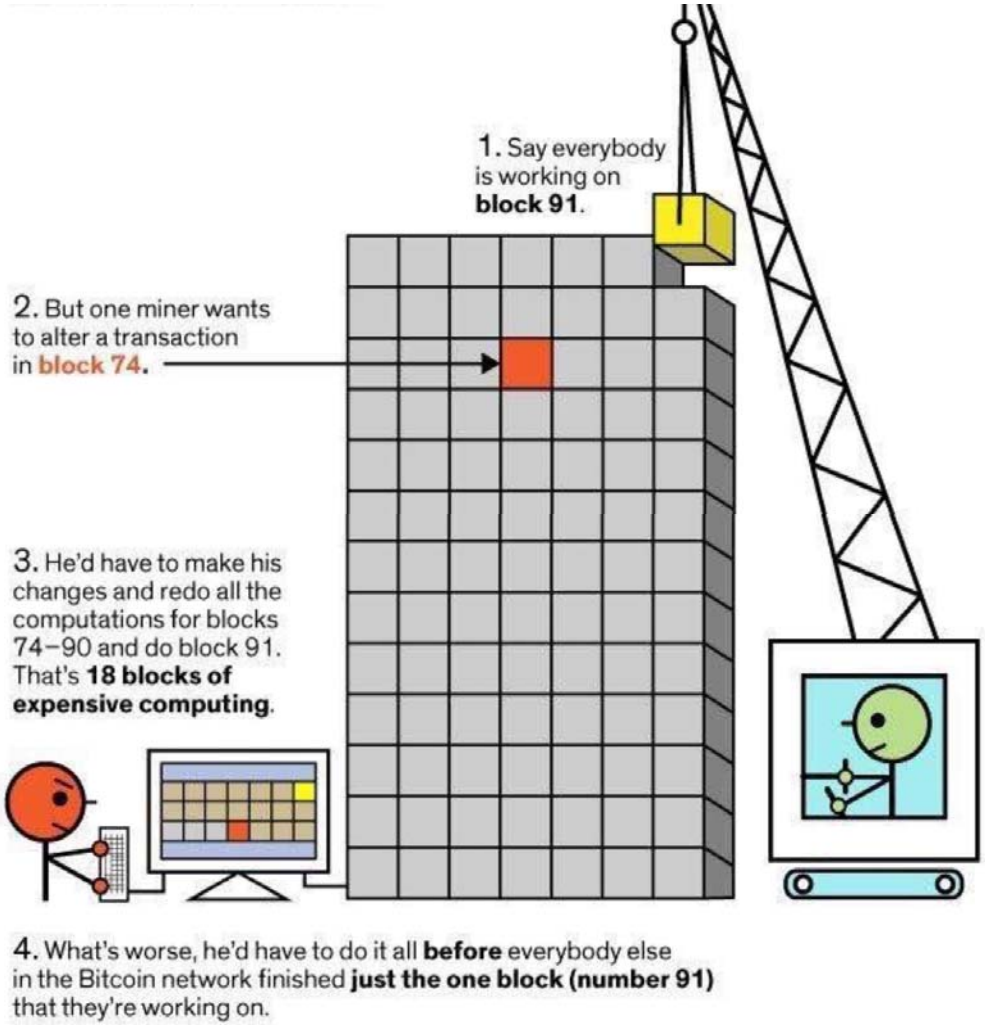

Source: Medium, How does Bitcoin/blockchain mining works?

# HOW DOES BLOCKCHAIN MINING WORK?



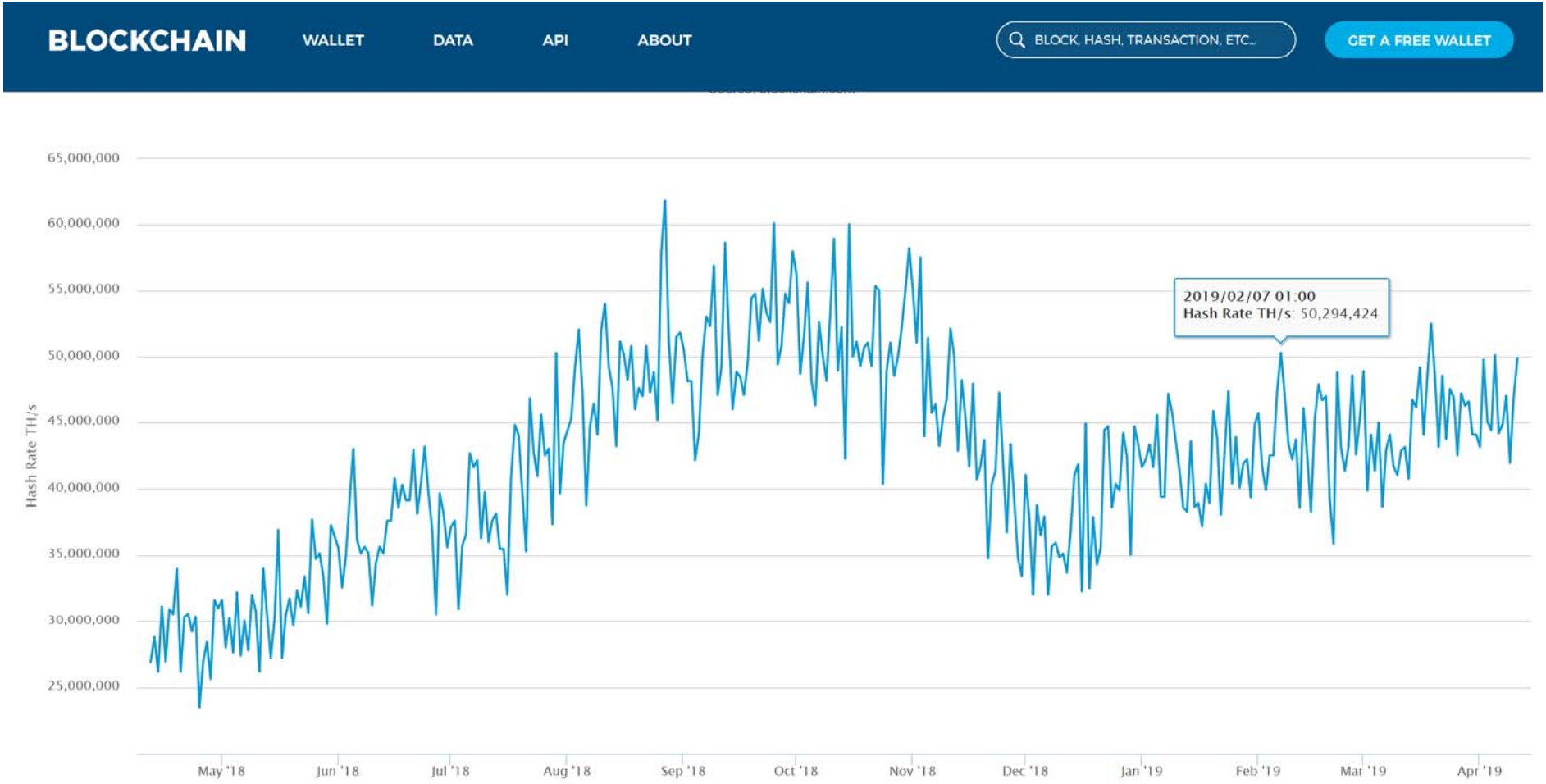

Source: Medium, How does Bitcoin/blockchain mining works?

# WHY YOU CAN’T CHEAT AT BITCOIN




Source: LinkedIn publication

# THE HASHRATE POWER



# WHAT ARE CRYPTOCURRENCIES AND TOKEN?

# DEFINITION

a. EBA (2014): “a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically” https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

b. 5° EU AML Directive (2018): “virtual currencies” means a representation of digital value that is not issued or guaranteed by a central bank or a public body, is not necessarily linked to a legally established currency, does not have the legal status of currency or currency, but is accepted by physical and legal people as a medium of exchange and can be transferred, stored and exchanged electronically”

c. FINMA ICO Guidance (2018): *Payment tokens [m*eans of payment for goods or services] vs *Utility tokens [*give their holders access to blockchainpowered services or platforms] vs a*sset tokens [r*epresent debt or equity claim on the issuer]

# DEFINITION

d. ESMA (2018): “A virtual currency is a digital representation of value that is neither issued by a central bank or a public authority , rarely attached to a fiat currency, but is accepted by a growing number of natural or legal persons as a means of payment and can be transferred, stored or traded electronically” https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf

e. FATF (2018): “A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.” http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

# 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?

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.

# A BRIEF HISTORY OF BITCOIN MARKET

| Year | Highest price USD | Comment |
|---|---|---|
| 2009 | 0 | No market for bitcoin so no real price |
| 2010 | 0.39 | Someone bough 2 pizza for 10’000 btc |
| 2011 | 31 | First bubble, btc rise from USD 1 to 31 for 6 days and than collapst to USD 2 |
| 2012 | 7.08 | First 2 bear markets, price loose 40% in 185 days from 7.08 to 4.22, recover and loose another 35%before end of the year |
| 2013 | 1’149 | Explosing of the secondo buble and start of the second bear market which will last for 415 days |

# A BRIEF HISTORY OF BITCOIN MARKET

| Year | Highest price USD | Comment |
|---|---|---|
| 2014 | 770 | Year of the bear market, with prices declining during all the year reaching a low of USD 195 |
| 2015 | 333 | End of the bear market and cumulation period |
| 2016 | 960 | Recovering to the previous high |
| 2017 | 19’800 | Year of the third bubble |
| 2018 | 17’090 | Year of the bear market, with price collapasing to USD 3’270 |
| 2019 | ? | If the price follow the past patterns, we will see the highest price probably by year end |

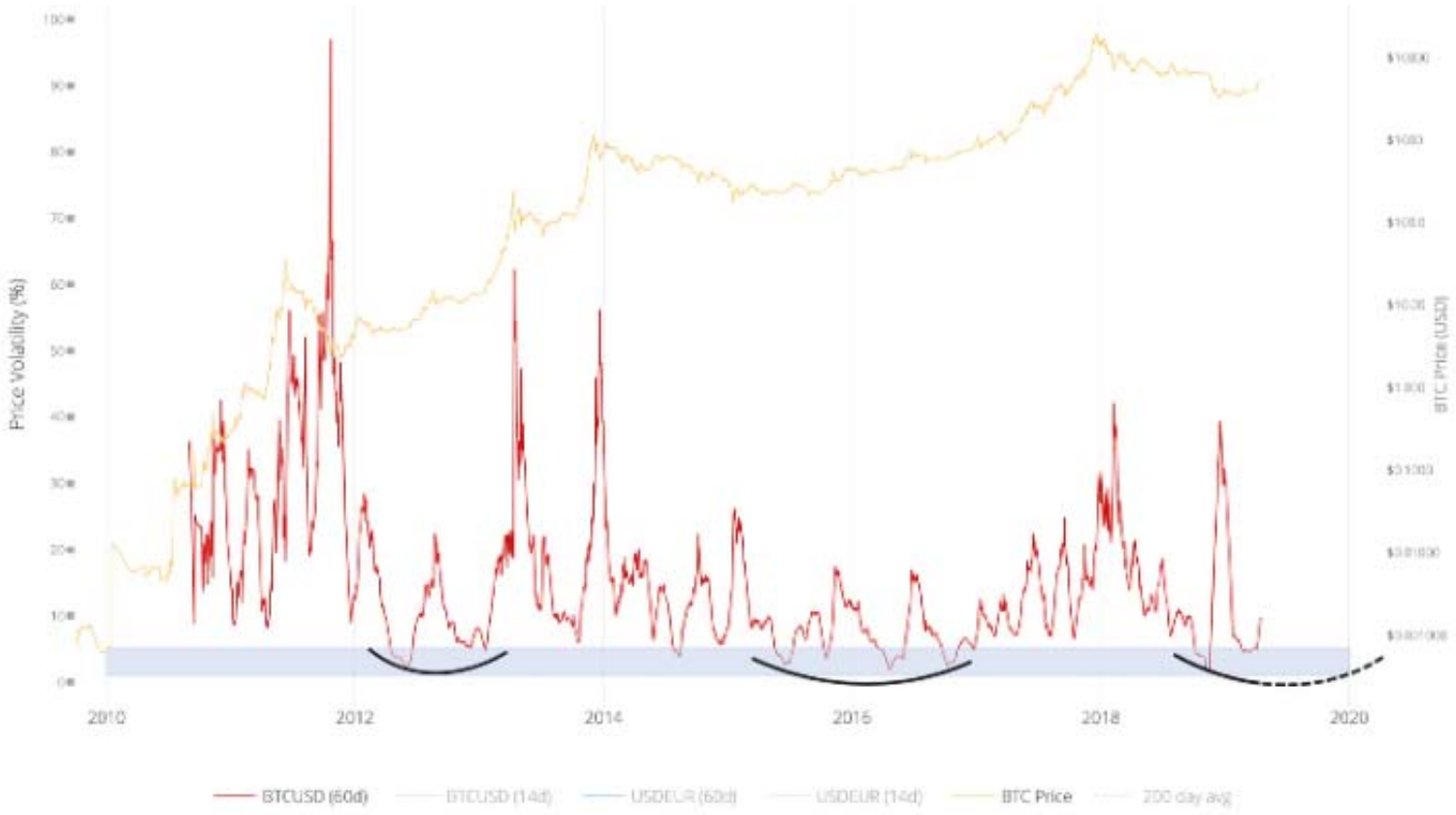
# A BRIEF HISTORY OF BITCOIN MARKET

| | DATE | DAYS | BTC PRICE | % GAIN | % PER DAY |
|---|---|---|---|---|---|
| First peak | 09/06/2011 | 449 | 30 | 984567% | 1.36% |
| First trough | 11/20/2011 | 164 | 2 | -92% | -1.64% |
| Second peak | 11/30/2013 | 741 | 1,133 | 50921% | 0.86% |
| Second trough | 01/15/2015 | 410 | 175 | -85% | -0.45% |
| Third peak | 12/17/2017 | 1068 | 19,494 | 9480% | 0.44% |
| Third trough | 12/16/2018 | 345 | 3,141 | -84% | -0.53% |

Source: Adamant Capital, Bitcoin in heavy accumulation, April 18, 2019

# A BRIEF HISTORY OF BITCOIN MARKET


# BRIEF HISTORY OF BITCOIN MARKET




Volatility is decreasing

Source: Adamant Capital, Bitcoin in heavy accumulation, April 18, 2019

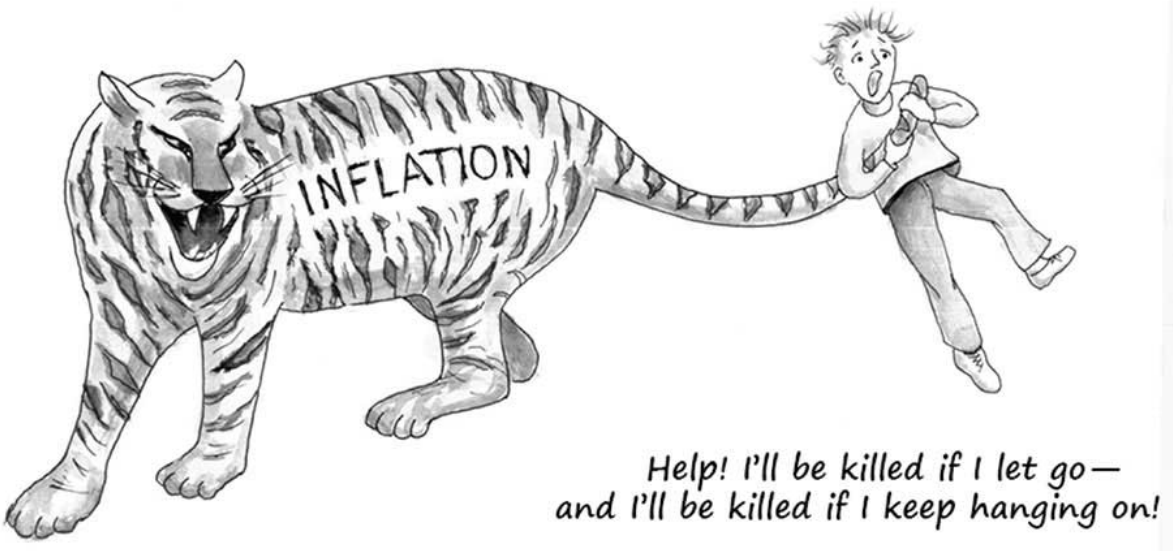
# A BRIEF HISTORY OF BITCOIN MARKET

a. Bitcoin is highly influenced by specific events and narratives, both positive and negative (eg. Mt. Gox, Silk road, Cryprus crisis, etc…), as well as through news outlets and social media channels.

# CRYPTOCURRENCY AND MONEY

# FRIEDRICH VON HAYECK

a. Austrian-British economist and philosopher
b. shared the 1974 Nobel Memorial Prize in Economic Sciences with Gunnar Myrdal for his pioneering work in the <u>theory of money</u>
c. Inflation Theory

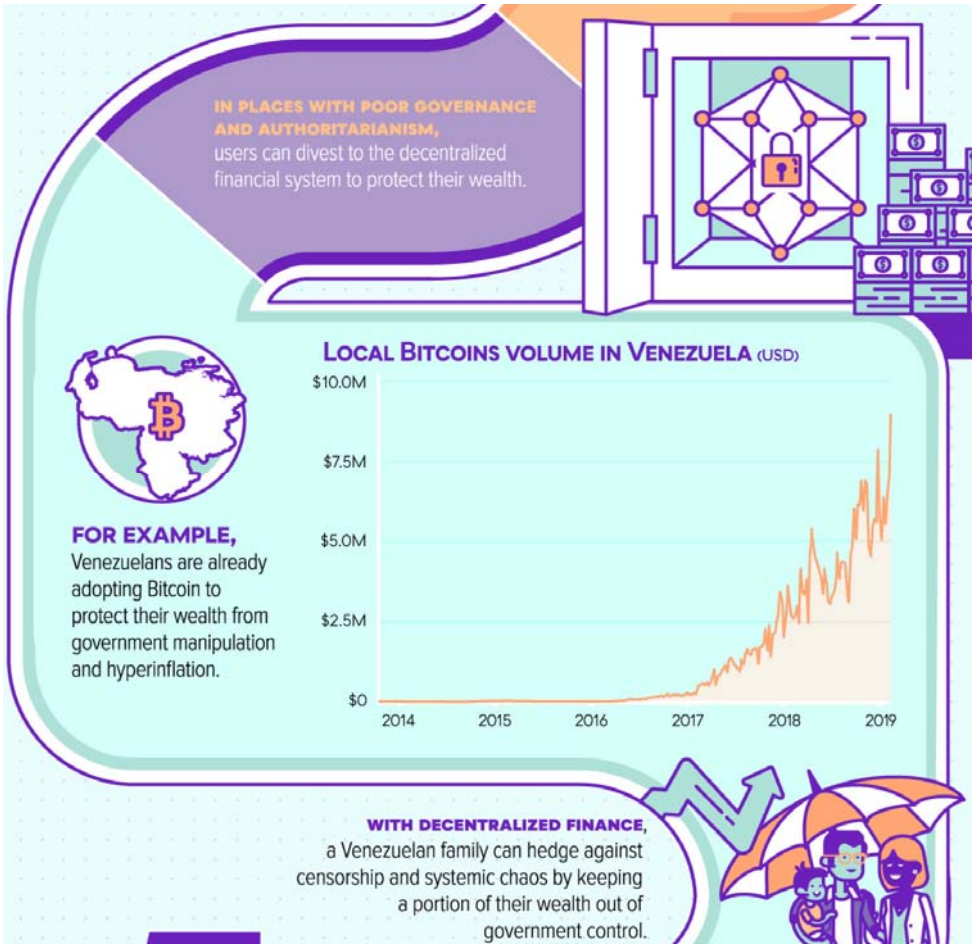


# FRIEDRICH VON HAYECK

Hayeck Inflation Theory (source http://www.essentialhayek.org/Essential-Hayek-ch08):

- Inflation is a decline in money's purchasing power.
- By far the most common cause of inflation is an increase in the supply of money.
- stopping inflation is easy in principle, but made difficult by politics, not least because it is politics that usually is to blame for starting inflation in the first place.
- Fiat money is money backed by nothing other than faith in the government that issues it.
- Solution: denationalization of money, getting government completely out of the business of issuing money and controlling the money supply
- Competitive market forces would instead be responsible for supplying sound money.

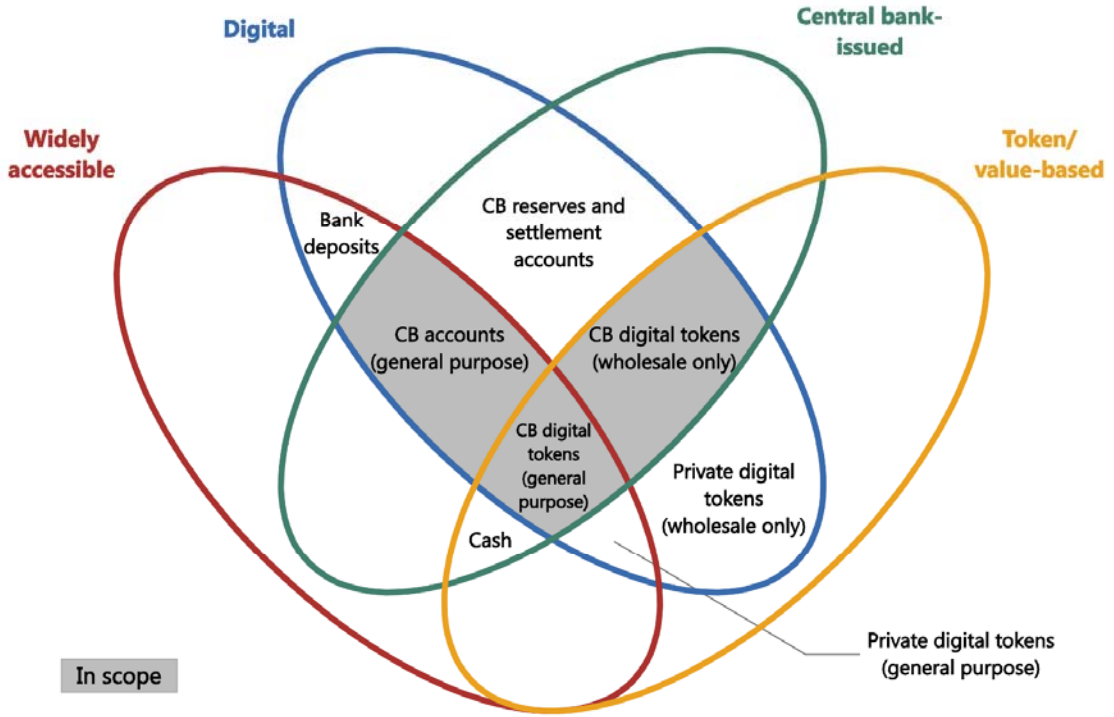
# A REAL EXAMPLE OF HAYECK INFLATION THEORY




Source: visualcapitalist.com

# WHAT IS MONEY

The money flower: a taxonomy of money — Graph 1




The Venn diagram illustrates the four key properties of money: *issuer* (central bank or not); *form* (digital or physical); *accessibility* (widely or restricted); and *technology* (account-based or token-based). CB = central bank. *Private digital tokens (general purpose)* include cryptocurrencies, such as Bitcoin. For examples of how other forms of money may fit in the diagram, please refer to the source.

Sources: CPMI-MC (2018); Bech and Garratt (2017).

# MONEY ISSUANCE

a. Only the Swiss National Bank can issues the Swiss Franc, which is the only official mean of payment in Switzerland (art. 99 Cost., art. 4 National Bank Act). Nobody can refuse the Swiss Franc as a mean of payment (Art. 3 Federal Act on Currency and Payment Instruments).

b. However, any other value can be used as a mean of payment as far as all the party involved agrees on it.

c. Only banks can accepts deposit from the public (not only in Swiss franc, but in any other value, art. 1 Banking Act)

# ACCEPTANCE OF BITCOIN AS PUBLIC DEPOSIT

a. Acceptance of bitcoin can be qualified as a public **deposit** (which required a banking licence) if
   - (i) the client cannot dispose of Bitcoins any time without the involvement of a dealer or custodian,
   - (ii) the dealer or custodian has a repayment obligation to the client, and
   - (iii) the accepted Bitcoins would be included in the bankruptcy assets of the dealer or custodian in the event of bankruptcy.

b. Accordingly, the safekeeping of tokens is not considered to be a deposit business subject to authorisation in line with FINMA practice if the balance is transferred solely for secure safekeeping, is held (directly) on the blockchain and can be attributed to the individual client at any time. In this case the provider act as a **custodian** of crypto asset.

(source, federal council blockchain report, page 86)

# ACCEPTANCE OF BITCOIN AS PUBLIC DEPOSIT

The treatment of tokens and similar assets under bank insolvency law cannot be separated from the general treatment of such assets in the case of insolvency in accordance with DEBA.

The provisions under banking law must ultimately be understood as special provisions supplementing DEBA, with DEBA taking a subsidiary role in the context of bank insolvency proceedings.

The Federal Council intends to review the treatment of tokens in the case of bank insolvency and to amend BankA in line with the planned amendments to general insolvency law.

(source, federal council blockchain report, page 92)

# CONSEQUENCES OF THE DISTINCTION DEPOSIT VS CUSTODIAN

| DEPOSIT | CUSTODY |
|---|---|
| Finma authorization is required | No authorisation is required |
| Digital asset to fall within the bankrupcy mass of the deposit provider andused for the proportionate satisfaction of creditors | Digital asset to be segregated from the bankrupcy mass |

# ACCEPTING DEPOSITS FROM THE PUBLIC

Banking Licence required:

- Accepting assets for more than CHF 100 Mio
- Publicly advertise to accept assets for more than CHF 100 Mio
- Accepting assets for less than CHF 100 Mio but investing them or rewarding the deposit
- it refinances with several non-participating banks its capital, with the aim of financing an indeterminate number of persons
- Legal references: art. 1a Banking Act, art. 2 Banking Ordinance

Banking Licence Light required:

- Accepting assets for less than CHF 100 Mio without investing them or rewarding the deposit
- Publicly advertize to accept assets for less than CHF 100 Mio without investing them or rewarding the deposit
- Legal references: art. 1a$^{bis}$ Banking Act, art. 14a ff Banking Ordonnance

No Banking Licence required:

- Accepting assets for less than CHF 1 Mio without investing them or rewarding the deposit and inform investors that there is no FINMA supervision or deposits protection
- Accepting deposits for less than 20 persons without publicly advertise to accepts assets
- Accepting assets which are not considerate as deposit from the public according to art. 5 Banking Ordinance
- Accepting assets which are not considerate as deposit according to art. 5 par. 3 Banking
- Legal references: art. 1a$^{bis}$ Banking Act, art. 5 and 6 Banking Ordinance, Circular FINMA 08/3

# ACCEPTING DEPOSITS FROM THE PUBLIC

Exemption according to Art. 5 BankO

a) *Consideration for the acquisition of property or the use of services*

b) *Bonds*

c) *Settlements accounts*

d) *Money entered into a means of payment or payment system up to CHF 3'000*

e) *Money with a default guarantee from a bank*

# ACCEPTING DEPOSITS FROM THE PUBLIC

FINMA, in its Circulare 08/3 was very restrictive about the sandbox rule, in fact:

a. deposits paid in by clients must remain constant and liquid until they are passed on or repaid. Deposits may not be held in the company's normal business accounts for day-to-day operations, instead at least one separate bank account must be opened for holding deposits (Circ. FINMA 08/3, no. 8.2).

b. This restrictive interpretation severely limits the application possibilities for the new "Fintech license". The only possible options are business models in the areas of brokerage (e.g. crowdlending) or payment service providers (e.g. pre-paid issuers, top-up wallets).

c. the execution accounts exception according to art. 5 par. 3 lit. c BankO is not applicable for crypto exchanger (Circ. FINMA 08/3 no. 16.2)

# WILL BITCOIN EVER BE A PAYMENT SYSTEM?


Source: visualcapitalist.com

# WILL BITCOIN EVER BE A PAYMENT SYSTEM?

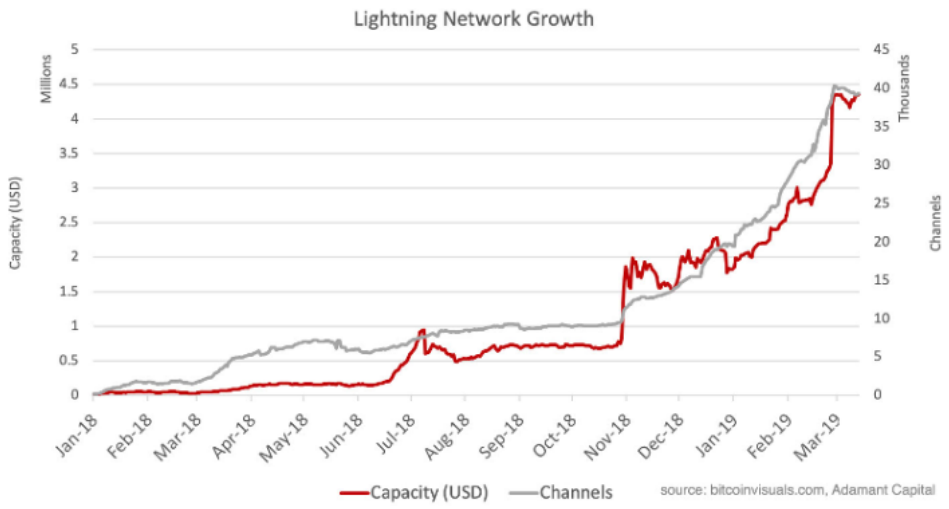
a. However, with lighting network, a secondo layer on the bitcoin blockchain, the number of transaction per second can increase to unlimited, depending only on the number of nodes

b. Lighting Network Torch (1Q 2019)

# WILL BITCOIN EVER BE A PAYMENT SYSTEM?

**BOTTOM-UP SCALING**

Bitcoin stays close to its roots of being a lightweight, robust, and universally accessible protocol. It is now possible to connect to the network via satellite and to run a full node on an off-the-shelf android phone. At the same time we're now seeing Satoshi's vision of payment channels on top of Bitcoin implemented as the Bitcoin Lightning Network, which over time will allow for millions of Bitcoin payments per second. Over the past year, the Lighting Network has seen monthly growth rates of over 45%:

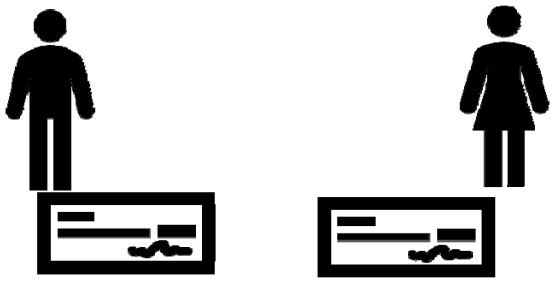



Source: Adamant Capital, Bitcoin in heavy accumulation, April 18, 2019

# CIVIL LAW ASPECTS OF HOLDING TOKEN

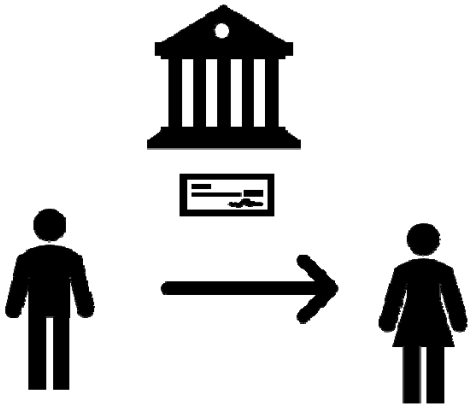
# THE STORY OF NEGOTIABLE SECURITY

– Order Instrument



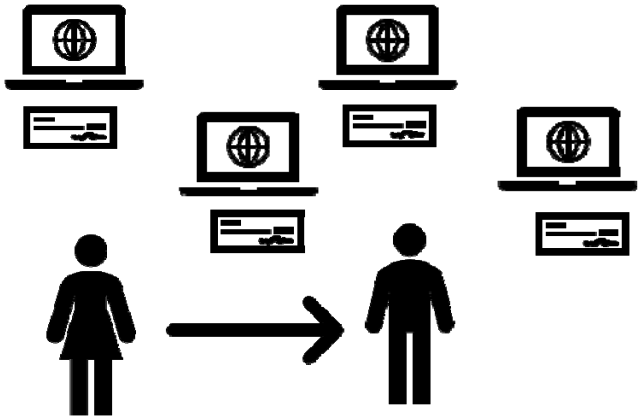
Those who had purchased a credit from a stranger wanted to be able to trust in the right to dispose of the transferor and in the securitized right

– Global certificate



Order Instruments have been replaced by the trust placed in banks and in their accounting records

– Token on a blockchain



With the representation of rights through tokens, individual negotiate rights again directly, without referring to a trusted intermediary

# CAN A TOKEN BE A LEGALLY OWNED?

a. Since rights in rem can be asserted against anyone, they should also be recognizable to everyone (principle of publicity).
b. As a rule, publicity is fulfilled by the possession of the object. In exceptional cases, register entries may fulfil the principle of publicity.
c. Is blockchain recognized as such a register? Does the ownership of a token stay in relation with the private key?
d. This point need to be clarified in order to have legal certitude about the ownership of a token.
e. Amendment of the Code of obligation, new Art. 973d CO allow the creation of uncertificated securities on the blockchain and allow the issue of recognizable rights on a distributed ledger

# EFFECTS OF A TOKEN, ART. 973E PRELIMINARY DRAFT CO

a. Presentation effect: execution of a claim only against the token (I do not look at the contract behind that token)
b. Legitimation effect: the token holder is the owner of the claim
c. Good fait effect: even the buyer of a stolen token can claim the execution of the service if he is in good faith
d. restriction of opposable exceptions: only those exceptions coming from the use of the blockchain or the holder of the token can be invoked
e. Paper form has priority over TDR

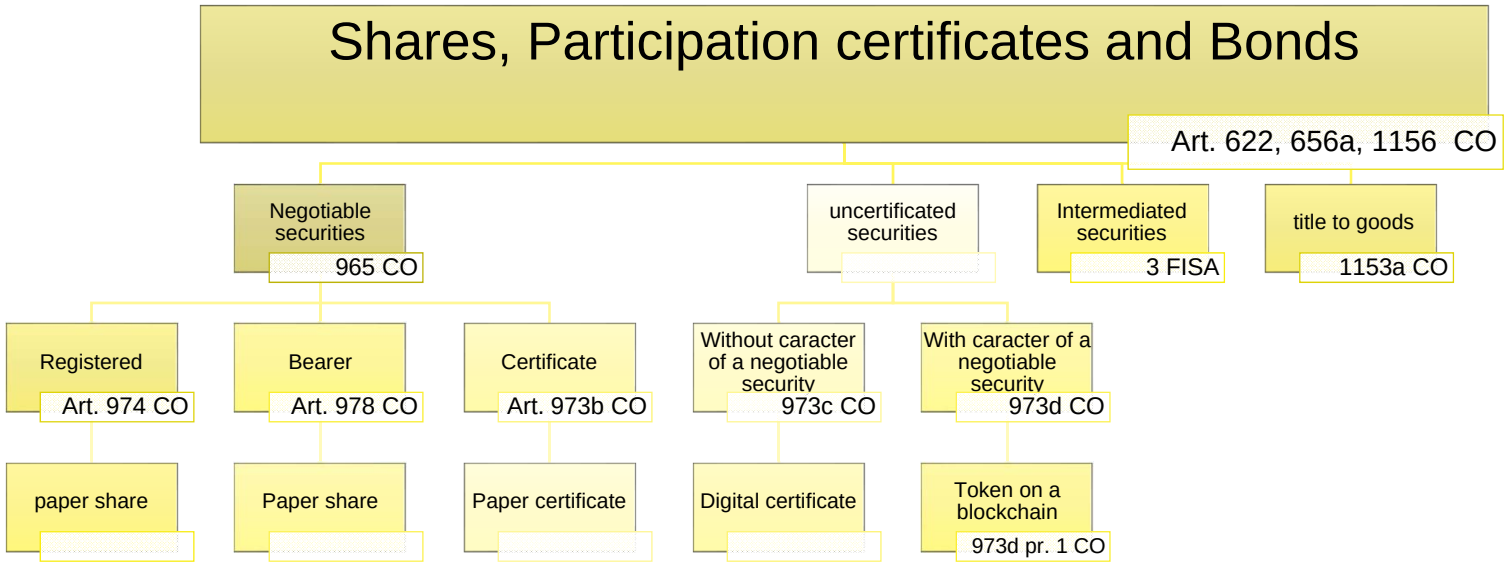
# ARE TOKEN SECURITIES (ART. 2 LETT. B FMIA)?

a. **certificated securities** are tangible objects embodying or objectifying rights. In other words, the special rules of securities law are based on the linking of a non-physical right with a physical object. The concept of a security thus does not appear readily available to digitalization

b. According to some authors, the issuance of **uncertificated securities** would have to be intentional, if an issuer of a token does not have the intention to create an uncertificated security, this view holds that tokens should be defined as uncertificated securities only with reservations (but this is not FINMA approach)

c. The Federal Intermediated Securities Act (FISA),regulates the custody of certificated and uncertificated securities by custodians and their transfer. It applies to **intermediated securities** that are credited to a securities account by a custodian. Since a token does not require a custodian, cof tokens as intermediated securities will therefore generally not be conceivable.

# ASSET TOKENIZATION (ACCORDING TO AP CO)



# CONCLUSION

# READY FOR THE BLOCKCHAIN?

# WHO IS SATOSHI NAKAMOTO?

– Check this:

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

CENTRO
DI STUDI BANCARI
VILLA NEGRONI
ASSOCIAZIONE BANCARIA TICINESE

# Investimento Passivo in Bitcoin per GEI (Gestori Esterni Indipendenti)



Bitmax

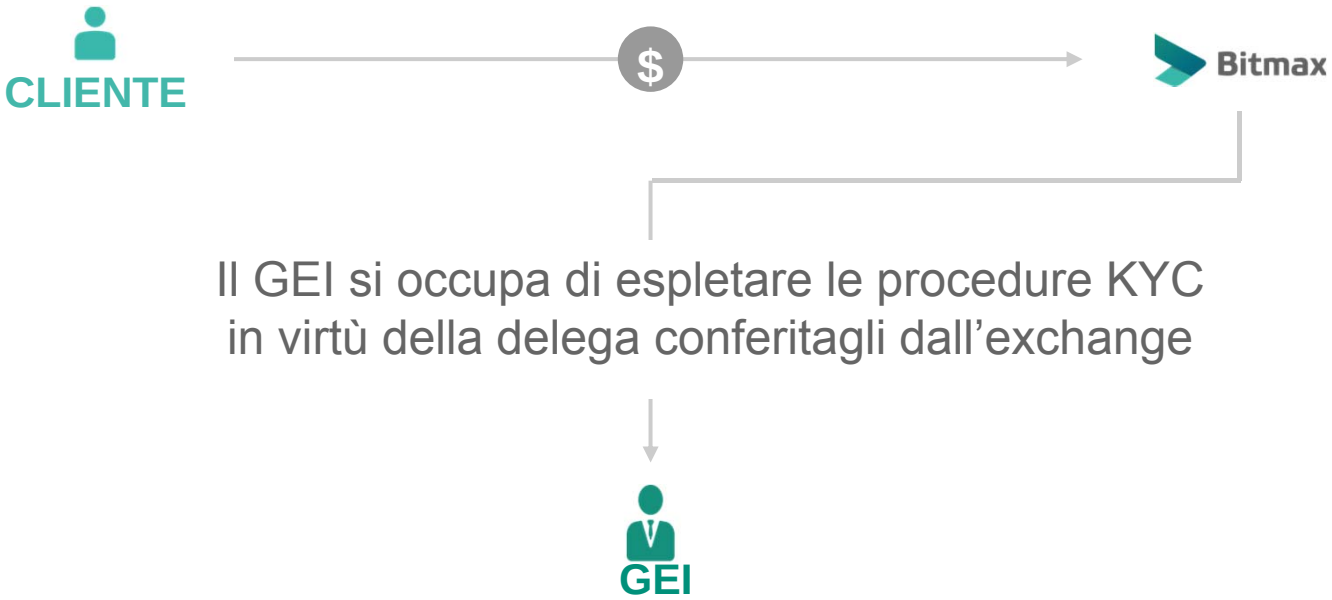
# IN - Acquisto

**GEI** — Viene siglato un mandato speciale con il → **CLIENTE**

*In quanto:*

- BTC è un asset particolare
- Per decidere quali commissioni applicare a favore del gestore (commissioni di courtage, success fee o costi di custodia)

# IN - Acquisto



# IN - Purchase

GEI

1

Condivide con l'exchange la KYC del cliente

Bitmax

2

Procede all'acquisto e consegna un paper wallet (PW) contenente i BTC

# Custodia

GEI

*Decide di*

- consegnare il PW al cliente
- custodire il PW nel proprio safe
- far custodire il PW presso il safe di Eidoo Sagl

# Paper Wallet


# Paper Wallet

Il fatto di possedere un **paper wallet** elimina il rischio di controparte.

Permette di negoziare le criptomonete 7/7 24/24.

**Invece:**
I certificati, i trackers, i fondi che investono in criptomonete vengono negoziati tramite i canali tradizionali e negli orari standard.
A differenza dal paper wallet questi prodotto sottostanno alle rigide condizioni e normative previste all'interno della MIFID e della LSerFi, con obbligo di verifica dell'adeguatezza, dell'appropriatezza, oltre che, per la MIFID, dell'analisi ex ante e ex post dei costi del prodotto.
I certificati sono altresì più semplici da inserire in una asset allocation ma non eliminano il rischio di controparte di chi gestisce questi veicoli

# Paper Wallet

Sistema di custodia **realmente** offline

Immune alla contraffazione

Nessun software

Nessun hardware

Nessuna password

Nessun recovery seed

# OUT - Vendita

GEI

Decide che è arrivato il momento di vendere i BTC e consegna il PW a

Bitmax

# OUT - Vendita

Bitmax — Il ricavato della vendita viene accreditato a favore del → **CONTO BANCARIO DEL CLIENTE**