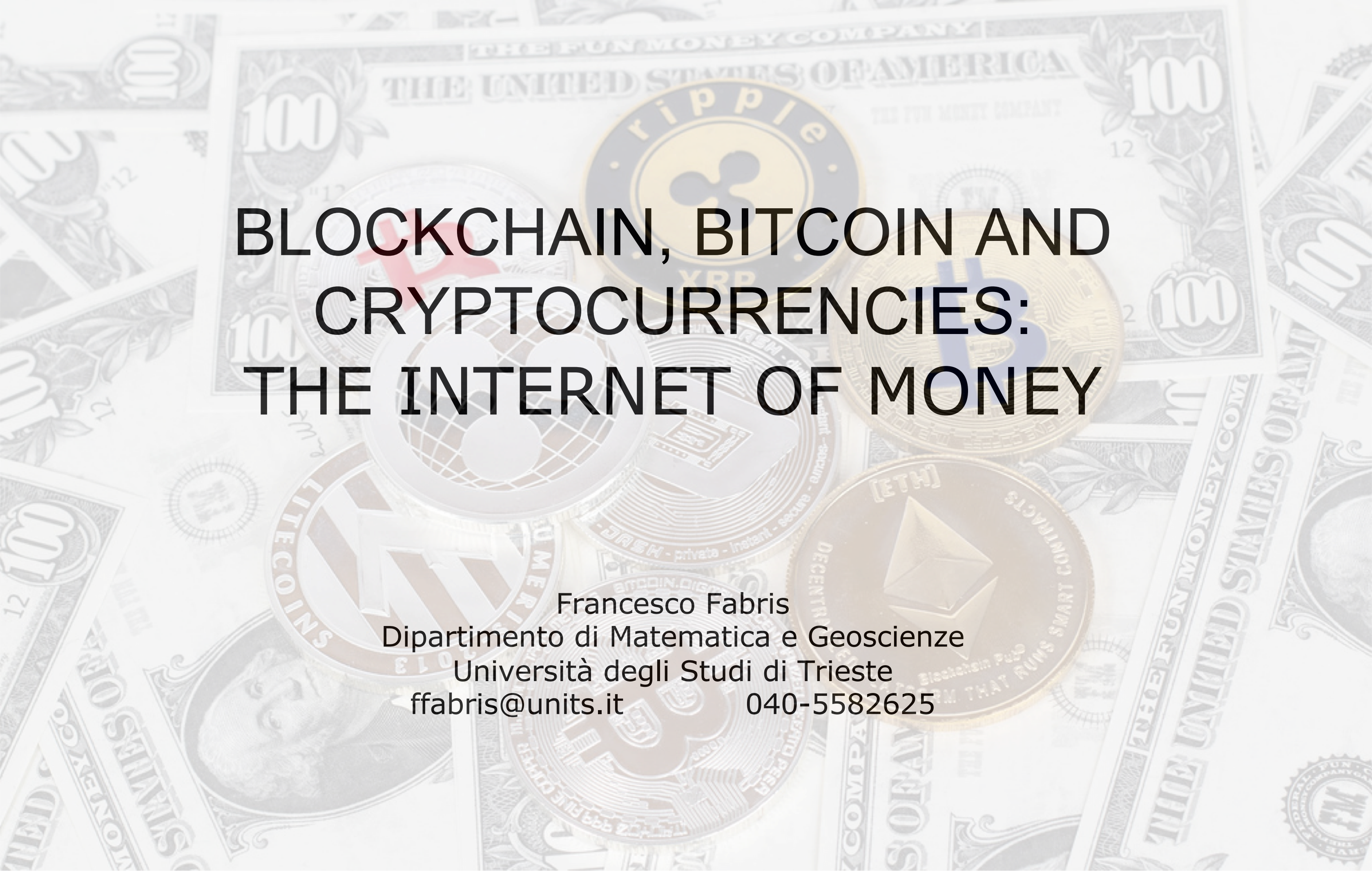


BLOCKCHAIN, BITCOIN AND CRYPTOCURRENCIES: THE INTERNET OF MONEY

Francesco Fabris
Dipartimento di Matematica e Geoscienze
Università degli Studi di Trieste
ffabris@units.it 040-5582625

flickr.com

Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain

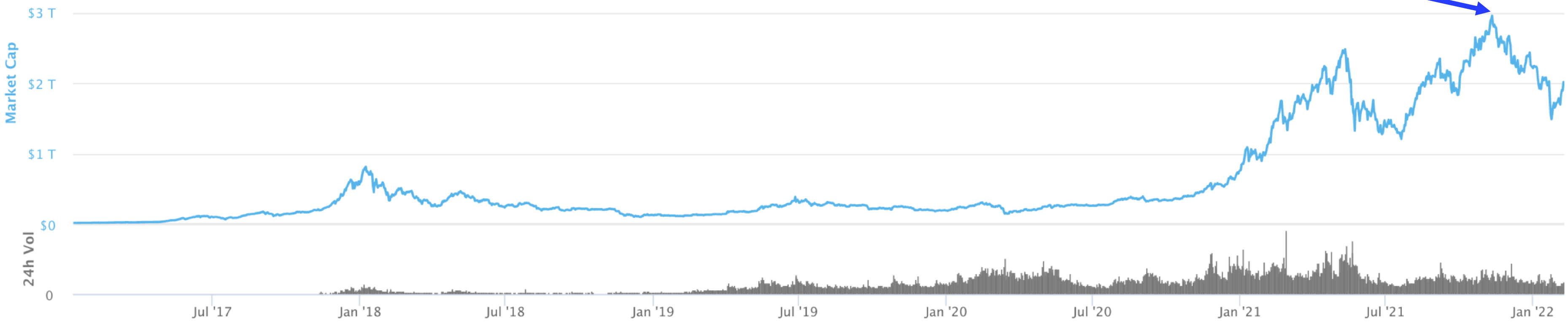
Ministero per lo Sviluppo Economico **(*luglio 2020*)**

2.18 Focalizzazione su formazione e ricerca universitaria

Viste le caratteristiche del tema e l'importanza di supportarne lo sviluppo, **si raccomanda una forte focalizzazione nella creazione di linee di ricerca sui temi delle DLT e di *Blockchain*, anche attraverso l'inserimento esplicito delle tematiche negli strumenti di ricerca nazionali (e.g. PRIN, progetti regionali, ecc...),** lo sviluppo di linee di dottorato industriale ad-hoc, la possibilità di avere una via prioritaria di finanziamento per progetti che siano di natura "*follow-up*" rispetto a progetti di ricerca che hanno già ottenuto finanziamenti in bandi competitivi internazionali (e.g., EU H2020), in modo da sfruttare la possibilità di trasferimento tecnologico di progetti già sviluppati e l'expertise e l'eccellenza di team di ricerca che hanno già lavorato su questi argomenti. A livello universitario, attualmente le attività formative relative al campo dei sistemi distribuiti ed in particolare dei DLT, sono relative principalmente all'attivazione di singoli corsi che coprono alcune competenze base della tecnologia dei DLT, quali crittografia, *networking*, sistemi distribuiti, teoria dei giochi. Si raccomanda il supporto ad iniziative relative alla attivazione di interi percorsi organici che possano amalgamare in modo coerente le varie competenze e contribuire alla formazione di figure professionali specifiche nel campo di queste tecnologie".

Economic dimension of the phenomenon: market capitalization

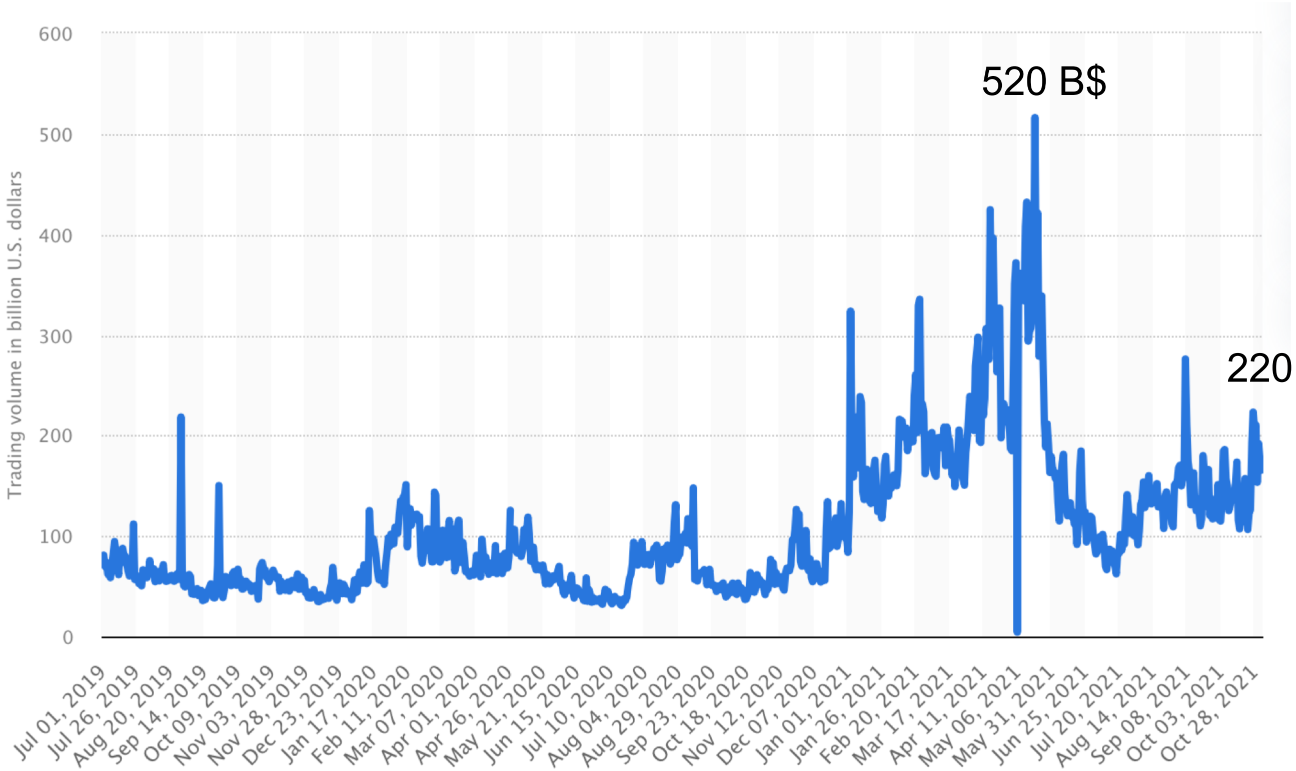
max 3 T$



1 T$ = 1000 mld $

source
https://coinmarketcap.com

Economic dimension of the phenomenon: daily trading volumes

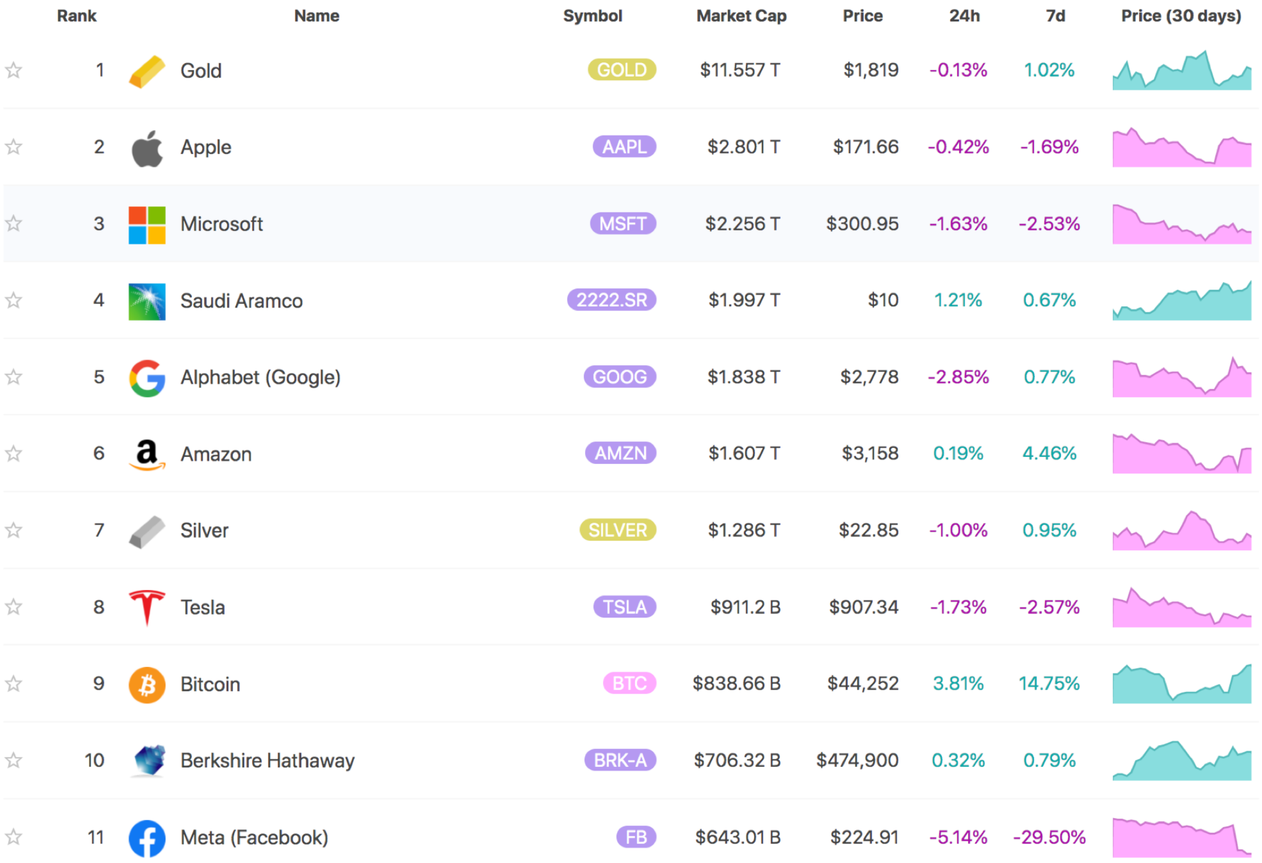


520 B$

220 B$

source:
www.statista.com

Economic dimension of the phenomenon



	Rank	Name	Symbol	Market Cap	Price	24h	7d	Price (30 days)
☆	1	Gold	GOLD	$11.557 T	$1,819	-0.13%	1.02%	
☆	2	Apple	AAPL	$2.801 T	$171.66	-0.42%	-1.69%	
☆	3	Microsoft	MSFT	$2.256 T	$300.95	-1.63%	-2.53%	
☆	4	Saudi Aramco	2222.SR	$1.997 T	$10	1.21%	0.67%	
☆	5	Alphabet (Google)	GOOG	$1.838 T	$2,778	-2.85%	0.77%	
☆	6	Amazon	AMZN	$1.607 T	$3,158	0.19%	4.46%	
☆	7	Silver	SILVER	$1.286 T	$22.85	-1.00%	0.95%	
☆	8	Tesla	TSLA	$911.2 B	$907.34	-1.73%	-2.57%	
☆	9	Bitcoin	BTC	$838.66 B	$44,252	3.81%	14.75%	
☆	10	Berkshire Hathaway	BRK-A	$706.32 B	$474,900	0.32%	0.79%	
☆	11	Meta (Facebook)	FB	$643.01 B	$224.91	-5.14%	-29.50%	

Crypto

BTC

source:
https://8marketcap.com/
date 8 feb 22

Political dimension of the phenomenon

Facebook

Wikimedia Commons

Wikimedia Commons

On **June 18th 2019**
Facebook published the whitepaper of the new own digital currency, whose name is Libra

On **July 2 2019**, The ***United States House of Representatives*** *Committee on Financial Services* wrote a very firm letter of intimation to the CEO of Facebook....

We write to request that Facebook and its partners immediately agree to a moratorium on any movement forward on Libra -its proposed cryptocurrency- and Calibra -its proposed digital wallet. It appears that these products may lend themselves to an entirely new global financial system that is based out of Switzerland and intended to rival U.S. monetary policy and the dollar. This raises serious privacy, trading, national security, and monetary policy concerns for not only Facebook's over 2 billion users, but also for investors, consumers, and the broader global economy.

......

As a results, several brands who initially supported the project,

such as

VISA, stripe, PayPal, ebay, Mastercard

withdrew

It is not a true blockchain

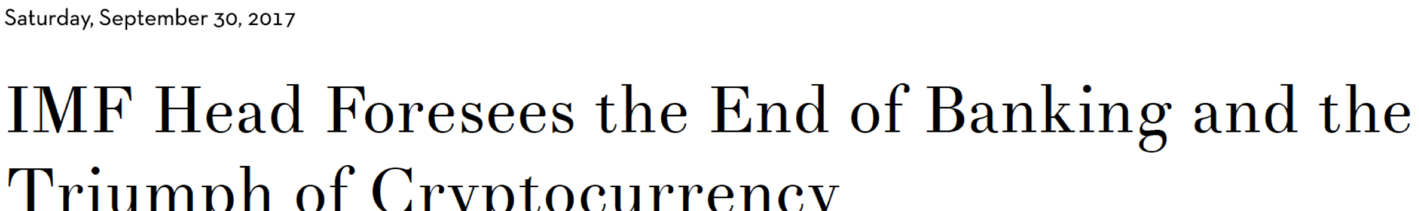
It is not decentralized

Access to (approximately) 100 nodes (currently only 28) per depositing company
$ 10 million and $ 300k per year in commissions in order to guarantee an adequate amount of the underlying fiduciary currencies.

Basket composition of underlying fiduciary currencies:

USD	50%
EURO	18%
YEN	14%
GBP	11%
SGD	7%

Political dimension of the phenomenon



Saturday, September 30, 2017

IMF Head Foresees the End of Banking and the Triumph of Cryptocurrency

Bitcoin "puts a question mark on the fractional banking model we know today."

How will central banking change with the next generation?

Impact of cryptocurrencies on the monetary and financial system: need to implement new models of financial intermediation

All of this raises a question mark about the fractional banking model as we know today

Christine Lagarde

Wikimedia Commons

ex IMF President
curret ECB President

Deutsche Bank Strategist Says End of Fiat-based Currency Systems Near, Recommends Bitcoin

Prophesy

"The beginning of the end of legal tender currencies"

“Cryptocurrencies have for now a mere character speculative, but at some point they could become a real competitor of paper money. "

Jim Reid

Deutsche Bank
Senior financial analyst

Political dimension of the phenomenon

> “You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990s. ”

Blythe Masters, CEO of Digital Asset Holdings and former CFO of J.P. Morgan's Investment Bank

Wikimedia Commons

L’evoluzione del Web

Web 1.0 ➔ global library
(text files, poor websites and intended as data repository)

Web 2.0 ➔ use of images, videos and social media (complex files and interactivity)

Web 3.0 ➔ semantic web, decentralized web,
transmission of value without intermediaries,
?? decentralized services and the end of the GAFAM monopoly, decentralized finance, global digital bank, metaverse …

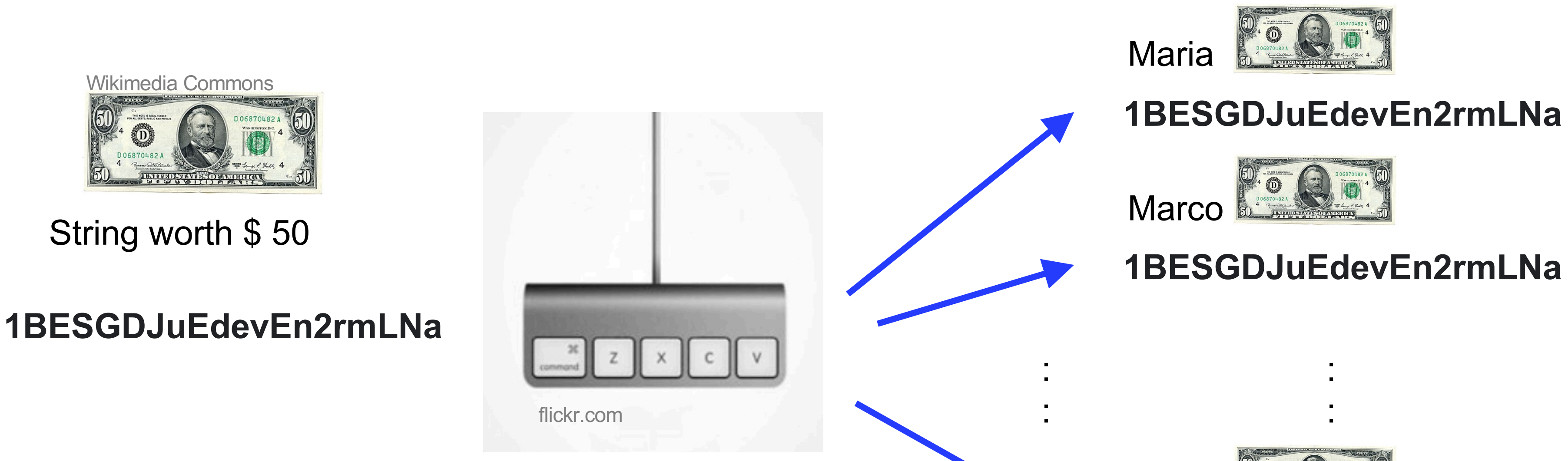
Central problem in digital transfer of value: the double spending problem

Traditionally the problem is solved in two ways:

1. transaction of a physical entity (cash, i.e. coins or banknotes)

2. intermediary (bank) that guarantees the impossibility of a double spending transaction

Double spending problem in the digital environment



Wikimedia Commons

String worth $ 50

1BESGDJuEdevEn2rmLNa

flickr.com

Maria

1BESGDJuEdevEn2rmLNa

Marco

1BESGDJuEdevEn2rmLNa

⋮ ⋮

Lucia

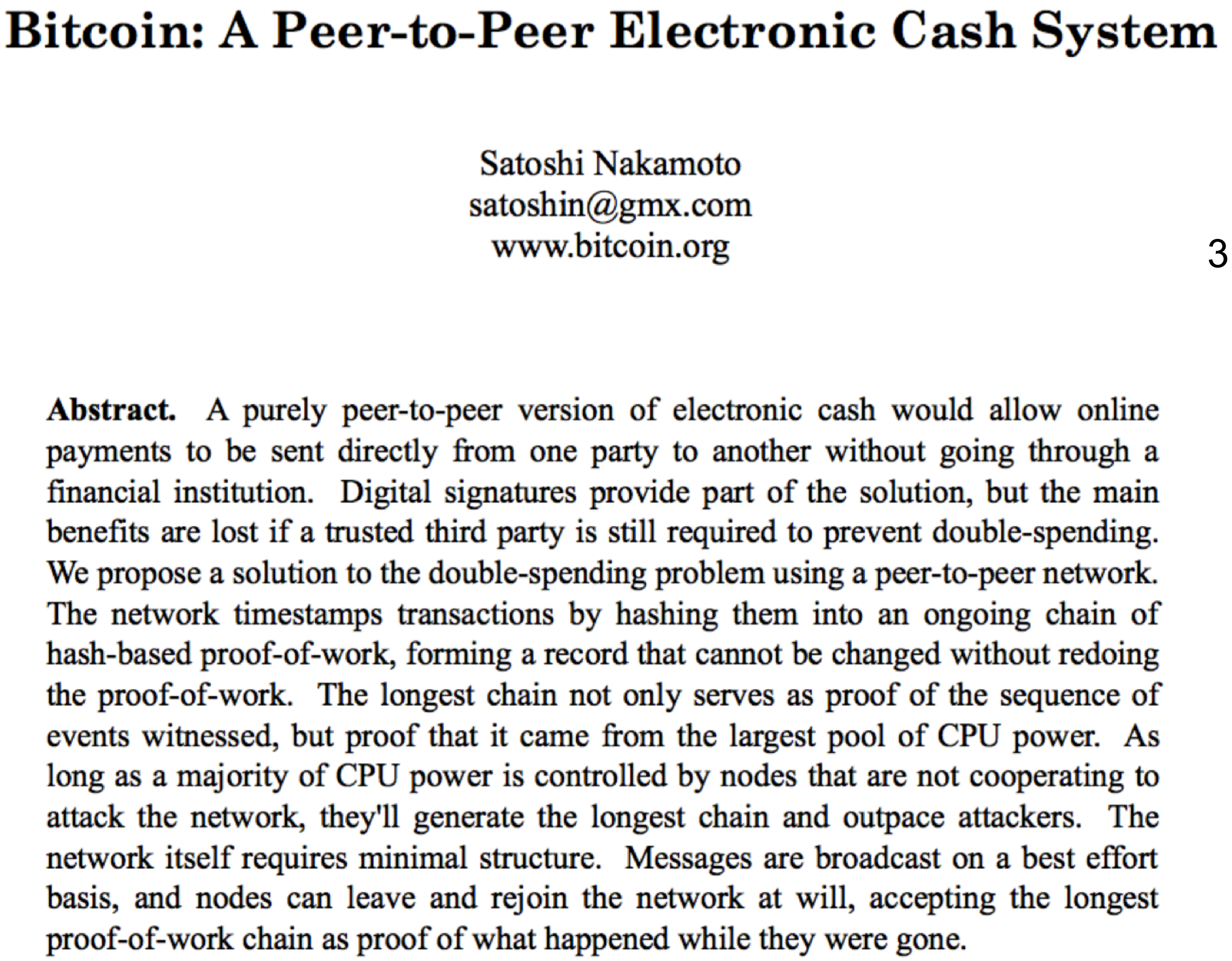
1BESGDJuEdevEn2rmLNa

... provably unsolvable problem!

Bitcoin: it all starts with a handful of "nerds"...

- In August 2008, the «Bitcoin.org» domain was registered
- On October 31 of the same year, on a mailing list of cryptographers, a link appears to an article by a certain Satoshi Nakamoto, entitled “*Bitcoin: A Peer-to-Peer Electronic Cash System*”.
- Nakamoto makes the open source software for bitcoin and releases it in January 2009 on *SourceForge*. *Bitcoin* (BTC) is born!
- The activation of the network took place in January 2009
- The identity of Satoshi Nakamoto remains shrouded in mystery

The birth of bitcoin



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

31 ottobre 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

31 October 2008

Initial release	0.1.0	9 gennaio 2009
Last release	22.0	13 settembre 2021

“I just want to report that I successfully traded 10.000 bitcoins for pizza” wrote user *laszlo* on *Bitcoin forum* on May 2010 (about 41$ at that time)

... now those pizzas would cost 450 mln $!!

Bitcoin - Basic concepts:

1. Internet as a tool for transmitting value
2. Value transmission without a bank as an intermediary (*Peer-to-peer transactions*)
3. Decentralized
4. Value transmitted (ideally) instantaneously
5. Based on a *public distributed ledger* called *blockchain*
6. Anonymous
7. Irreversible
8. Out of the control of central banks, state authorities and political power (censorship resistant)
9. One can activate how many addresses (s)he desire
10. Free of inflation (21 million Bitcoins will be produced in all)

Bitcoin and cryptocurrencies:
an artificial ecosystem
of hybrid type, which involves
different levels:

technological

economic

financial

social

politic

ecological

legal

I LEVEL OF ANALYSIS:
THE STRUCTURE OF THE BITCOIN

II LEVEL OF ANALYSIS:
THE OVERALL ECOSYSTEM

I LEVEL OF ANALYSIS: THE STRUCTURE OF THE BITCOIN

What is Bitcoin and what are the essential characteristics?

flickr.com

Wikimedia Commons

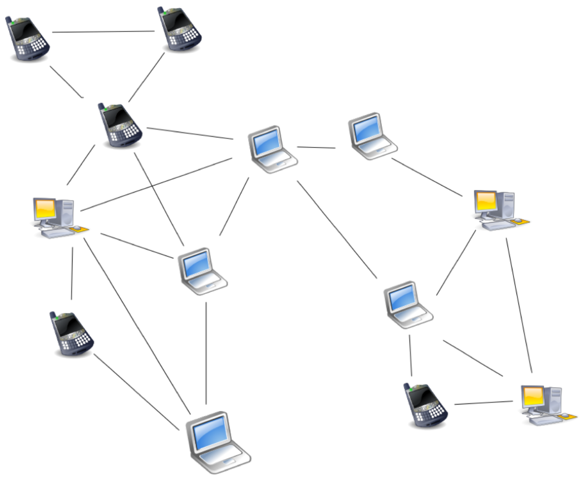
Bitcoin carries out transactions without an intermediary

Constituent elements:

1. ***Distributed ledger***
2. ***Blockchain***
3. ***Miners*** and their activity of *mining*

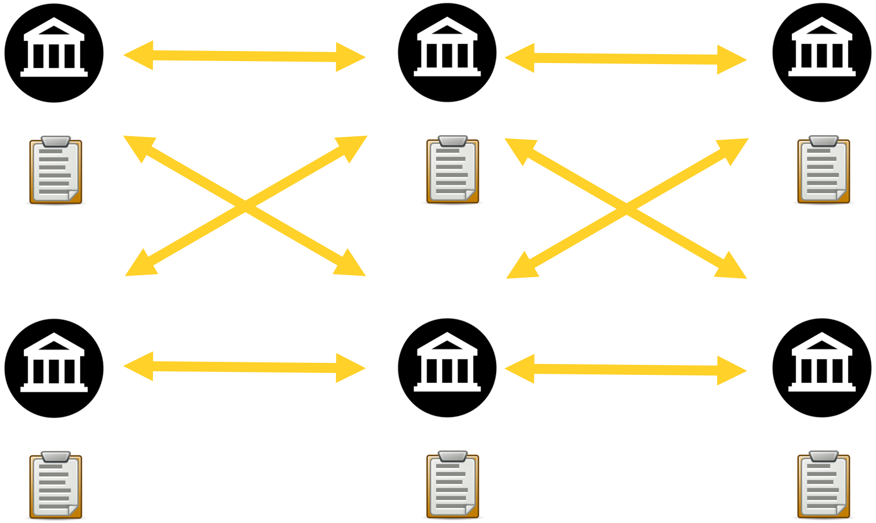
1 – *Distributed ledger*

It is a network of servers ...



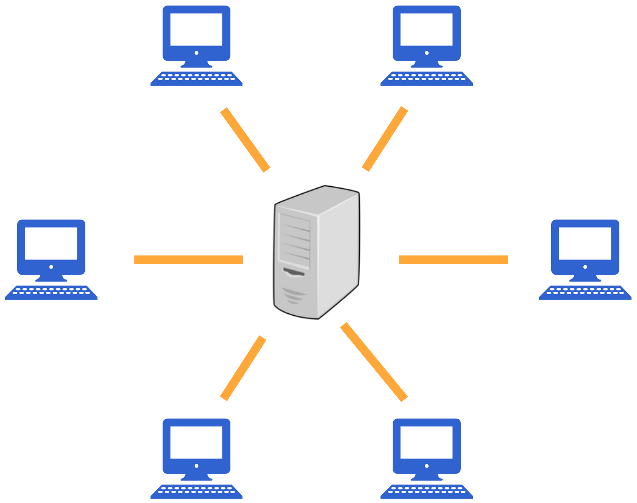
Wikipedia.org

... each server contains a ledger on which all transactions are noted

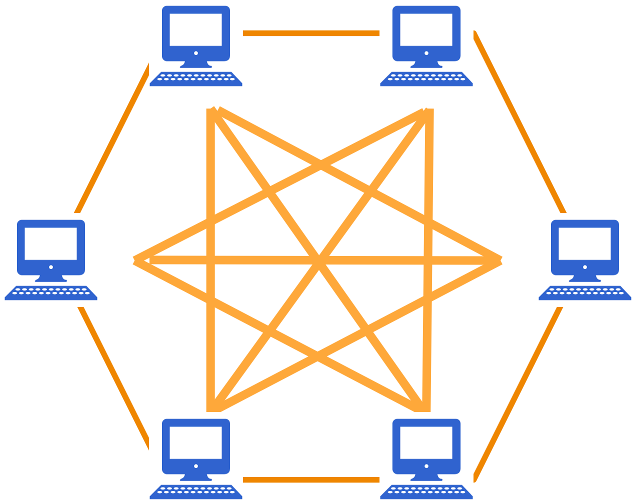


Wikimedia Commons

Transaction without intermediaries: *peer-to-peer* (P2P) network



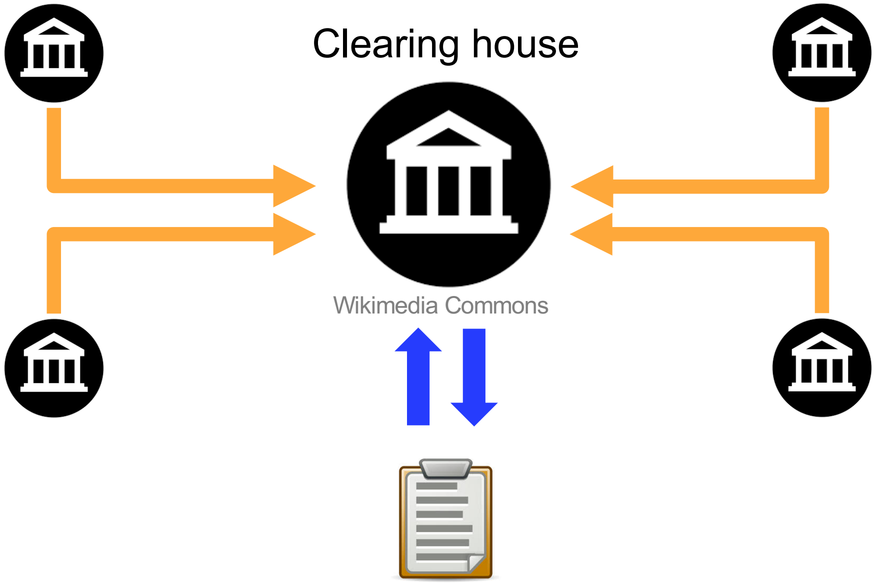
Server-based



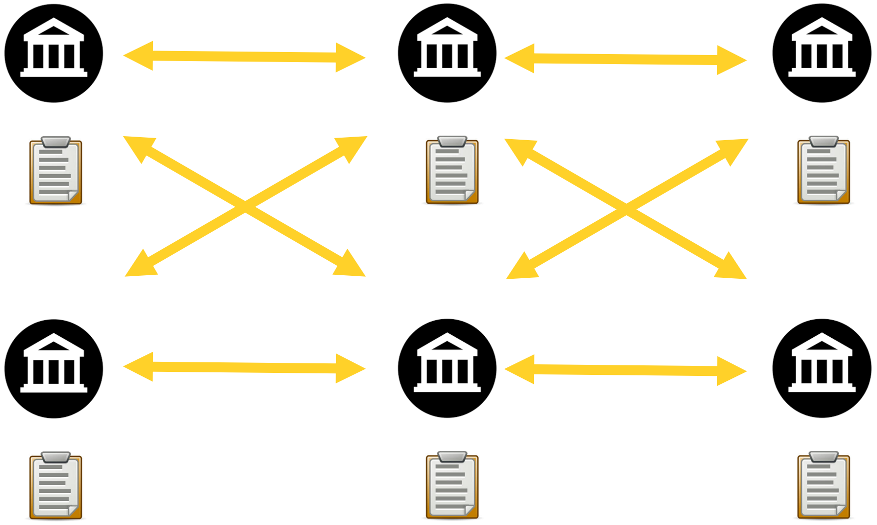
P2P network

Wikimedia Commons

Transaction without intermediaries: the distributed data-base

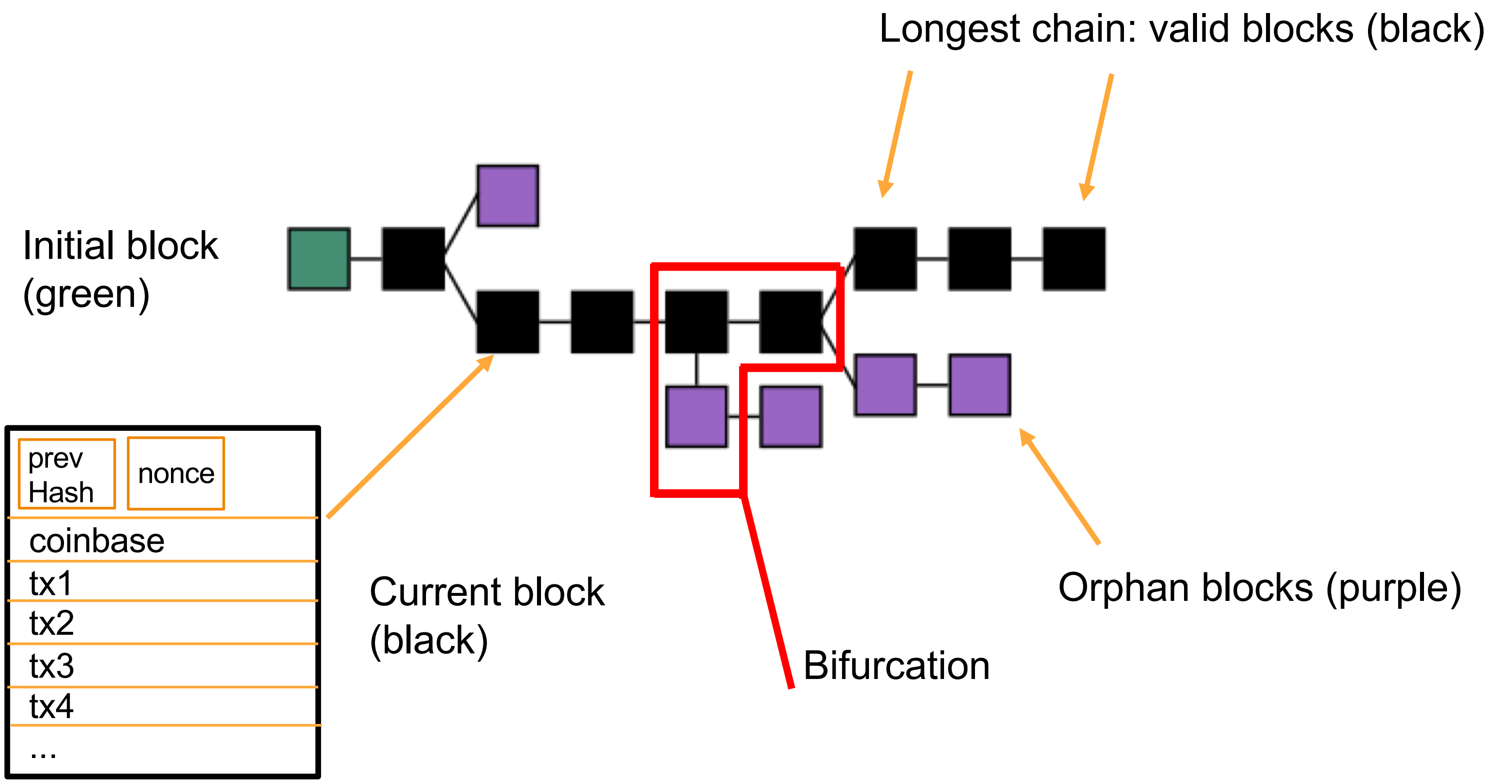


Centralized ledger



Distributed ledger

2. Blockchain (chain of blocks of ∼1 Mb)



Longest chain: valid blocks (black)

Initial block (green)

prev Hash

nonce

coinbase

tx1

tx2

tx3

tx4

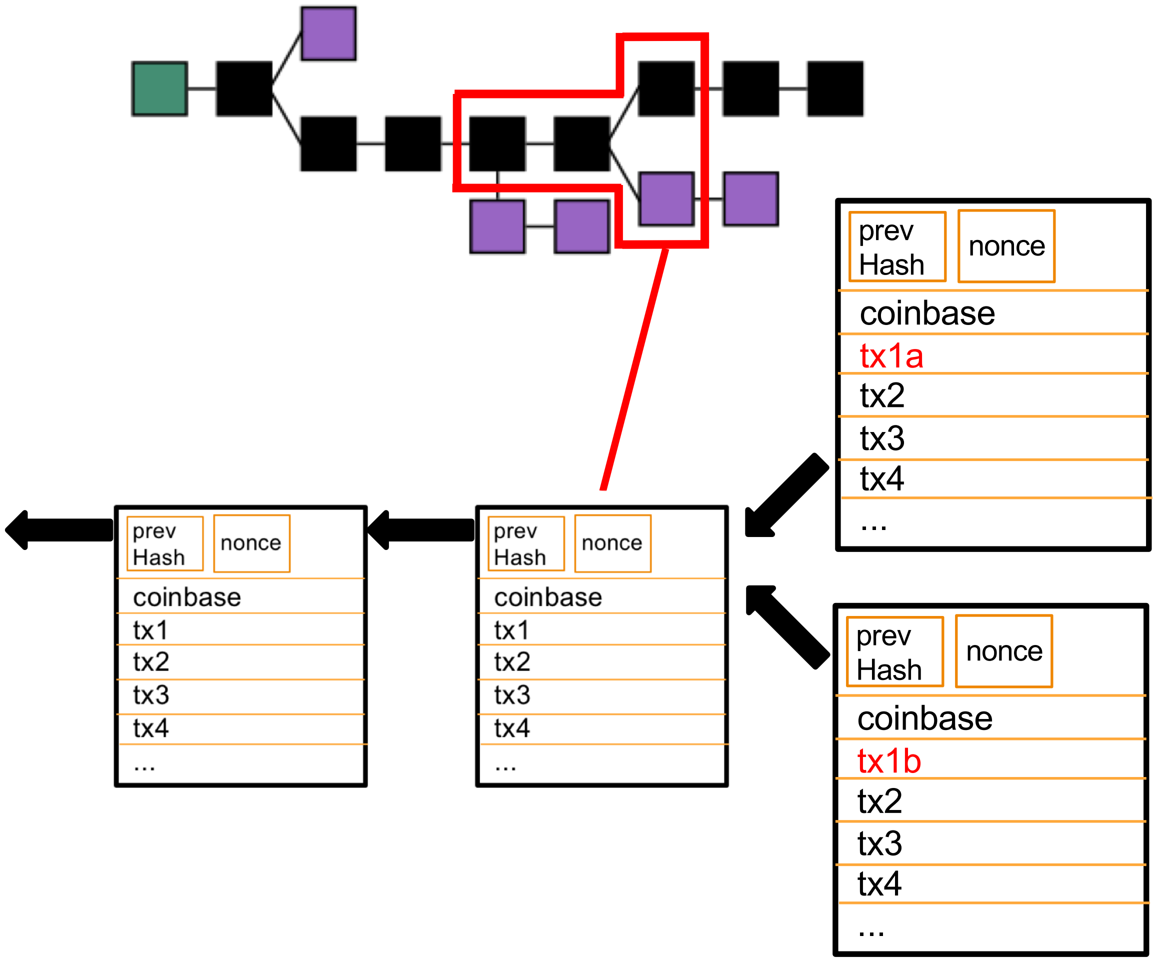
…

Current block (black)

Bifurcation

Orphan blocks (purple)

Bitcoin structure



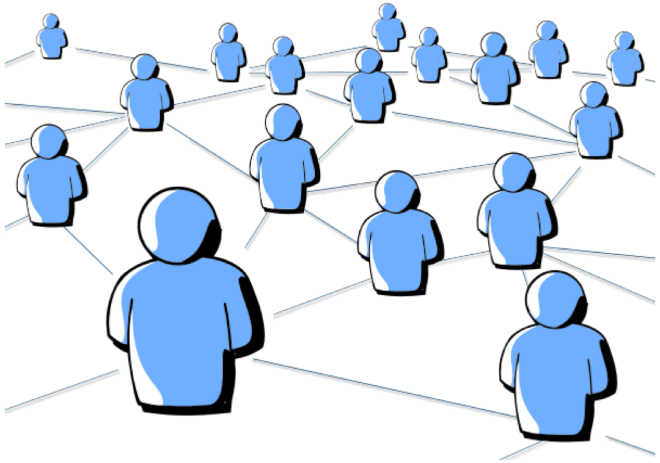
prev Hash | nonce
coinbase
tx1
tx2
tx3
tx4
…

prev Hash | nonce
coinbase
tx1
tx2
tx3
tx4
…

prev Hash | nonce
coinbase
tx1a
tx2
tx3
tx4
…

prev Hash | nonce
coinbase
tx1b
tx2
tx3
tx4
…

3 – *Miners* - or the network nodes



creatingcommons.org

They form the nodes of the network and keep it running
> 14800 nodes currently for BTC (Bitcoin)

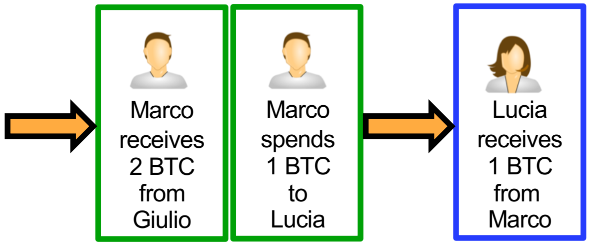
Proof of Work - PoW

The problem of *double spending* (of a digital string) without intermediary: linked to the problem of *consensus* among the nodes of an unreliable network.

Linked to the problem of the *Byzantine generals* (*Byzantin Fault Tolerant*)
It is a provably unsolvable problem

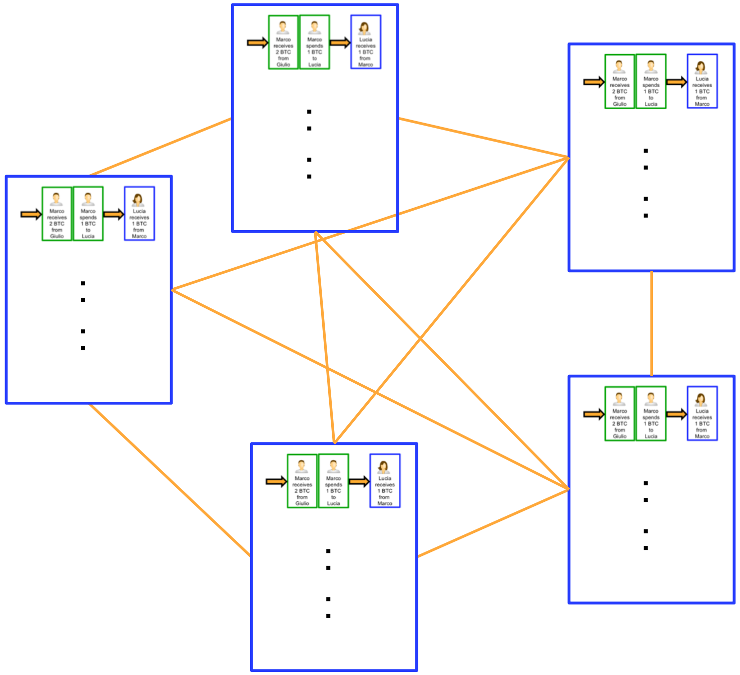
Bitcoin solves (in practice) the problem with a probabilistic method, based on the so-called Proof-of-Work, without contradicting the unsolvability of the theorem

Bitcoin structure


Marco receives 2 BTC from Giulio
Marco spends 1 BTC to Lucia
Lucia receives 1 BTC from Marco

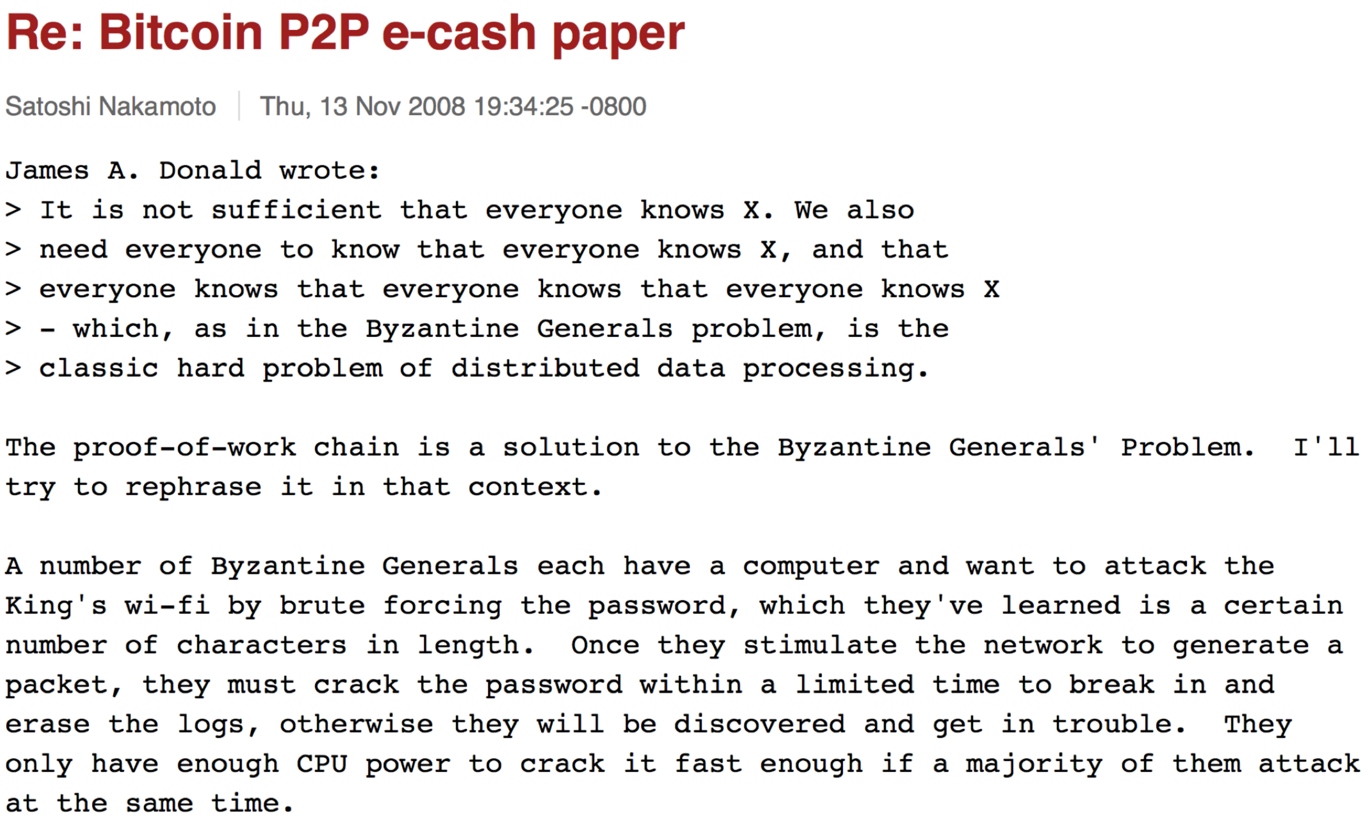
Consensus among network nodes

When a new transaction is entered into the network...



... each node can accept it,
putting it on the block, or ignoring it

If the majority of nodes agree on
a certain state you get the *consensus*



Re: Bitcoin P2P e-cash paper

Satoshi Nakamoto | Thu, 13 Nov 2008 19:34:25 -0800

James A. Donald wrote:

> It is not sufficient that everyone knows X. We also need everyone to know that everyone knows X, and that everyone knows that everyone knows that everyone knows X - which, as in the Byzantine Generals problem, is the classic hard problem of distributed data processing.

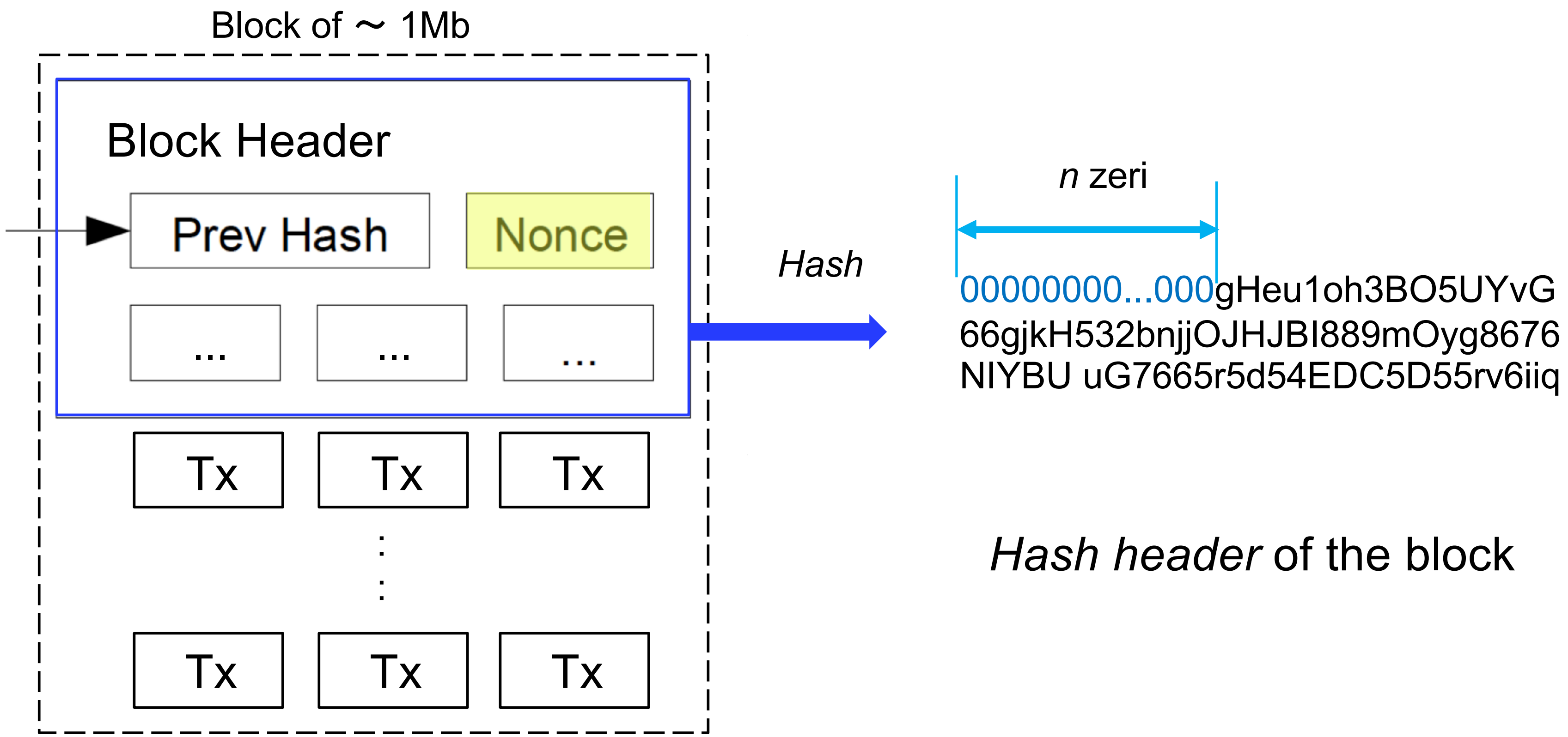
The proof-of-work chain is a solution to the Byzantine Generals' Problem. I'll try to rephrase it in that context.

A number of Byzantine Generals each have a computer and want to attack the King's wi-fi by brute forcing the password, which they've learned is a certain number of characters in length. Once they stimulate the network to generate a packet, they must crack the password within a limited time to break in and erase the logs, otherwise they will be discovered and get in trouble. They only have enough CPU power to crack it fast enough if a majority of them attack at the same time.

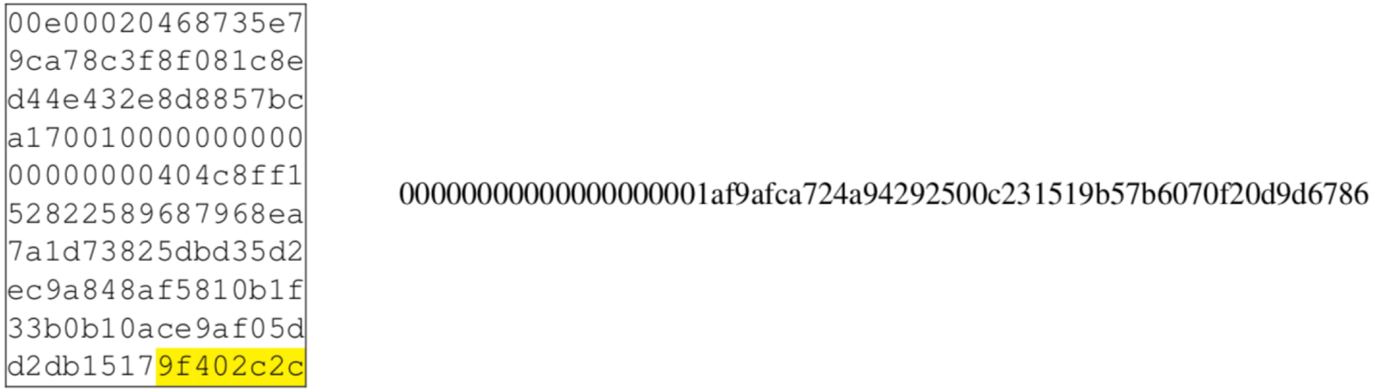
⋮

⋮

Proof of Work - PoW


Block of ∼ 1Mb
Block Header
Prev Hash
Nonce
...
...
...
Tx
Tx
Tx
Tx
Tx
Tx
Hash
n zeri
00000000...000gHeu1oh3BO5UYvG
66gjkH532bnjjOJHJBI889mOyg8676
NIYBU uG7665r5d54EDC5D55rv6iiq

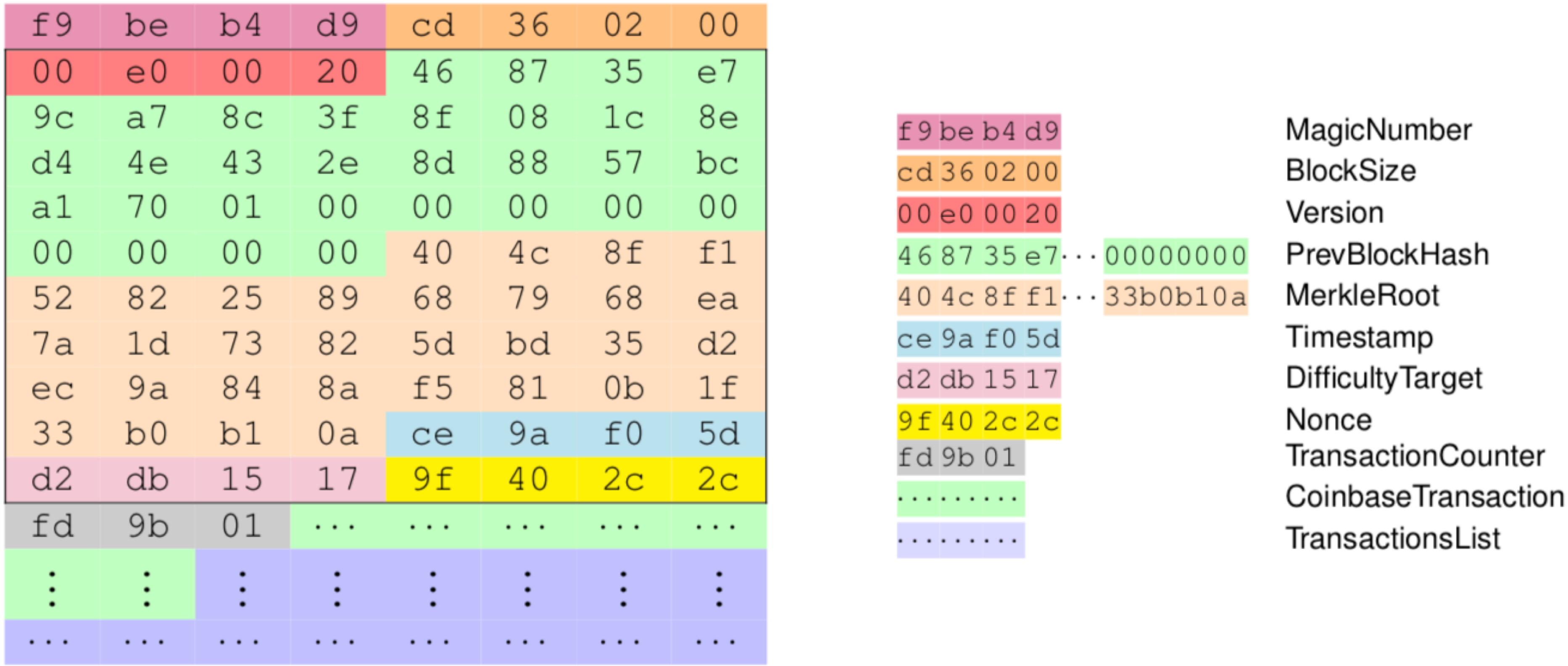
Hash header of the block



```
00e00020468735e7
9ca78c3f8f081c8e
d44e432e8d8857bc
a170010000000000
00000000404c8ff1
5282258968796 8ea
7a1d73825dbd35d2
ec9a848af5810b1f
33b0b10ace9af05d
d2db15179f402c2c
```

```
0000000000000000001af9afca724a94292500c231519b57b6070f20d9d6786
```

Header of the block 607617 and the Hash value obtained by applying SHA256(SHA256(*Header*)) starting from the *Nonce* `9f402c2c`



f9	be	b4	d9	cd	36	02	00
00	e0	00	20	46	87	35	e7
9c	a7	8c	3f	8f	08	1c	8e
d4	4e	43	2e	8d	88	57	bc
a1	70	01	00	00	00	00	00
00	00	00	00	40	4c	8f	f1
52	82	25	89	68	79	68	ea
7a	1d	73	82	5d	bd	35	d2
ec	9a	84	8a	f5	81	0b	1f
33	b0	b1	0a	ce	9a	f0	5d
d2	db	15	17	9f	40	2c	2c
fd	9b	01	...	...	...	...	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
...	...	...	...	...	...	...	...

f9 be b4 d9	MagicNumber
cd 36 02 00	BlockSize
00 e0 00 20	Version
46 87 35 e7 ··· 00000000	PrevBlockHash
40 4c 8f f1 ··· 33b0b10a	MerkleRoot
ce 9a f0 5d	Timestamp
d2 db 15 17	DifficultyTarget
9f 40 2c 2c	Nonce
fd 9b 01	TransactionCounter
········	CoinbaseTransaction
········	TransactionsList

Hexadecimal structure of the Header the block 607617

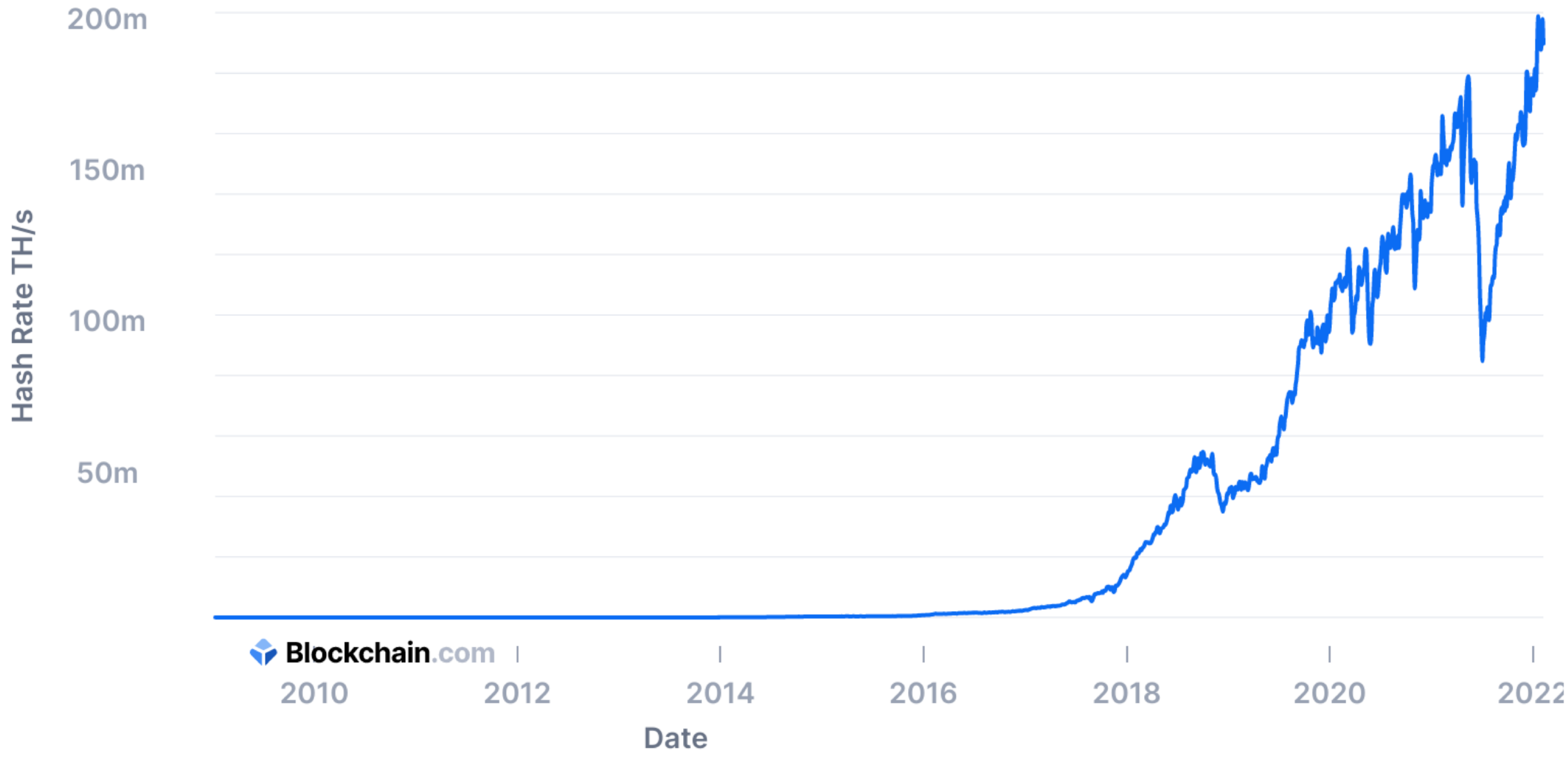
Proof of Work - PoW

PoW ➔ competition among miners

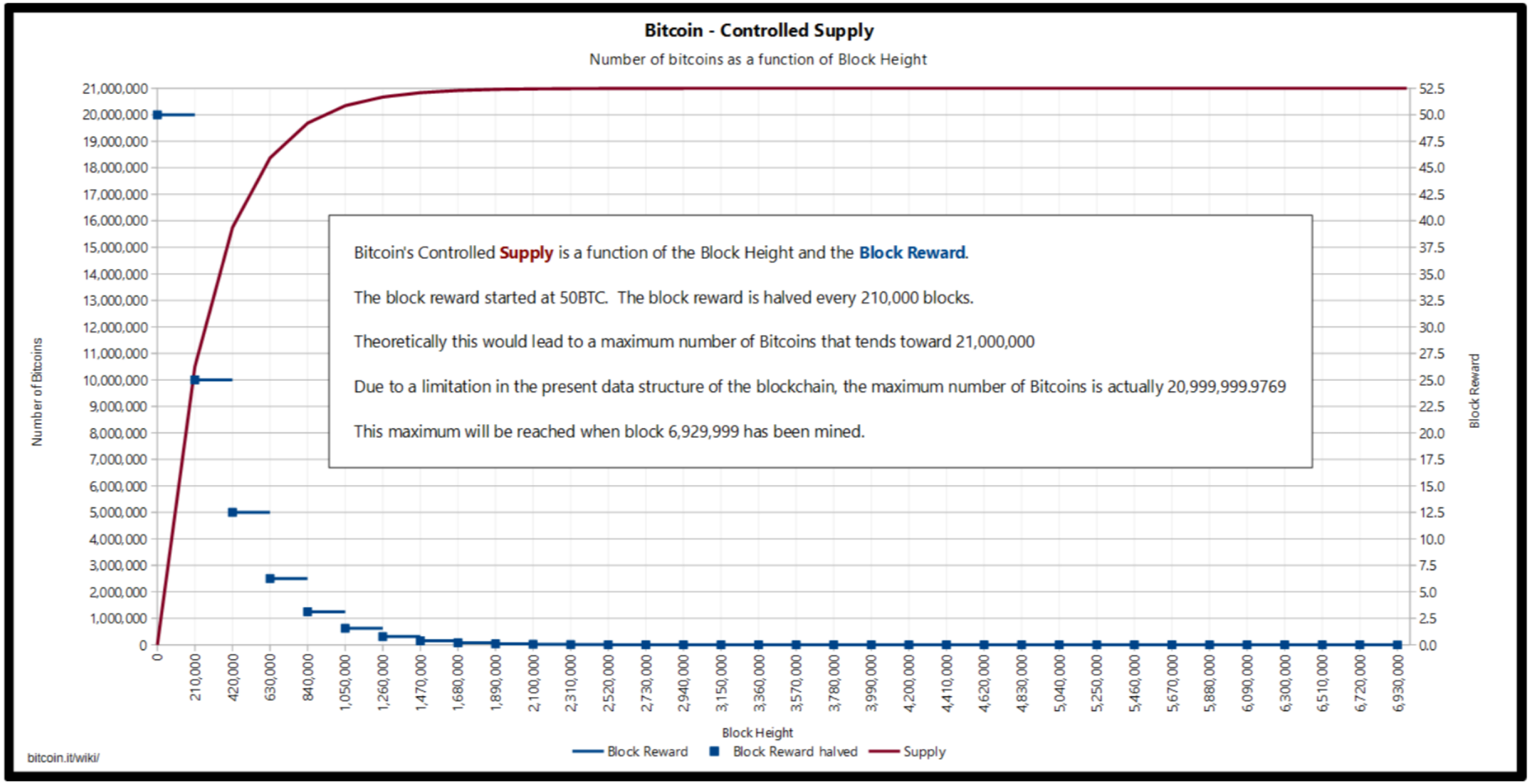
- reward in BTC halved every 210,000 blocks (about 4 years) starting at 50 BTC
- latest *Halving*: May 11, 2020 (6.25 BTC)
- current reward: 6.25 BTC (about 375k $)
- average block generation time: 10 min
- difficulty update: every 2016 blocks (about 14 days)

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



Bitcoin structure



Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

Wikimedia Commons

mining with a PC

mining with a GPU

mining with an array of GPU

Wikimedia Commons

mining
factory

Wikimedia Commons

mining factory

Proof of Stake - PoS

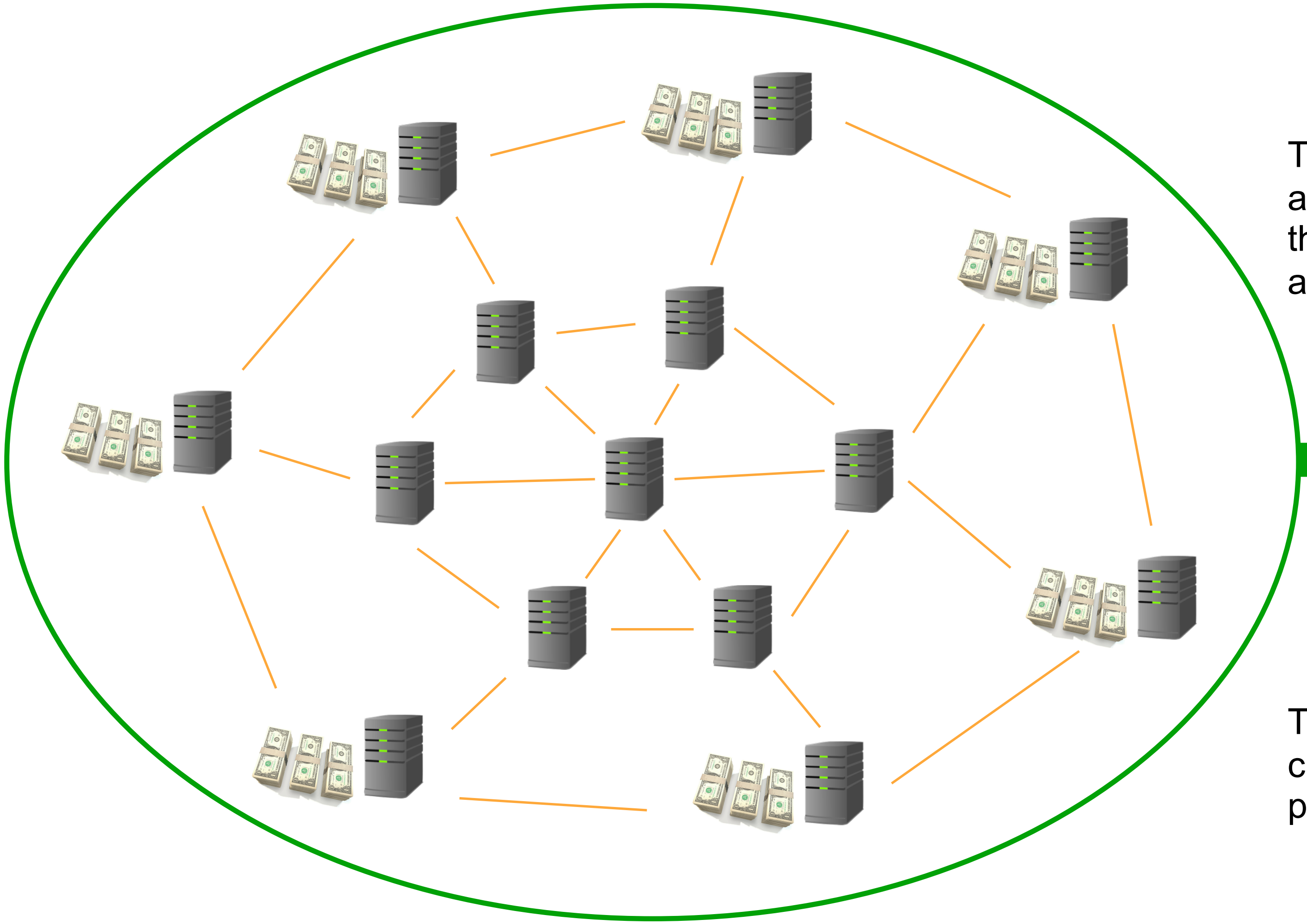
Another approach to transaction validation:

pixabay.com

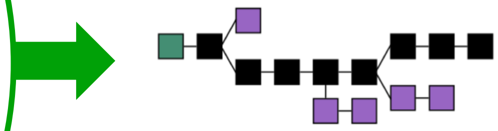
creativecommons.org

- each node must own a certain amount (stake) of the underlying cryptocurrency
- the node receives transaction fees in the underlying cryptocurrency
- the nodes with the expected stake become validator nodes and can certify the block

Proof of Stake



The validating nodes asseverate and crystalyze the blocks of transitions to add to the blockchain



Blockchain

The validating nodes are chosen with a probability proportional to the *Stake*

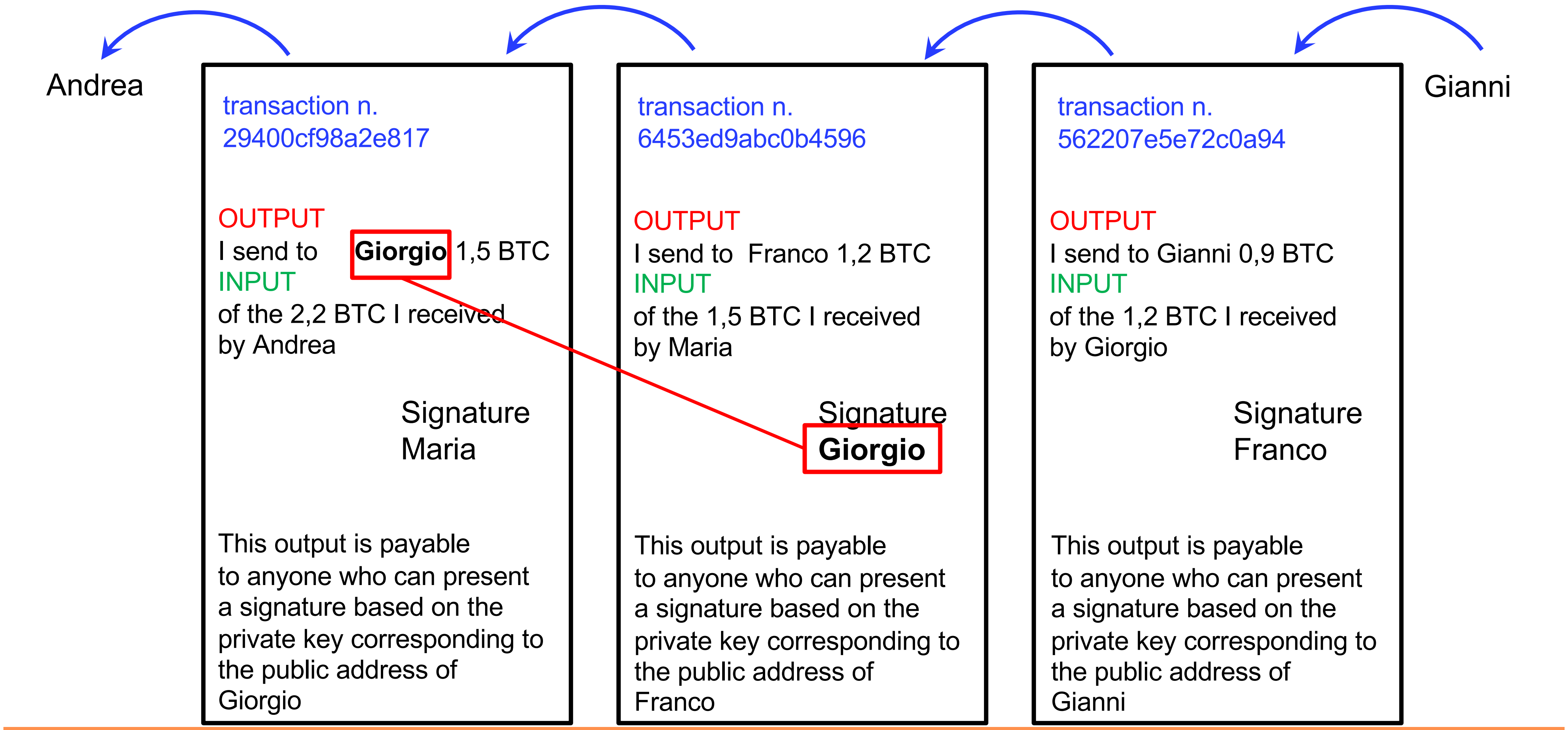
Concept underlying the *PoX*

- *Lottery*: as the number of tickets owned increases, the probability of winning increases
- *PoW*: as computing power increases, the probability of being able to win the race of finding the correct *Nonce* increases
- *PoS*: as the stake increases, the probability of being chosen to swear a block increases

Structure of a BTC transaction:

1. The user who wishes to send money creates a message with the transfer request
2. the node that accepts the request validates the transaction
3. transfers are made via BTC addresses (bitcoin address), which are the equivalent of a bank BIC/SWIFT
4. each BTC address is the hash of a cryptographic public key
5. each user can generate as many addresses as he wants
6. the sender's message is digitally signed to prove ownership of the money
7. the receiving node verifies the signature and forwards the message to all other nodes on the network
8. all Bitcoin transactions are public

Transaction structure



Andrea

transaction n.
29400cf98a2e817

OUTPUT
I send to **Giorgio** 1,5 BTC
INPUT
of the 2,2 BTC I received
by Andrea

Signature
Maria

This output is payable to anyone who can present a signature based on the private key corresponding to the public address of Giorgio

transaction n.
6453ed9abc0b4596

OUTPUT
I send to Franco 1,2 BTC
INPUT
of the 1,5 BTC I received
by Maria

Signature
Giorgio

This output is payable to anyone who can present a signature based on the private key corresponding to the public address of Franco

transaction n.
562207e5e72c0a94

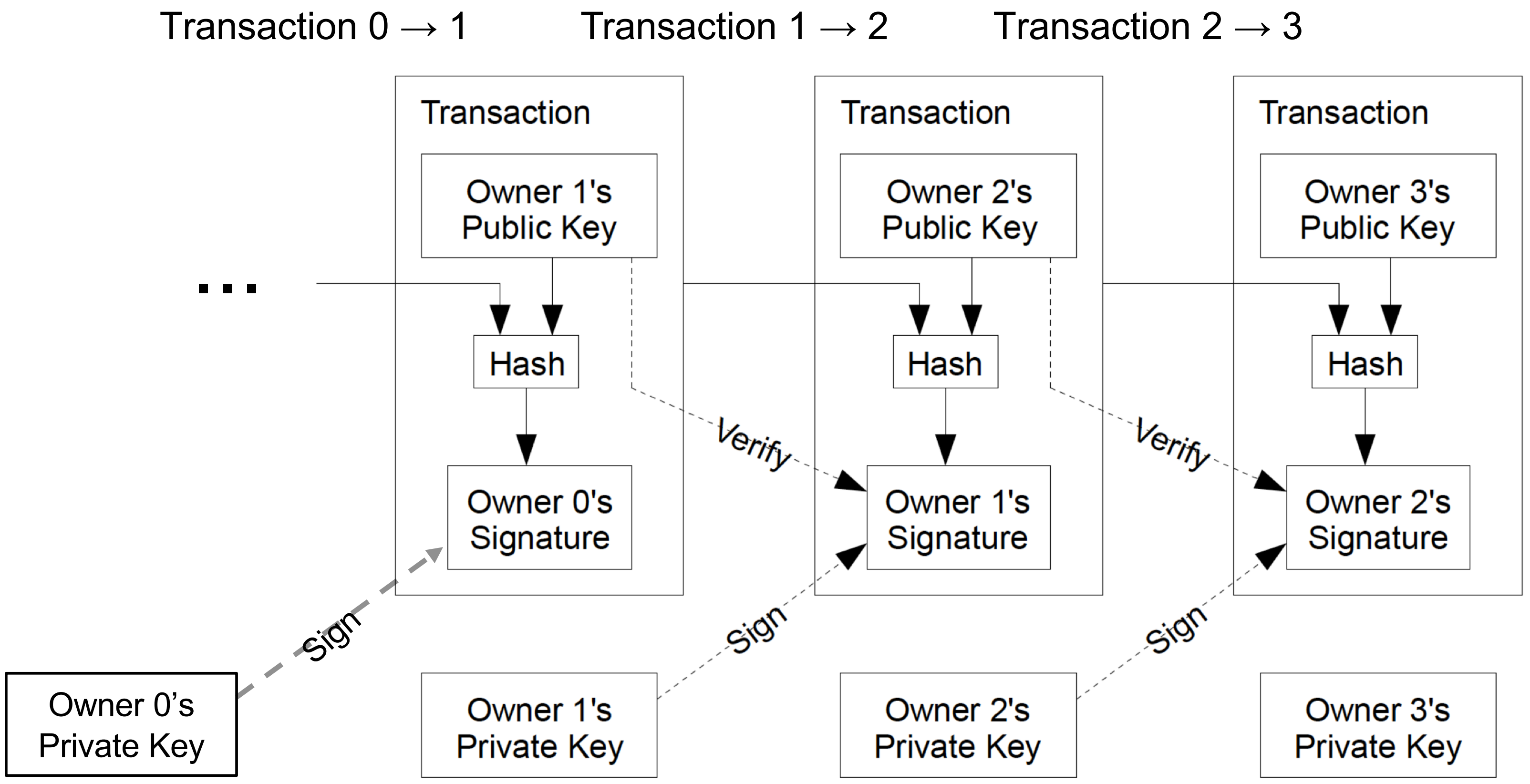
OUTPUT
I send to Gianni 0,9 BTC
INPUT
of the 1,2 BTC I received
by Giorgio

Signature
Franco

This output is payable to anyone who can present a signature based on the private key corresponding to the public address of Gianni

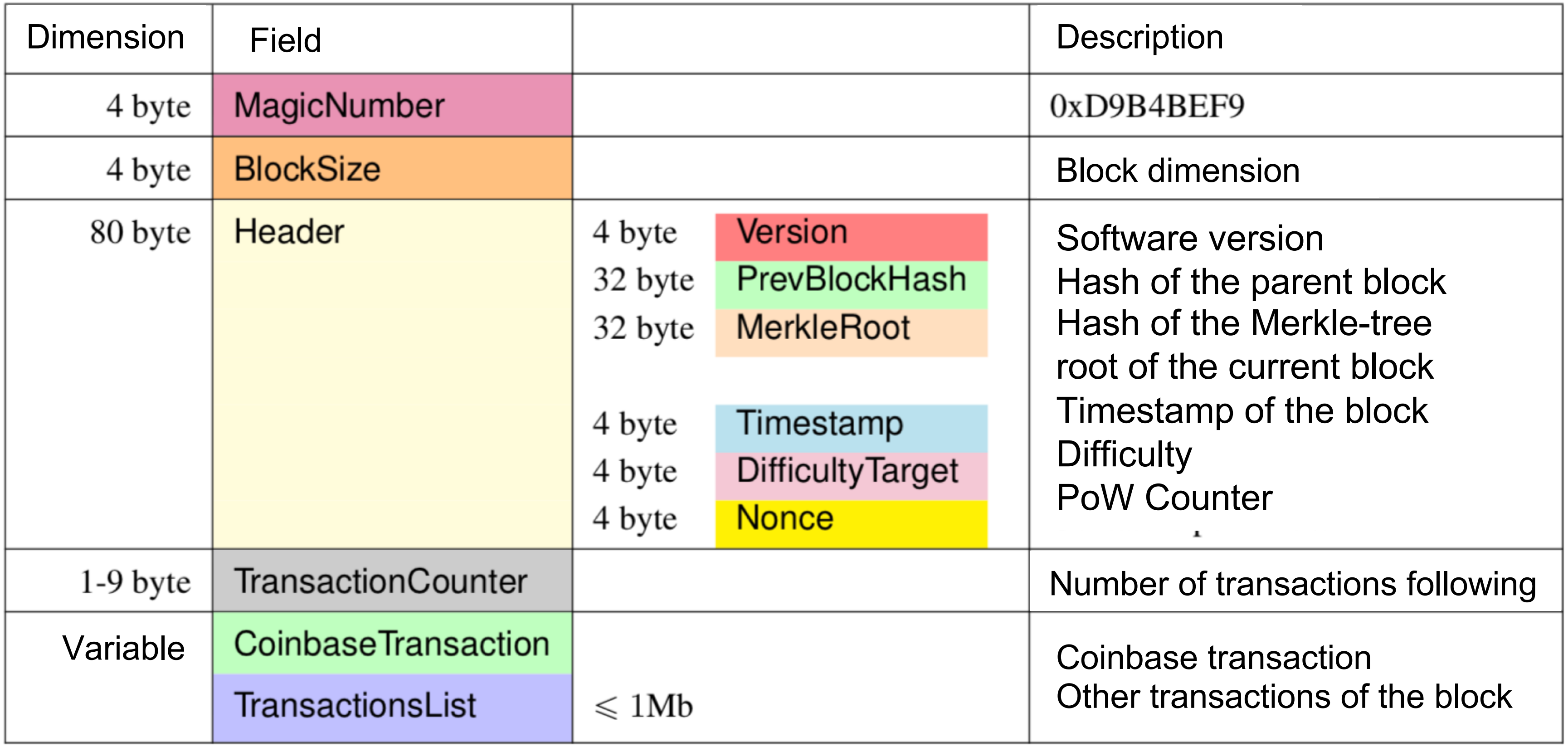
Gianni

Transaction structure



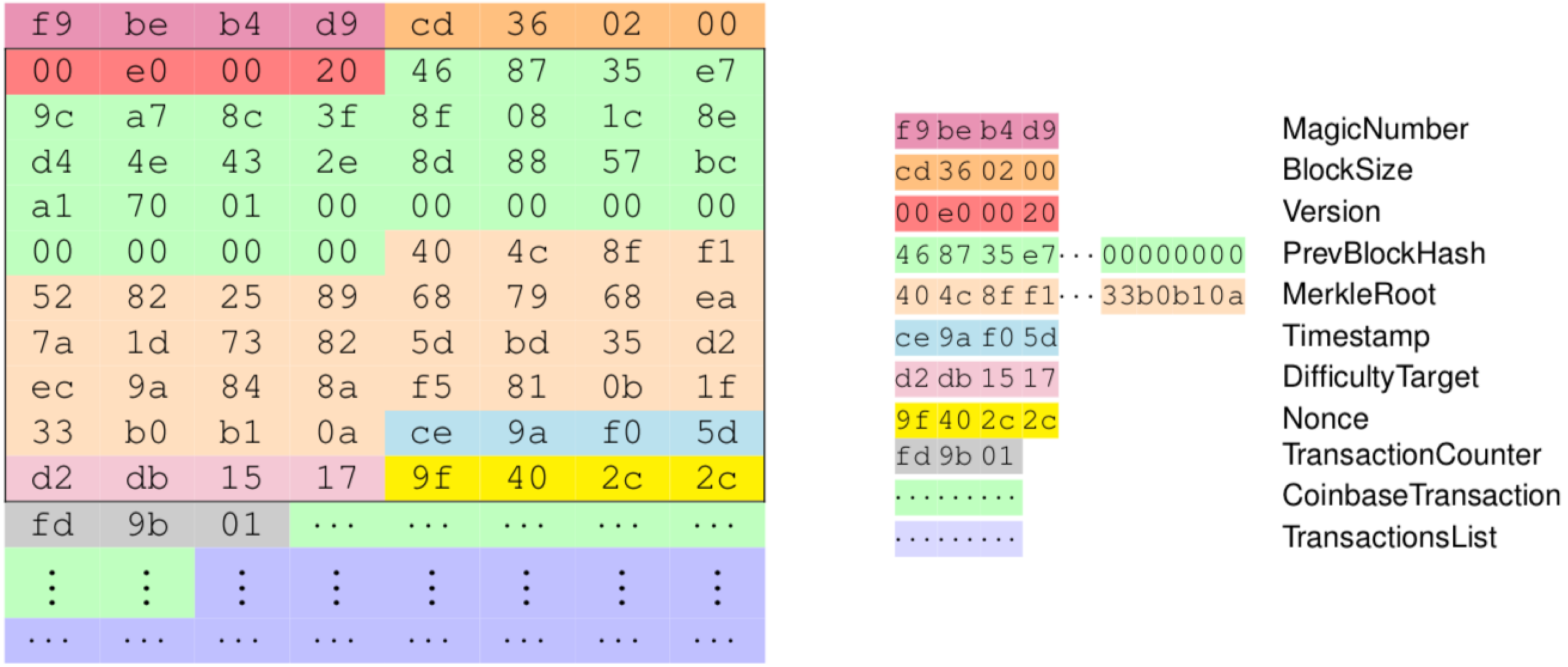
Nakamoto original picture

Transaction structure



Dimension	Field			Description
4 byte	MagicNumber			0xD9B4BEF9
4 byte	BlockSize			Block dimension
80 byte	Header	4 byte	Version	Software version
		32 byte	PrevBlockHash	Hash of the parent block
		32 byte	MerkleRoot	Hash of the Merkle-tree root of the current block
		4 byte	Timestamp	Timestamp of the block
		4 byte	DifficultyTarget	Difficulty
		4 byte	Nonce	PoW Counter
1-9 byte	TransactionCounter			Number of transactions following
Variable	CoinbaseTransaction			Coinbase transaction
	TransactionsList	$\leqslant$ 1Mb		Other transactions of the block

Logical structure of a block

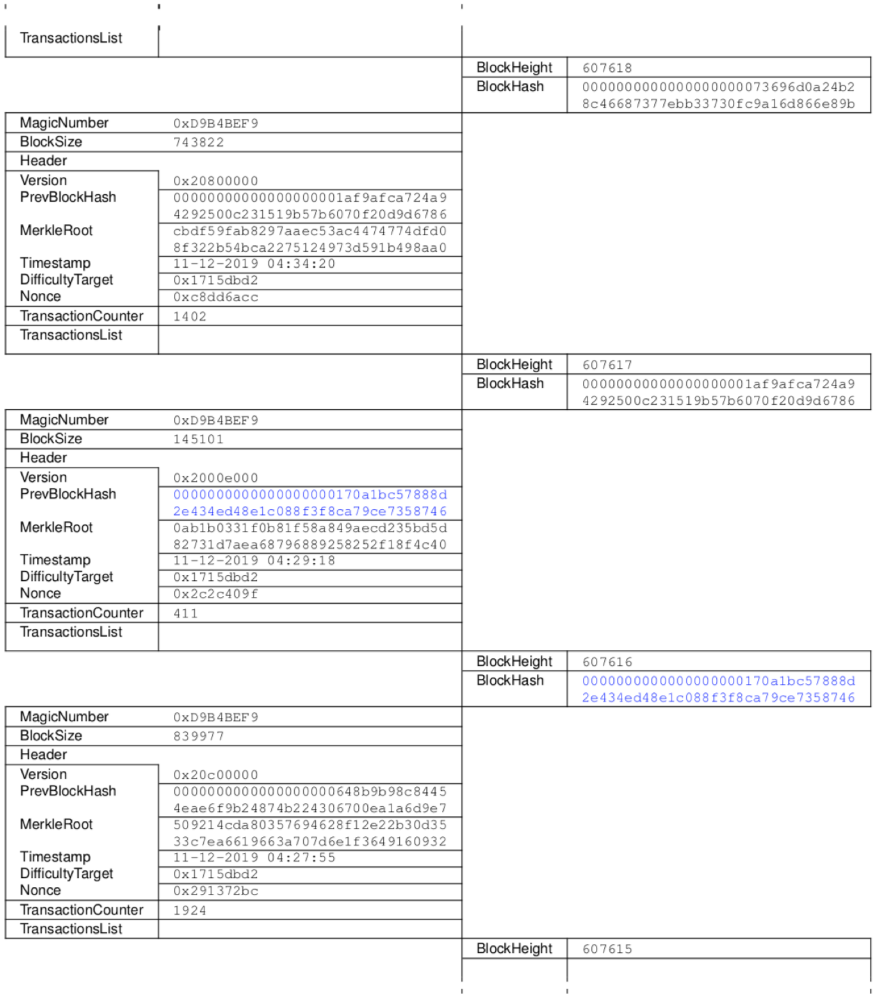


f9	be	b4	d9	cd	36	02	00
00	e0	00	20	46	87	35	e7
9c	a7	8c	3f	8f	08	1c	8e
d4	4e	43	2e	8d	88	57	bc
a1	70	01	00	00	00	00	00
00	00	00	00	40	4c	8f	f1
52	82	25	89	68	79	68	ea
7a	1d	73	82	5d	bd	35	d2
ec	9a	84	8a	f5	81	0b	1f
33	b0	b1	0a	ce	9a	f0	5d
d2	db	15	17	9f	40	2c	2c
fd	9b	01	...	...	...	...	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
...	...	...	...	...	...	...	...

f9 be b4 d9	MagicNumber
cd 36 02 00	BlockSize
00 e0 00 20	Version
46 87 35 e7 ··· 00000000	PrevBlockHash
40 4c 8f f1 ··· 33b0b10a	MerkleRoot
ce 9a f0 5d	Timestamp
d2 db 15 17	DifficultyTarget
9f 40 2c 2c	Nonce
fd 9b 01	TransactionCounter
········	CoinbaseTransaction
········	TransactionsList

Hexadecimal structure of the Header of block 607617

Transaction structure



TransactionsList	

BlockHeight	607618
BlockHash	0000000000000000000073696d0a24b2 8c46687377ebb33730fc9a16d866e89b

MagicNumber	0xD9B4BEF9
BlockSize	743822
Header	
Version	0x20800000
PrevBlockHash	00000000000000000001af9afca724a9 4292500c231519b57b6070f20d9d6786
MerkleRoot	cbdf59fab8297aaec53ac4474774dfd0 8f322b54bca2275124973d591b498aa0
Timestamp	11-12-2019 04:34:20
DifficultyTarget	0x1715dbd2
Nonce	0xc8dd6acc
TransactionCounter	1402
TransactionsList	

BlockHeight	607617
BlockHash	00000000000000000001af9afca724a9 4292500c231519b57b6070f20d9d6786

MagicNumber	0xD9B4BEF9
BlockSize	145101
Header	
Version	0x2000e000
PrevBlockHash	0000000000000000000170a1bc57888d 2e434ed48e1c088f3f8ca79ce7358746
MerkleRoot	0ab1b0331f0b81f58a849aecd235bd5d 82731d7aea68796889258252f18f4c40
Timestamp	11-12-2019 04:29:18
DifficultyTarget	0x1715dbd2
Nonce	0x2c2c409f
TransactionCounter	411
TransactionsList	

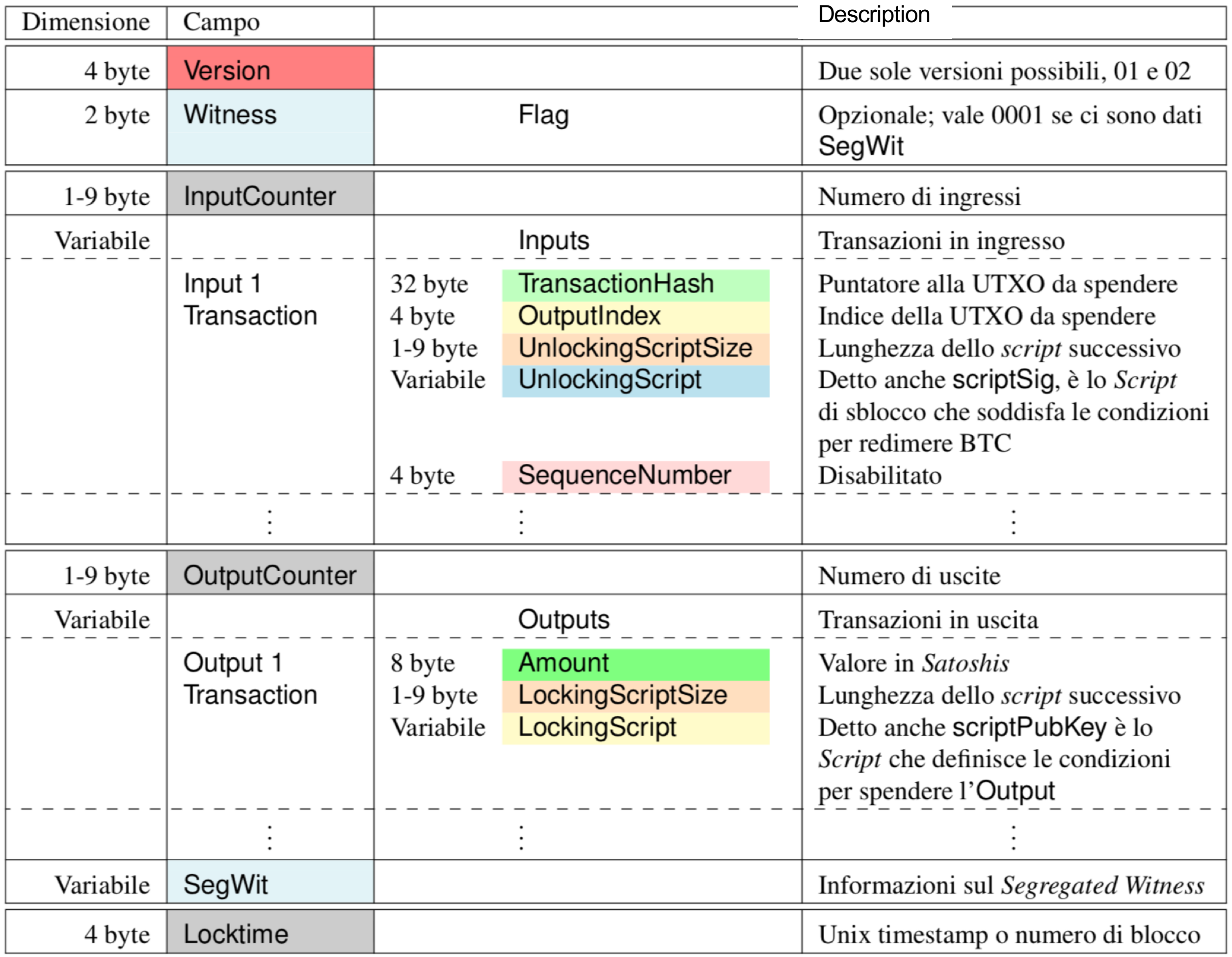
BlockHeight	607616
BlockHash	0000000000000000000170a1bc57888d 2e434ed48e1c088f3f8ca79ce7358746

MagicNumber	0xD9B4BEF9
BlockSize	839977
Header	
Version	0x20c00000
PrevBlockHash	0000000000000000000648b9b98c8445 4eae6f9b24874b224306700ea1a6d9e7
MerkleRoot	509214cda80357694628f12e22b30d35 33c7ea6619663a707d6e1f3649160932
Timestamp	11-12-2019 04:27:55
DifficultyTarget	0x1715dbd2
Nonce	0x291372bc
TransactionCounter	1924
TransactionsList	

BlockHeight	607615

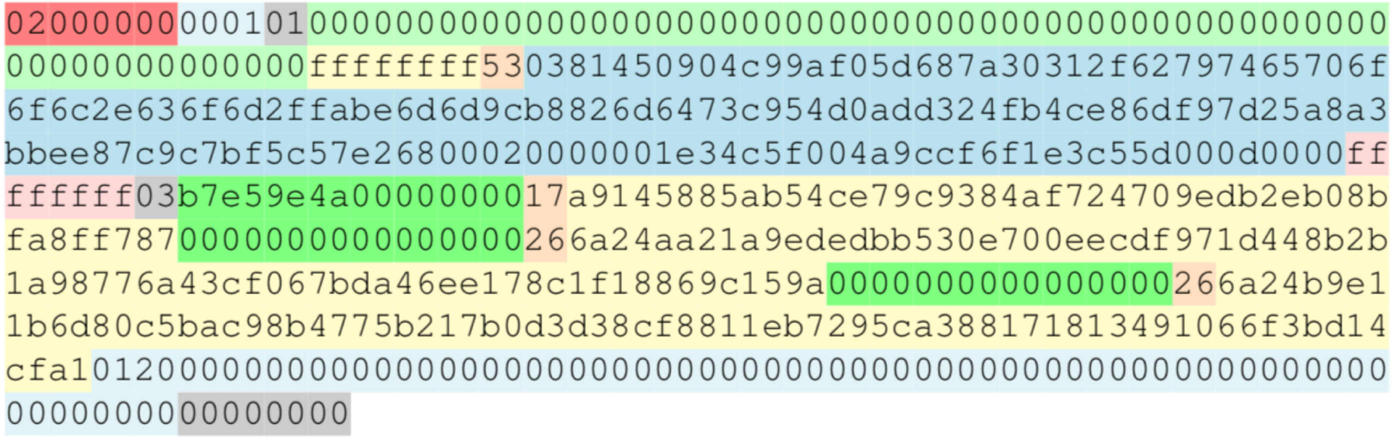
Blockchain structure in correspondence with block 607617

Transaction structure



Dimensione	Campo			Description
4 byte	Version			Due sole versioni possibili, 01 e 02
2 byte	Witness		Flag	Opzionale; vale 0001 se ci sono dati SegWit
1-9 byte	InputCounter			Numero di ingressi
Variabile			Inputs	Transazioni in ingresso
	Input 1 Transaction	32 byte	TransactionHash	Puntatore alla UTXO da spendere
		4 byte	OutputIndex	Indice della UTXO da spendere
		1-9 byte	UnlockingScriptSize	Lunghezza dello *script* successivo
		Variabile	UnlockingScript	Detto anche scriptSig, è lo *Script* di sblocco che soddisfa le condizioni per redimere BTC
		4 byte	SequenceNumber	Disabilitato
	⋮		⋮	⋮
1-9 byte	OutputCounter			Numero di uscite
Variabile			Outputs	Transazioni in uscita
	Output 1 Transaction	8 byte	Amount	Valore in *Satoshis*
		1-9 byte	LockingScriptSize	Lunghezza dello *script* successivo
		Variabile	LockingScript	Detto anche scriptPubKey è lo *Script* che definisce le condizioni per spendere l'Output
	⋮		⋮	⋮
Variabile	SegWit			Informazioni sul *Segregated Witness*
4 byte	Locktime			Unix timestamp o numero di blocco

Structure of a transaction

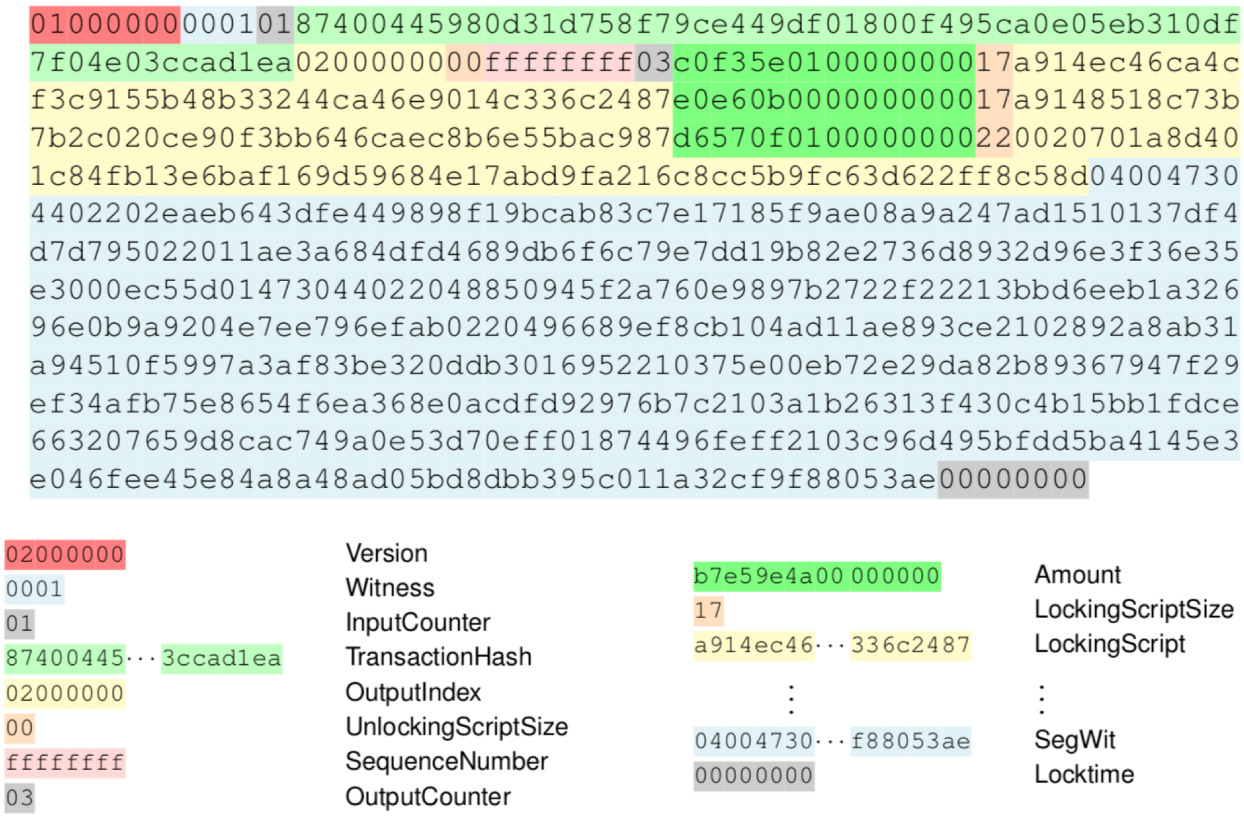


```
0200000000010100000000000000000000000000000000000000000000000000
00000000000000ffffffff530381450904c99af05d687a30312f62797465706f
6f6c2e636f6d2ffabe6d6d9cb8826d6473c954d0add324fb4ce86df97d25a8a3
bbee87c9c7bf5c57e26800020000001e34c5f004a9ccf6f1e3c55d000d0000ff
ffffff03b7e59e4a0000000017a9145885ab54ce79c9384af724709edb2eb08b
fa8ff7870000000000000000266a24aa21a9ededbb530e700eecdf971d448b2b
1a98776a43cf067bda46ee178c1f18869c159a0000000000000000266a24b9e1
1b6d80c5bac98b4775b217b0d3d38cf8811eb7295ca388171813491066f3bd14
cfa1012000000000000000000000000000000000000000000000000000000000
0000000000000000
```

02000000	Version		
0001	Witness	b7e59e4a00 000000	Amount
01	InputCounter	17	LockingScriptSize
00000000···00000000	TransactionHash	a9145885···fa8ff787	LockingScript
ffffffff	OutputIndex	⋮	⋮
53	UnlockingScriptSize	01200000···00000000	SegWit
03814509···000d0000	UnlockingScript	00000000	Locktime
ffffffff	SequenceNumber		
03	OutputCounter		

Hexadecimal structure of the Coinbase transaction of block 607617

Transaction structure



```
01000000000101874004459 80d31d758f79ce449df01800f495ca0e05eb310df
```

```
0100000000010187400445980d31d758f79ce449df01800f495ca0e05eb310df
7f04e03ccad1ea0200000000ffffffff03c0f35e010000000017a914ec46ca4c
f3c9155b48b33244ca46e9014c336c2487e0e60b000000000017a9148518c73b
7b2c020ce90f3bb646caec8b6e55bac987d6570f01000000002200207 01a8d40
1c84fb13e6baf169d59684e17abd9fa216c8cc5b9fc63d622ff8c58d04004730
4402202eaeb643dfe449898f19bcab83c7e17185f9ae08a9a247ad1510137df4
d7d795022011ae3a684dfd4689db6f6c79e7dd19b82e2736d8932d96e3f36e35
e3000ec55d0147304402204885094 5f2a760e9897b2722f22213bbd6eeb1a326
96e0b9a9204e7ee796efab0220496689ef8cb104ad11ae893ce2102892a8ab31
a94510f5997a3af83be320ddb3016952210375e00eb72e29da82b89367947f29
ef34afb75e8654f6ea368e0acdfd92976b7c2103a1b26313f430c4b15bb1fdce
663207659d8cac749a0e53d70eff01874496feff2103c96d495bfdd5ba4145e3
e046fee45e84a8a48ad05bd8dbb395c011a32cf9f88053ae00000000
```

02000000	Version	b7e59e4a00 000000	Amount
0001	Witness	17	LockingScriptSize
01	InputCounter	a914ec46···336c2487	LockingScript
87400445···3ccad1ea	TransactionHash	⋮	⋮
02000000	OutputIndex	04004730···f88053ae	SegWit
00	UnlockingScriptSize	00000000	Locktime
ffffffff	SequenceNumber		
03	OutputCounter		

Hexadecimal structure of the first transaction after the Coinbase of block 607617.

Type of BTC transactions

Pay-to-Public-Key (P2PK) This is the type of transaction present in the first versions of the Bitcoin protocol. It is the simplest, since the recipient's public key is used direa ctly as LockingScript.

Pay-to-Public-Key-Hash (P2PKH) It is the evolution of P2PK; instead of the recipient's public key, the Hash of the same is used within the LockingScript.

MultiSig - (MS) This is a type used in cases where it is necessary to use a certain amount of BTC on several different keys; the associated LockingScript is particularly cumbersome.

Pay-to-Script-Hash (P2SH) It is an evolution of MS, based on the use of the Hash of the corresponding MultiSig LockingScript.

DataStorage - (DS) It is a type used to store data on a BTC transaction that does not lead to UTXO. It is therefore a transaction without transfer of value.

Transaction structure

```
010000....000000434104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225
f374cd378d71302fa28414e7aab37397f554a7df5f142c21c1b7303b8a0626f1
baded5c72a704f7e6cd84cac00286bee....999b8643f656b412a3ac00000000
```

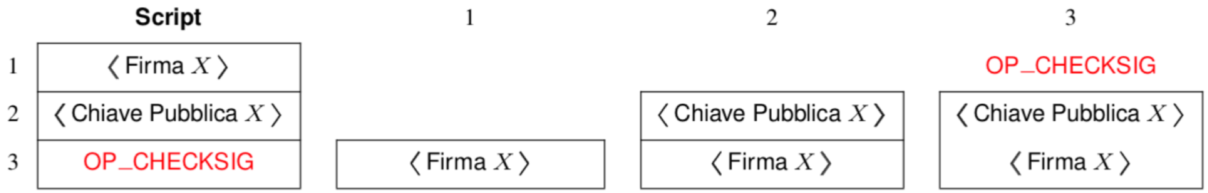
`41`	lunghezza di ⟨Chiave Pubblica X⟩
`04ae1a62···7e6cd84c`	⟨Chiave Pubblica X⟩
`ac`	OP_CHECKSIG

Hexadecimal structure of the block 170 in which are highlighted the scriptPubKey parts

```
010000....00000048473044022057649 7b7e6f9b553c0aba0d8929432550e09
2db9c130aae37b84b545e7f4a36c022066cb982ed80608372c139d7bb9af3354
23d5280350fe3e06bd510e695480914f01ffffffff....ed5cbb88ac00000000
```

`47`	lunghezza di ⟨ Firma X⟩
`30440220···80914f01`	⟨Firma X⟩

Hexadecimal structure of the block 92240 in which are highlighted the scriptSig parts



	Script	1	2	3
1	⟨Firma X⟩			OP_CHECKSIG
2	⟨Chiave Pubblica X⟩		⟨Chiave Pubblica X⟩	⟨Chiave Pubblica X⟩
3	OP_CHECKSIG	⟨Firma X⟩	⟨Firma X⟩	⟨Firma X⟩

Script computation of a P2PK transaction

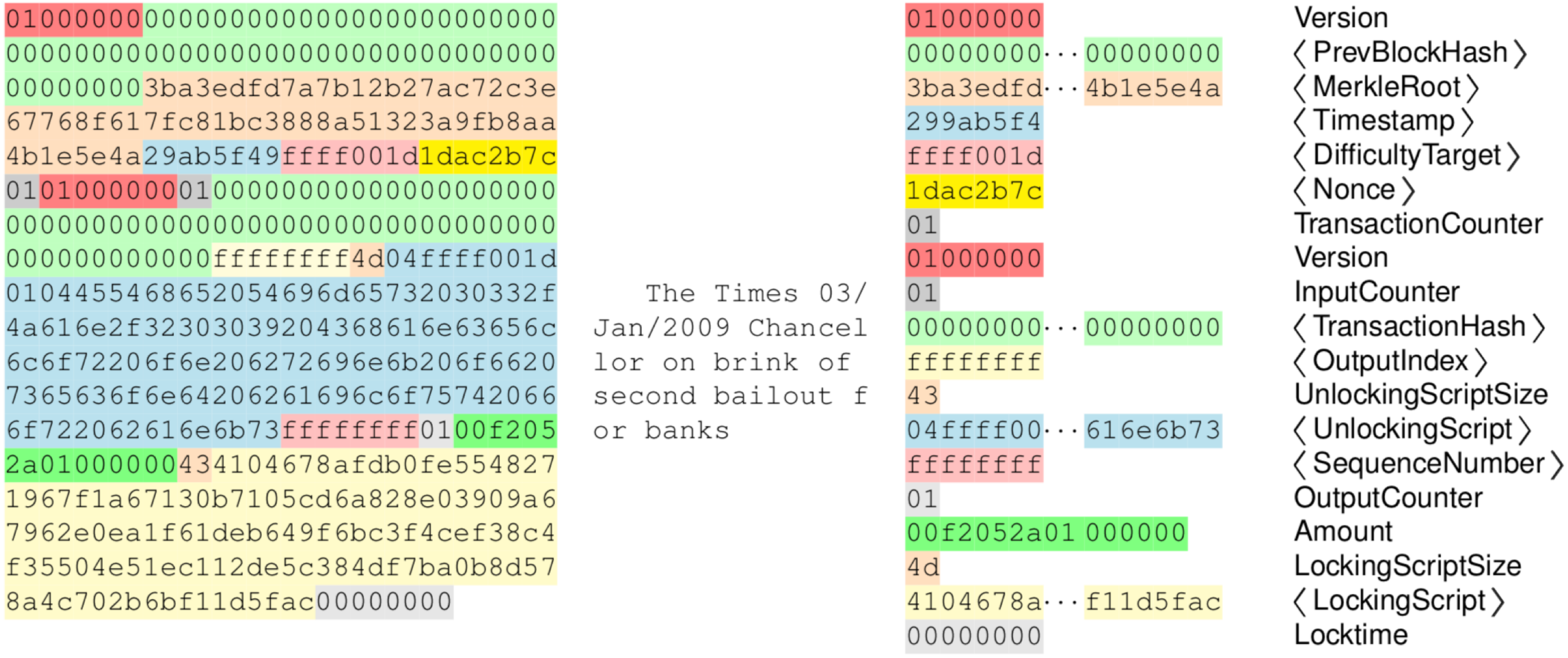
Bitcoin Script

- Interpreted language that uses a stack (stack language)
- It is NOT Turing-complete

ALCUNI OPERATORI DEL LINGUAGGIO BITCOIN SCRIPT

Operatore	Hex	Descrizione
OP_0	0x00	An empty array of bytes is pushed onto the stack
OP_VERIFY	0x69	**Marks transaction as invalid** if top stack value is not true.
OP_DUP	0x76	Duplicates the top stack item.
OP_EQUAL	0x87	Returns 1 if the inputs are exactly equal, 0 otherwise.
OP_EQUALVERIFY	0x88	Same as OP_EQUAL, but runs OP_VERIFY afterward.
OP_ADD	0x93	a is added to b.
OP_MUL	0x95	a is multiplied by b (disabled)
OP_HASH160	0xa9	Compute RIPEMD(SHA256(*x*))
OP_CHECKSIG	0xac	Get a public key and a signature and check if the signature is correct outputting True if it is

The Bitcoin network can be used to store data forever



```
01000000000000000000000000000000
00000000000000000000000000000000
000000003ba3edfd7a7b12b27ac72c3e
67768f617fc81bc3888a51323a9fb8aa
4b1e5e4a29ab5f49ffff001d1dac2b7c
01010000000100000000000000000000
00000000000000000000000000000000
000000000000ffffffff4d04ffff001d
0104455468652054696d65732030332f
4a616e2f32303039204368616e63656c
6c6f72206f6e206272696e6b206f6620
7365636f6e64206261696c6f75742066
6f722062616e6b73ffffffff0100f205
2a01000000434104678afdb0fe554827
1967f1a67130b7105cd6a828e03909a6
7962e0ea1f61deb649f6bc3f4cef38c4
f35504e51ec112de5c384df7ba0b8d57
8a4c702b6bf11d5fac00000000
```

```
   The Times 03/
Jan/2009 Chancel
lor on brink of
second bailout f
or banks
```

01000000	Version
00000000···00000000	⟨PrevBlockHash⟩
3ba3edfd···4b1e5e4a	⟨MerkleRoot⟩
299ab5f4	⟨Timestamp⟩
ffff001d	⟨DifficultyTarget⟩
1dac2b7c	⟨Nonce⟩
01	TransactionCounter
01000000	Version
01	InputCounter
00000000···00000000	⟨TransactionHash⟩
ffffffff	⟨OutputIndex⟩
43	UnlockingScriptSize
04ffff00···616e6b73	⟨UnlockingScript⟩
ffffffff	⟨SequenceNumber⟩
01	OutputCounter
00f2052a01 000000	Amount
4d	LockingScriptSize
4104678a···f11d5fac	⟨LockingScript⟩
00000000	Locktime

Text contained in the first BTC transaction between Nakamoto and Finney, inside the first sworn block, the Genesis Block

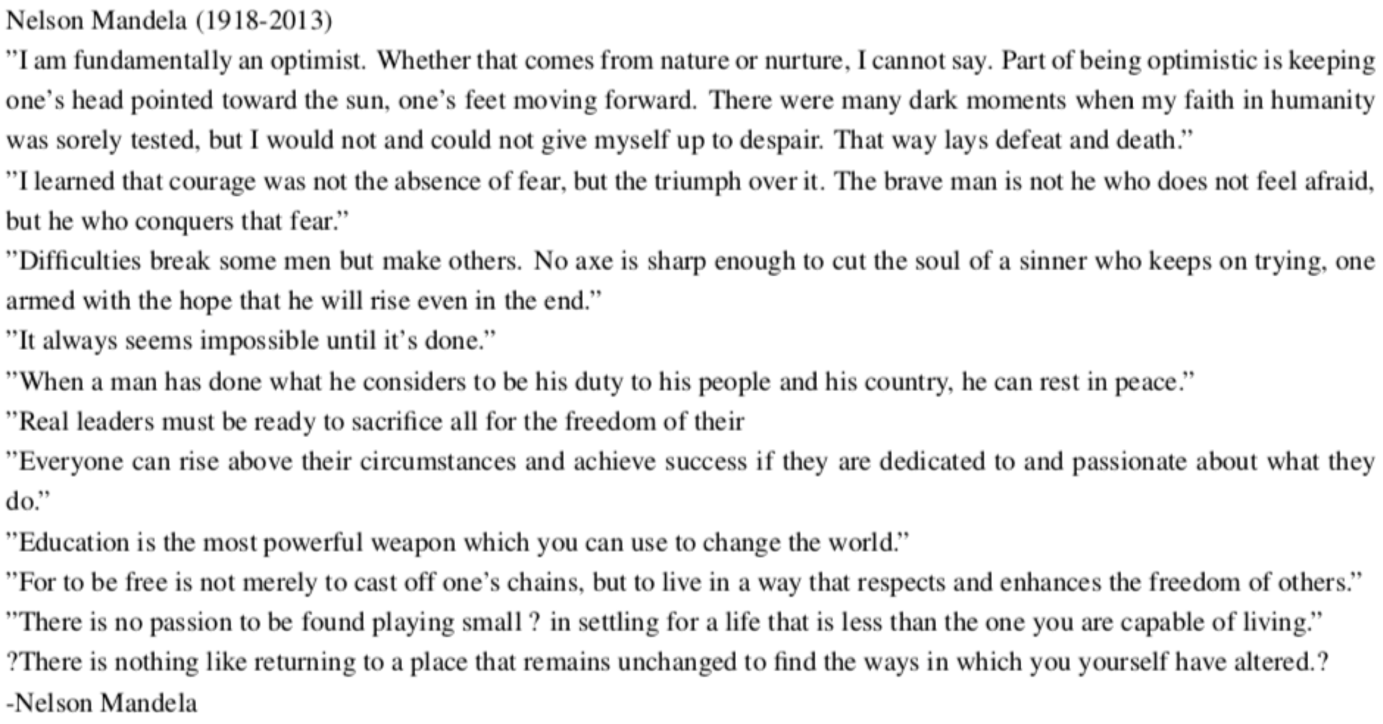
The Bitcoin network can be used to store data forever

Tribute to Nelson Mandela, present in the transaction

```
8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba
```

Picture of Nelson Mandela contained in blcock 273536

Within the transaction there is also the following written text:



Nelson Mandela (1918-2013)

”I am fundamentally an optimist. Whether that comes from nature or nurture, I cannot say. Part of being optimistic is keeping one’s head pointed toward the sun, one’s feet moving forward. There were many dark moments when my faith in humanity was sorely tested, but I would not and could not give myself up to despair. That way lays defeat and death.”

”I learned that courage was not the absence of fear, but the triumph over it. The brave man is not he who does not feel afraid, but he who conquers that fear.”

”Difficulties break some men but make others. No axe is sharp enough to cut the soul of a sinner who keeps on trying, one armed with the hope that he will rise even in the end.”

”It always seems impossible until it’s done.”

”When a man has done what he considers to be his duty to his people and his country, he can rest in peace.”

”Real leaders must be ready to sacrifice all for the freedom of their

”Everyone can rise above their circumstances and achieve success if they are dedicated to and passionate about what they do.”

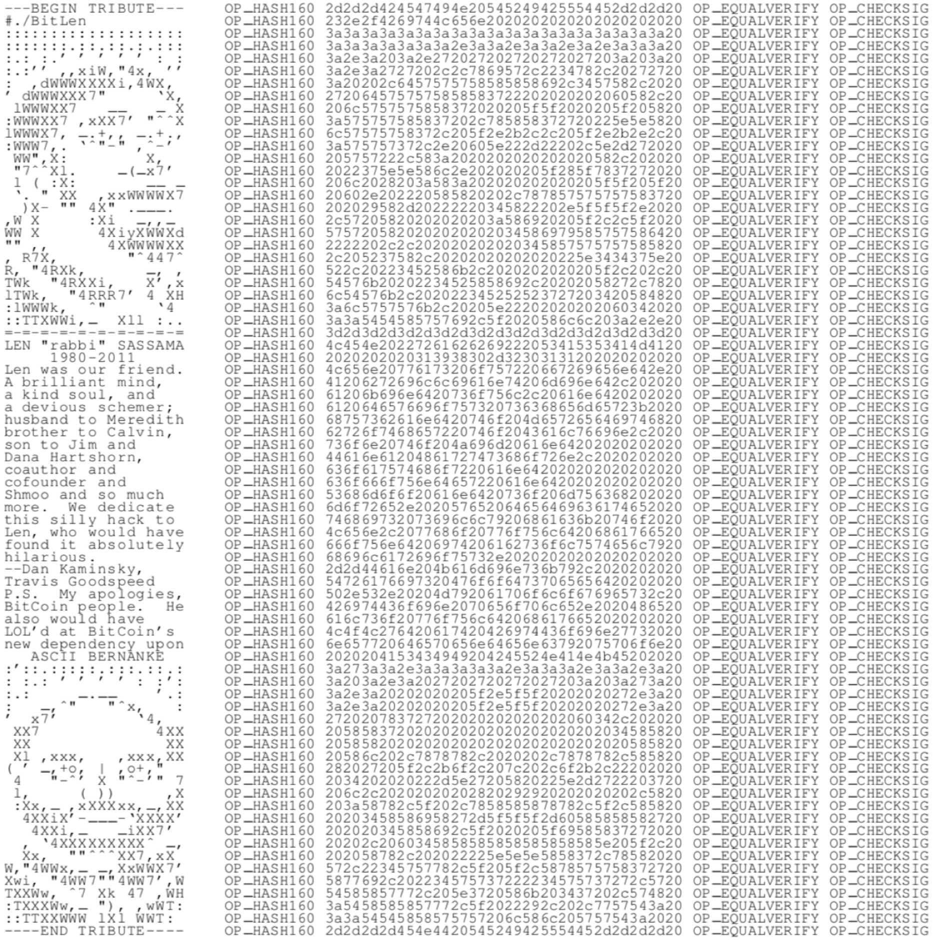
”Education is the most powerful weapon which you can use to change the world.”

”For to be free is not merely to cast off one’s chains, but to live in a way that respects and enhances the freedom of others.”

”There is no passion to be found playing small ? in settling for a life that is less than the one you are capable of living.”

?There is nothing like returning to a place that remains unchanged to find the ways in which you yourself have altered.?

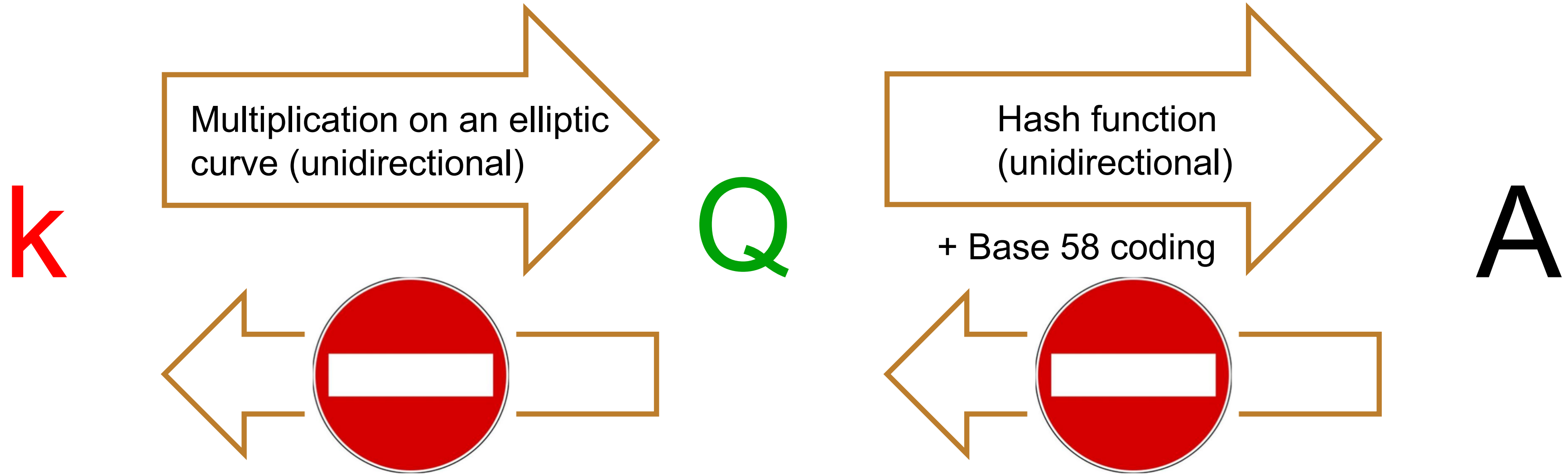
-Nelson Mandela



```
---BEGIN TRIBUTE---     OP_HASH160 2d2d2d424547494e20545249425554452d2d2d20 OP_EQUALVERIFY OP_CHECKSIG
#./BitLen               OP_HASH160 232e2f4269744c656e2020202020202020202020 OP_EQUALVERIFY OP_CHECKSIG
:::::::::::::::::::     OP_HASH160 3a3a3a3a3a3a3a3a3a3a3a3a3a3a3a3a3a3a3a20 OP_EQUALVERIFY OP_CHECKSIG
:::::::.::.::.:.:::     OP_HASH160 3a3a3a3a3a3a3a2e3a3a2e3a3a2e3a2e3a3a3a20 OP_EQUALVERIFY OP_CHECKSIG
:.: :.’ ’ ’ ’ ’ : :     OP_HASH160 3a2e3a203a2e272027202720272027203a203a20 OP_EQUALVERIFY OP_CHECKSIG
:.:’’ ,,xiW,"4x, ’’     OP_HASH160 3a2e3a2727202c2c7869572c2234782c20272720 OP_EQUALVERIFY OP_CHECKSIG
:  ,dWWWXXXXi,4WX,      OP_HASH160 3a20202c6457575758585858692c3457582c2020 OP_EQUALVERIFY OP_CHECKSIG
’ dWWWXXX7"     `X,     OP_HASH160 2720645757575858583722202020202060582c20 OP_EQUALVERIFY OP_CHECKSIG
 lWWWXX7   __   _ X     OP_HASH160 206c5757575858372020205f5f2020205f205820 OP_EQUALVERIFY OP_CHECKSIG
:WWWXX7 ,xXX7’ "^^X     OP_HASH160 3a575757585837202c785858372720225e5e5820 OP_EQUALVERIFY OP_CHECKSIG
lWWWX7, _.+,, _.+.,     OP_HASH160 6c57575758372c205f2e2b2c2c205f2e2b2e2c20 OP_EQUALVERIFY OP_CHECKSIG
:WWW7,. `^"-" ,^-’      OP_HASH160 3a575757372c2e20605e222d22202c5e2d272020 OP_EQUALVERIFY OP_CHECKSIG
 WW",X:         X,      OP_HASH160 205757222c583a202020202020202020582c2020 OP_EQUALVERIFY OP_CHECKSIG
 "7^^Xl.    _(_x7’      OP_HASH160 2022375e5e586c2e202020205f285f7837272020 OP_EQUALVERIFY OP_CHECKSIG
 l ( :X:       __ _     OP_HASH160 206c2028203a583a202020202020205f5f205f20 OP_EQUALVERIFY OP_CHECKSIG
 `. " XX  ,xxWWWWX7     OP_HASH160 20602e202220585820202c787857575757583720 OP_EQUALVERIFY OP_CHECKSIG
  )X- "" 4X" .___.      OP_HASH160 202029582d20222220345822202e5f5f5f2e2020 OP_EQUALVERIFY OP_CHECKSIG
,W X     :Xi  _,,_      OP_HASH160 2c57205820202020203a586920205f2c2c5f2020 OP_EQUALVERIFY OP_CHECKSIG
WW X      4XiyXWWXd     OP_HASH160 5757205820202020202034586979585757586420 OP_EQUALVERIFY OP_CHECKSIG
"" ,,      4XWWWWXX     OP_HASH160 2222202c2c202020202020345857575757585820 OP_EQUALVERIFY OP_CHECKSIG
, R7X,       "^447^     OP_HASH160 2c205237582c20202020202020225e3434375e20 OP_EQUALVERIFY OP_CHECKSIG
R, "4RXk,      _, ,     OP_HASH160 522c20223452586b2c2020202020205f2c202c20 OP_EQUALVERIFY OP_CHECKSIG
TWk  "4RXXi,   X’,x     OP_HASH160 54576b20202234525858692c20202058272c7820 OP_EQUALVERIFY OP_CHECKSIG
lTWk,  "4RRR7’ 4 XH     OP_HASH160 6c54576b2c202022345252523727203420584820 OP_EQUALVERIFY OP_CHECKSIG
:lWWWk,  ^"     `4      OP_HASH160 3a6c5757576b2c20205e22202020202060342020 OP_EQUALVERIFY OP_CHECKSIG
::TTXWWi,_  Xll :..     OP_HASH160 3a3a5454585757692c5f2020586c6c203a2e2e20 OP_EQUALVERIFY OP_CHECKSIG
=-=-=-=-=-=-=-=-=-=     OP_HASH160 3d2d3d2d3d2d3d2d3d2d3d2d3d2d3d2d3d2d3d20 OP_EQUALVERIFY OP_CHECKSIG
LEN "rabbi" SASSAMA     OP_HASH160 4c454e20227261626269222053415353414d4120 OP_EQUALVERIFY OP_CHECKSIG
     1980-2011          OP_HASH160 2020202020313938302d32303131202020202020 OP_EQUALVERIFY OP_CHECKSIG
Len was our friend.     OP_HASH160 4c656e20776173206f757220667269656e642e20 OP_EQUALVERIFY OP_CHECKSIG
A brilliant mind,       OP_HASH160 41206272696c6c69616e74206d696e642c202020 OP_EQUALVERIFY OP_CHECKSIG
a kind soul, and        OP_HASH160 61206b696e6420736f756c2c20616e6420202020 OP_EQUALVERIFY OP_CHECKSIG
a devious schemer;      OP_HASH160 6120646576696f757320736368656d65723b2020 OP_EQUALVERIFY OP_CHECKSIG
husband to Meredith     OP_HASH160 68757362616e6420746f204d6572656469746820 OP_EQUALVERIFY OP_CHECKSIG
brother to Calvin,      OP_HASH160 62726f7468657220746f2043616c76696e2c2020 OP_EQUALVERIFY OP_CHECKSIG
son to Jim and          OP_HASH160 736f6e20746f204a696d20616e64202020202020 OP_EQUALVERIFY OP_CHECKSIG
Dana Hartshorn,         OP_HASH160 44616e61204861727473686f726e2c2020202020 OP_EQUALVERIFY OP_CHECKSIG
coauthor and            OP_HASH160 636f617574686f7220616e642020202020202020 OP_EQUALVERIFY OP_CHECKSIG
cofounder and           OP_HASH160 636f666f756e64657220616e6420202020202020 OP_EQUALVERIFY OP_CHECKSIG
Shmoo and so much       OP_HASH160 53686d6f6f20616e6420736f206d756368202020 OP_EQUALVERIFY OP_CHECKSIG
more.  We dedicate      OP_HASH160 6d6f72652e202057652064656469636174652020 OP_EQUALVERIFY OP_CHECKSIG
this silly hack to      OP_HASH160 746869732073696c6c79206861636b20746f2020 OP_EQUALVERIFY OP_CHECKSIG
Len, who would have     OP_HASH160 4c656e2c2077686f20776f756c64206861766520 OP_EQUALVERIFY OP_CHECKSIG
found it absolutely     OP_HASH160 666f756e64206974206162736f6c7574656c7920 OP_EQUALVERIFY OP_CHECKSIG
hilarious.              OP_HASH160 68696c6172696f75732e20202020202020202020 OP_EQUALVERIFY OP_CHECKSIG
--Dan Kaminsky,         OP_HASH160 2d2d44616e204b616d696e736b792c2020202020 OP_EQUALVERIFY OP_CHECKSIG
Travis Goodspeed        OP_HASH160 54726176697320476f6f64737065656420202020 OP_EQUALVERIFY OP_CHECKSIG
P.S.  My apologies,     OP_HASH160 502e532e20204d792061706f6c6f676965732c20 OP_EQUALVERIFY OP_CHECKSIG
BitCoin people.  He     OP_HASH160 426974436f696e2070656f706c652e2020486520 OP_EQUALVERIFY OP_CHECKSIG
also would have         OP_HASH160 616c736f20776f756c6420686176652020202020 OP_EQUALVERIFY OP_CHECKSIG
LOL’d at BitCoin’s      OP_HASH160 4c4f4c276420617420426974436f696e27732020 OP_EQUALVERIFY OP_CHECKSIG
new dependency upon     OP_HASH160 6e657720646570656e64656e63792075706f6e20 OP_EQUALVERIFY OP_CHECKSIG
   ASCII BERNANKE       OP_HASH160 2020204153434949204245524e414e4b45202020 OP_EQUALVERIFY OP_CHECKSIG
:’::.:::::.:::.::.:     OP_HASH160 3a273a3a2e3a3a3a3a3a2e3a3a3a2e3a3a2e3a20 OP_EQUALVERIFY OP_CHECKSIG
: :.: ’ ’ ’ ’ : :’:     OP_HASH160 3a203a2e3a2027202720272027203a203a273a20 OP_EQUALVERIFY OP_CHECKSIG
:.:     _.__    ’.:     OP_HASH160 3a2e3a20202020205f2e5f5f20202020272e3a20 OP_EQUALVERIFY OP_CHECKSIG
;   _,^"    "^x,   :    OP_HASH160 3a2e3a20202020205f2e5f5f20202020272e3a20 OP_EQUALVERIFY OP_CHECKSIG
’  x7’        `4,       OP_HASH160 272020783727202020202020202060342c202020 OP_EQUALVERIFY OP_CHECKSIG
 XX7            4XX     OP_HASH160 2058583720202020202020202020202034585820 OP_EQUALVERIFY OP_CHECKSIG
 XX              XX     OP_HASH160 2058582020202020202020202020202020585820 OP_EQUALVERIFY OP_CHECKSIG
 Xl ,xxx,   ,xxx,XX     OP_HASH160 20586c202c7878782c2020202c7878782c585820 OP_EQUALVERIFY OP_CHECKSIG
( ’ _,+o, | ,o+,"       OP_HASH160 282027205f2c2b6f2c207c202c6f2b2c22202020 OP_EQUALVERIFY OP_CHECKSIG
 4   "-^’ X "^-’" 7     OP_HASH160 2034202020222d5e27205820225e2d2722203720 OP_EQUALVERIFY OP_CHECKSIG
 l,     ( ))     ,X     OP_HASH160 206c2c20202020202820292920202020202c5820 OP_EQUALVERIFY OP_CHECKSIG
 :Xx,_ ,xXXXxx,_,XX     OP_HASH160 203a58782c5f202c7858585878782c5f2c585820 OP_EQUALVERIFY OP_CHECKSIG
  4XXiX’-___-`XXXX’     OP_HASH160 20203458586958272d5f5f5f2d60585858582720 OP_EQUALVERIFY OP_CHECKSIG
   4XXi,_   _iXX7’      OP_HASH160 202020345858692c5f2020205f69585837272020 OP_EQUALVERIFY OP_CHECKSIG
  , `4XXXXXXXXX^ _,     OP_HASH160 20202c2060345858585858585858585e205f2c20 OP_EQUALVERIFY OP_CHECKSIG
  Xx,  ""^^^XX7,xX      OP_HASH160 202058782c202022225e5e5e5858372c78582020 OP_EQUALVERIFY OP_CHECKSIG
W,"4WWx,_ _,XxWWX7’     OP_HASH160 572c22345757782c5f205f2c5878575758372720 OP_EQUALVERIFY OP_CHECKSIG
Xwi, "4WW7""4WW7’,W     OP_HASH160 5877692c202234575737222234575737272c5720 OP_EQUALVERIFY OP_CHECKSIG
TXXWw, ^7 Xk 47 ,WH     OP_HASH160 54585857772c205e3720586b203437202c574820 OP_EQUALVERIFY OP_CHECKSIG
:TXXXWw,_ "), ,wWT:     OP_HASH160 3a5458585857772c5f2022292c202c7757543a20 OP_EQUALVERIFY OP_CHECKSIG
::TTXXWWW lXl WWT:      OP_HASH160 3a3a54545858575757206c586c205757543a2020 OP_EQUALVERIFY OP_CHECKSIG
----END TRIBUTE----     OP_HASH160 2d2d2d2d454e4420545249425554452d2d2d2d20 OP_EQUALVERIFY OP_CHECKSIG
```

Len Sassman's epitaph inserted in block 138725. The associated transactions are visible on the right

Private keys, public keys, Bitcoin addresses



k

Multiplication on an elliptic curve (unidirectional)

Q

Hash function (unidirectional)

+ Base 58 coding

A

Private Key

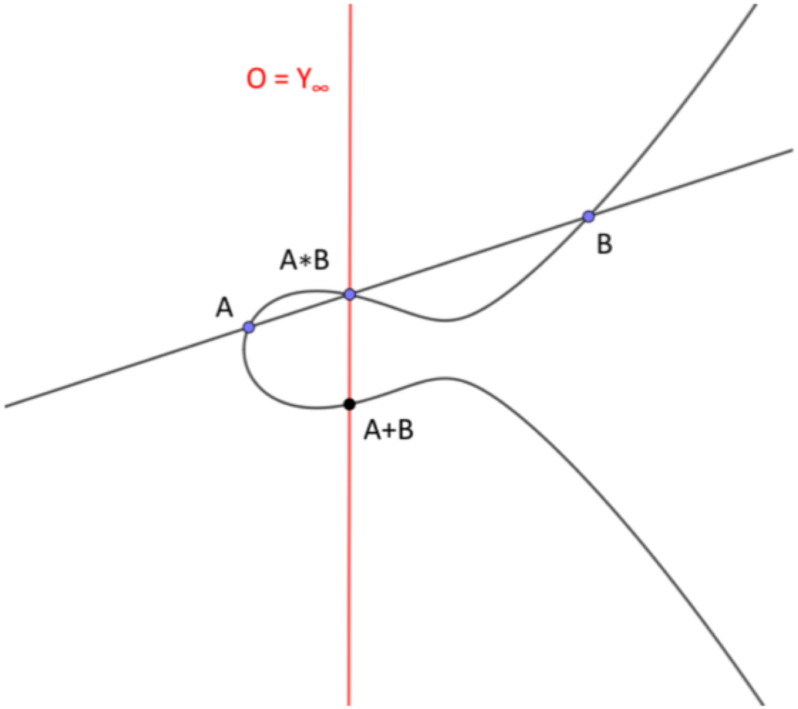
256 bit random

Public Key

(x,y) point on an elliptic curve 512 bit

Bitcoin address

ECDSA – *Elliptic Curve Digital Signature Algorithm*

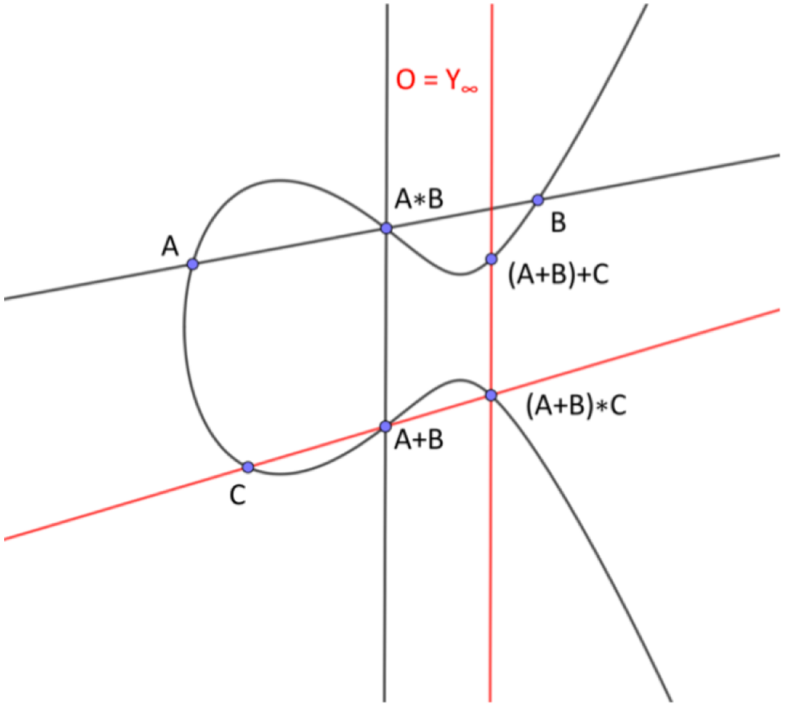


$$y^2 = (x^3 + 7)\text{over}(\mathbb{F}_p)$$

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

standard secp256k1, *National Institute of Standards and Technology* (NIST)

$$Q = k * G$$



(a) $(A + B) + C$

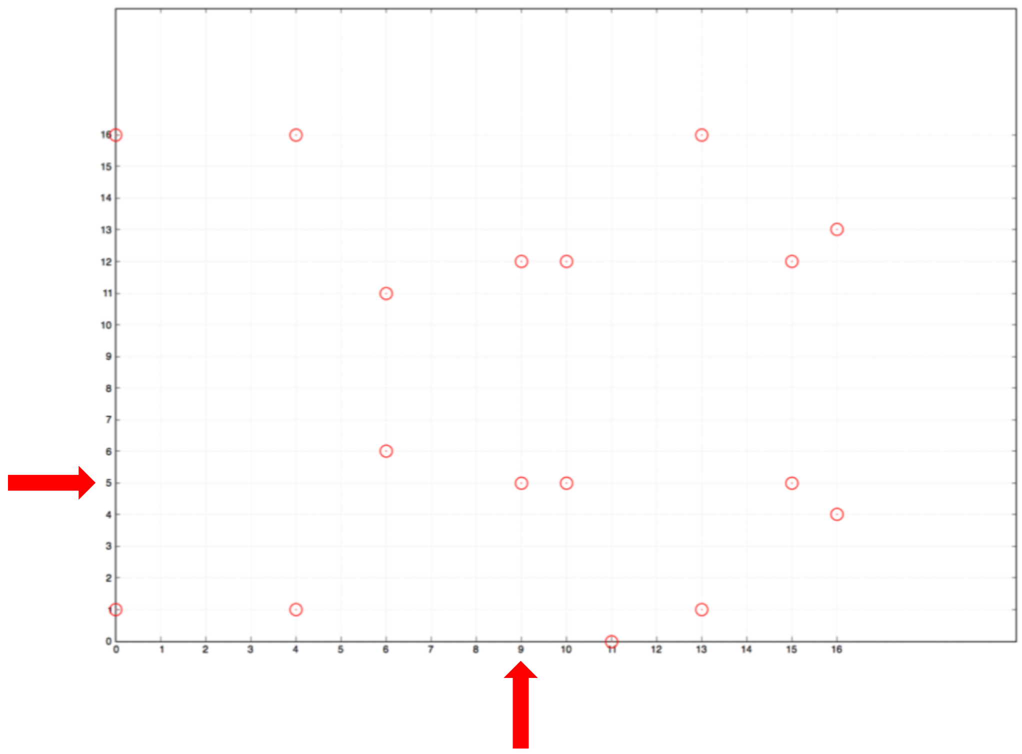
Multiplication on an elliptic curve (unidirectional)

Given *G* and *k*
I find ***Q*** *easily*

Given *G* and ***Q***
it is impossible to find *k*

Q = public key
k = private key
G = generator point

Elliptic curve over *F*(*p*) with *p*=17



$y^2 = x^3 + x + 1$ *mod* 17

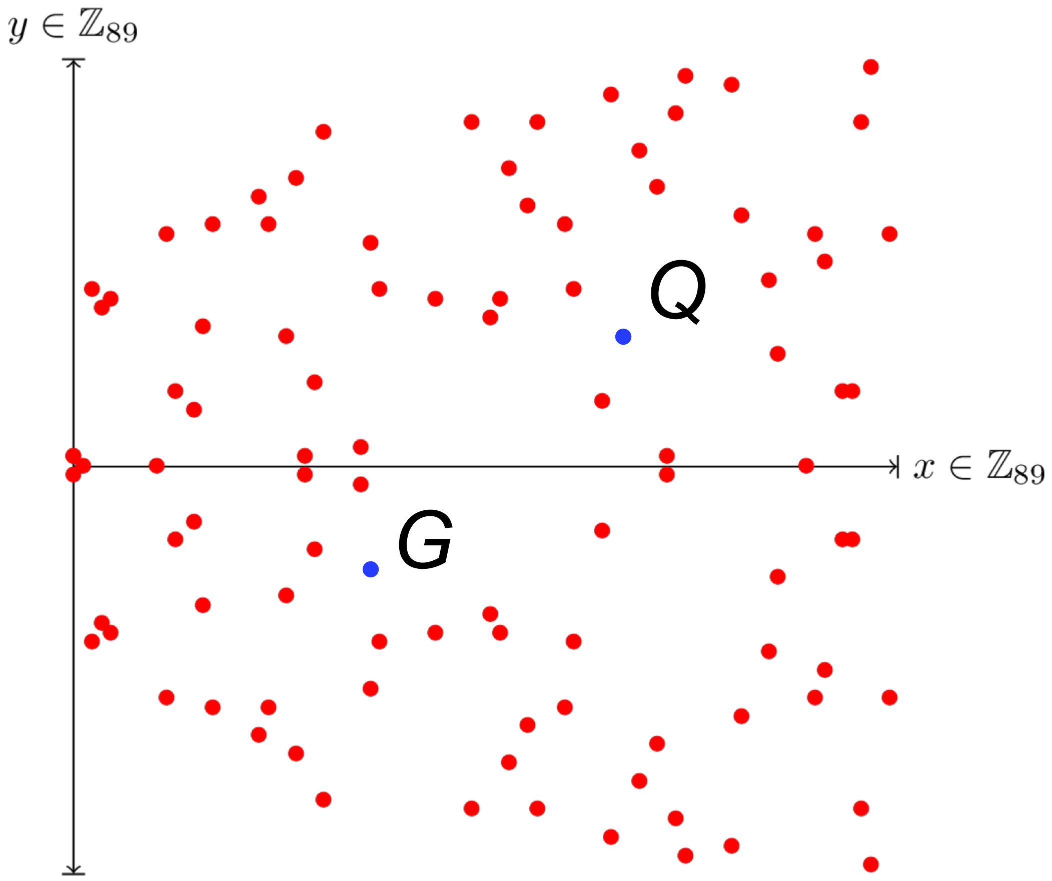
$5^2 = 9^3 + 9 + 1$ *mod* 17

8 = 729 + 9 + 1 *mod* 17

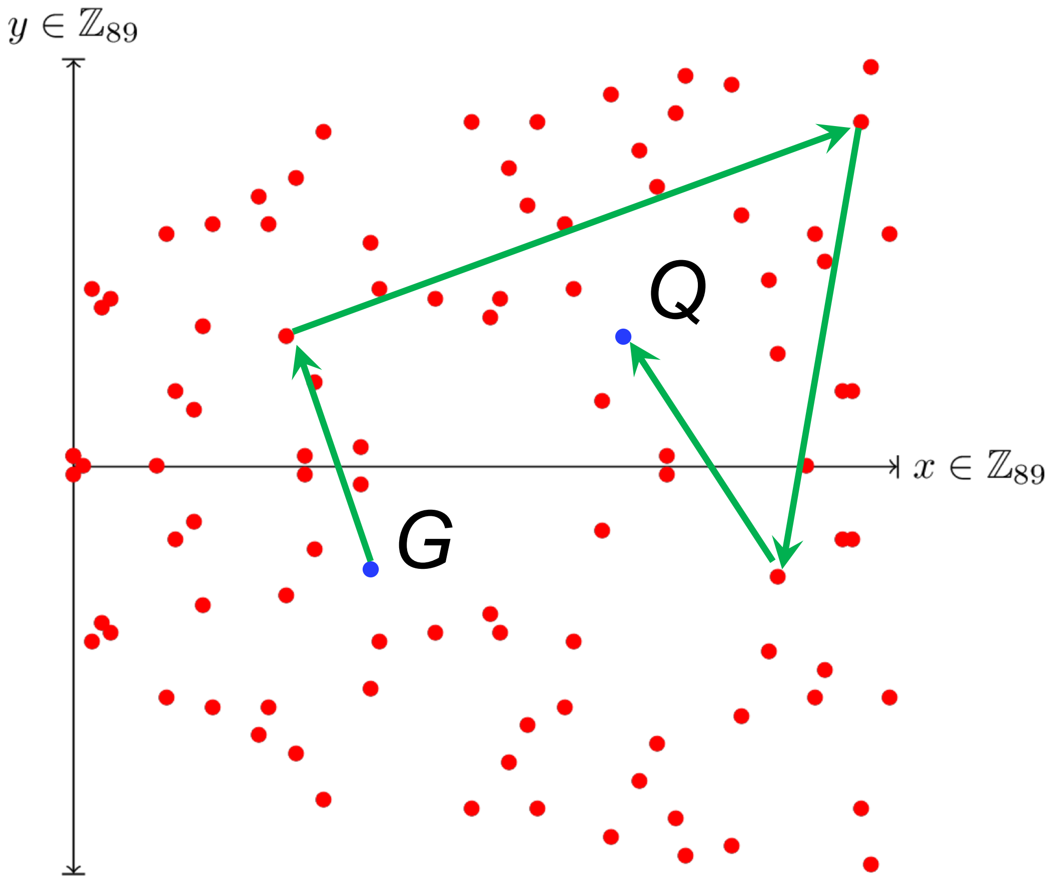
8 = 739 *mod* 17

8 = 43*17 + 8 *mod* 17

Actually we are working on a Galois finite field; here's how it could actually appear the "curve" on a Cartesian plane



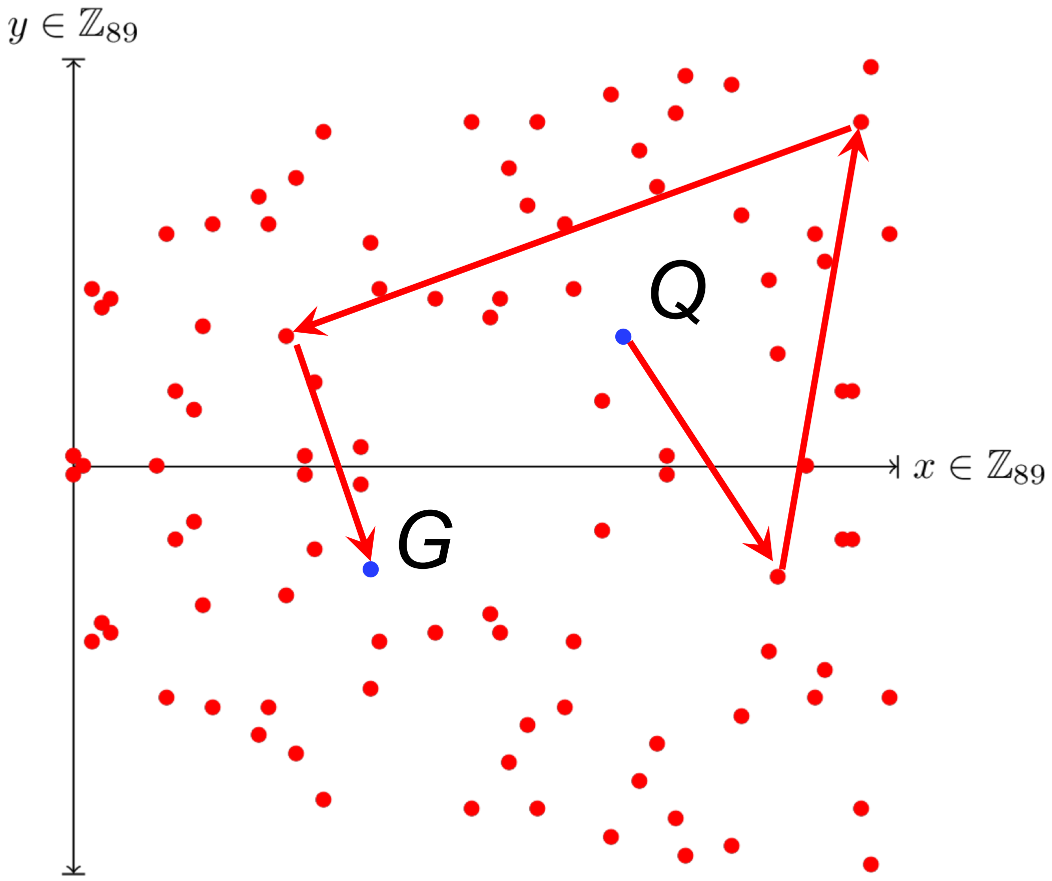
Actually we are working on a Galois finite field; here's how it could actually appear the "curve" on a Cartesian plane



given *k* and *G* compute

Q = *k G* **ease**

Actually we are working on a Galois finite field; here's how it could actually appear the "curve" on a Cartesian plane



given *G* and ***Q*** compute *k* **impossible**

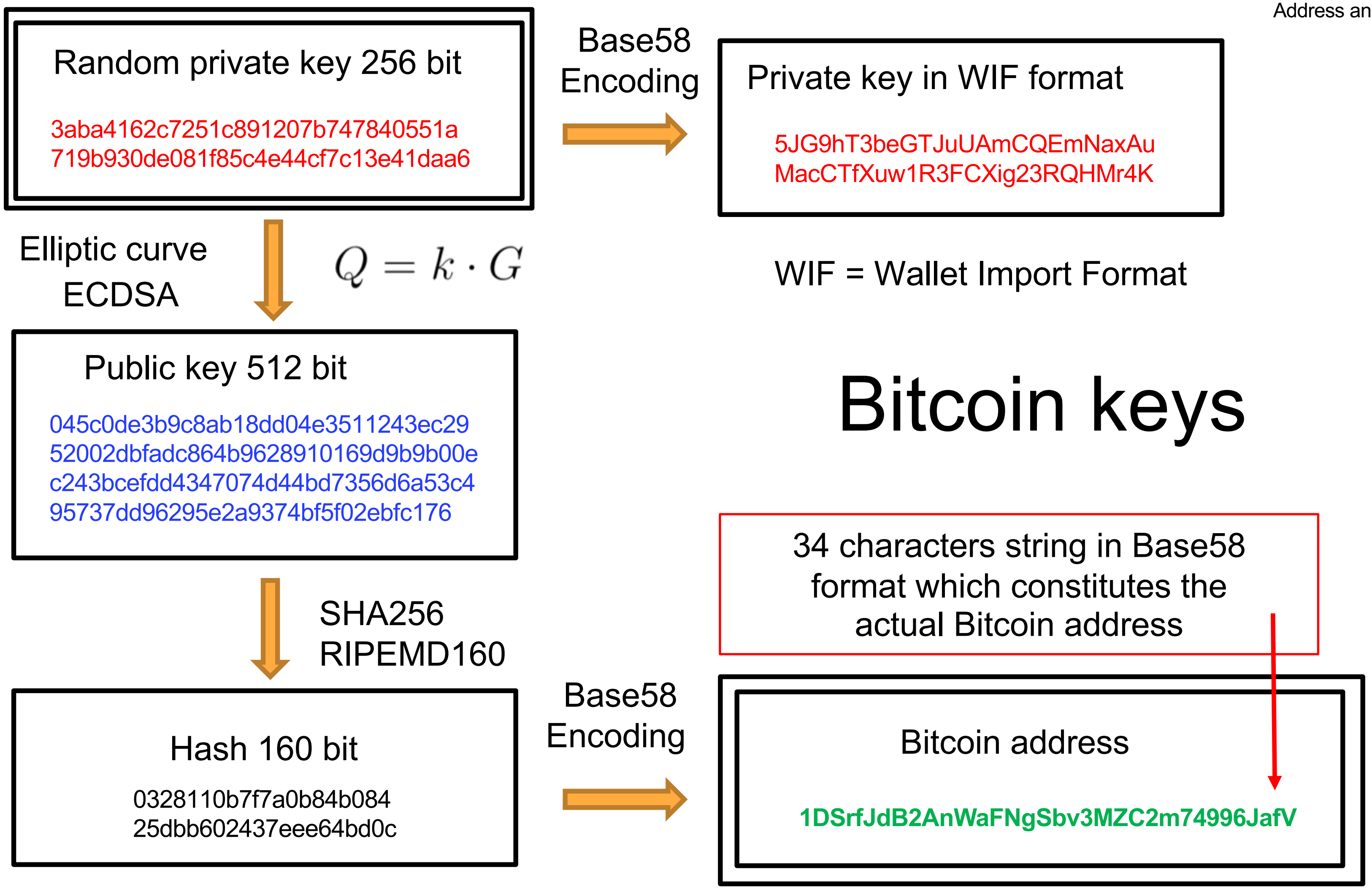
We are on $\mathbb{Z}_p = \mathbb{F}_p$; the ring of integers mod *p* becomes a field with *p* prime

$$
\begin{aligned}
p &= 2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} - 1 \\
&= \texttt{0xffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
&\qquad \texttt{fffffffe fffffc2f}
\end{aligned}
$$

$a = 0$ $\quad b = 7;$ and the eqation of the curve is $x^3 = x + 7$

$$
\begin{aligned}
G_x &= \texttt{0x79be667e f9dcbbac 55a06295 ce870b07 029bfcdb 2dce28d9} \\
&\qquad \texttt{59f2815b 16f81798} \\
G_y &= \texttt{0x483ada77 26a3c465 5da4fbfc 0e1108a8 fd17b448 a6855419} \\
&\qquad \texttt{9c47d08f fb10d4b8} \\
n &= \texttt{0xffffffff ffffffff ffffffff fffffffe baaedce6 af48a03b} \\
&\qquad \texttt{bfd25e8c d0364141} \\
h &= 1
\end{aligned}
$$

Bitcoin keys



Random private key 256 bit

3aba4162c7251c891207b747840551a
719b930de081f85c4e44cf7c13e41daa6

Base58
Encoding

Private key in WIF format

5JG9hT3beGTJuUAmCQEmNaxAu
MacCTfXuw1R3FCXig23RQHMr4K

WIF = Wallet Import Format

Elliptic curve
ECDSA

$$Q = k \cdot G$$

Public key 512 bit

045c0de3b9c8ab18dd04e3511243ec29
52002dbfadc864b9628910169d9b9b00e
c243bcefdd4347074d44bd7356d6a53c4
95737dd96295e2a9374bf5f02ebfc176

SHA256
RIPEMD160

Hash 160 bit

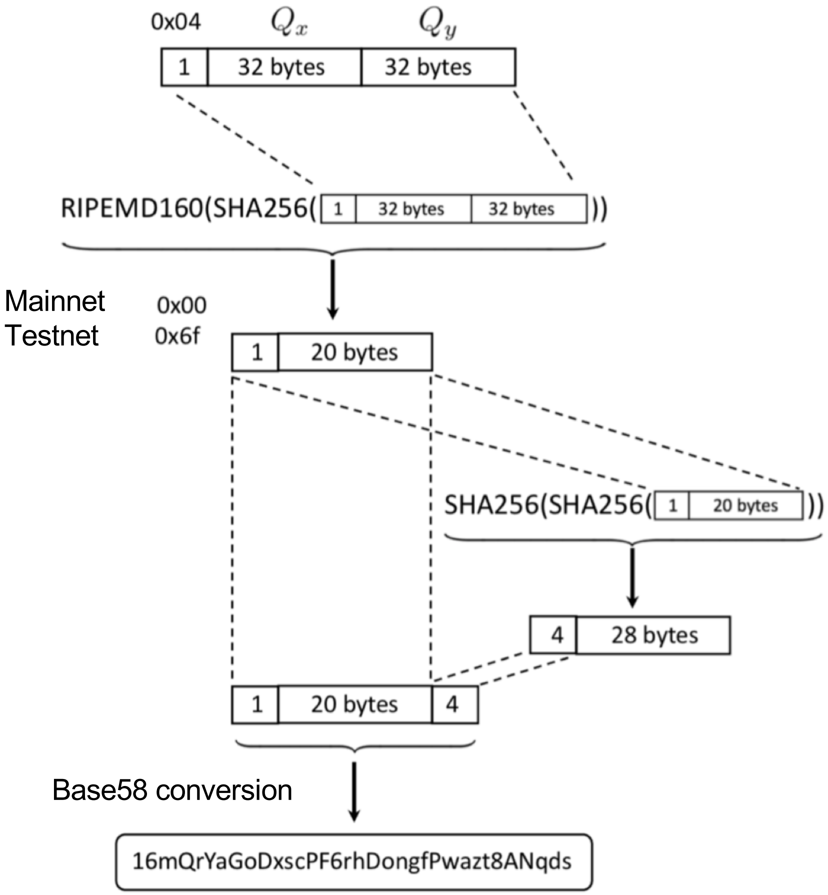
0328110b7f7a0b84b084
25dbb602437eee64bd0c

Base58
Encoding

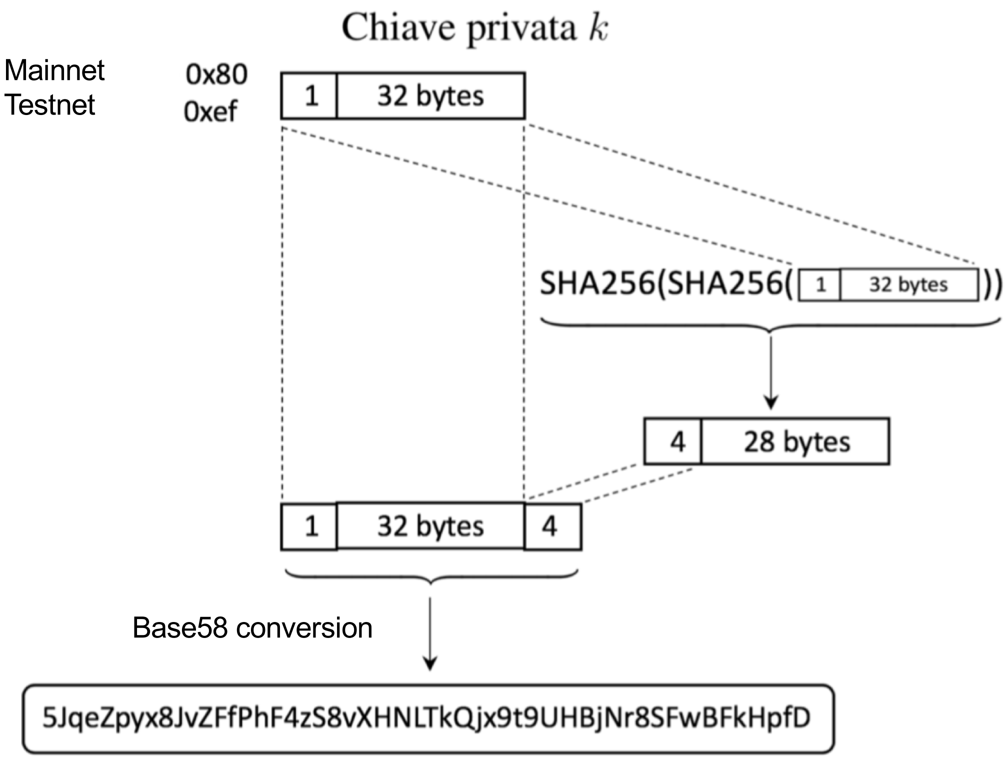
34 characters string in Base58
format which constitutes the
actual Bitcoin address

Bitcoin address

1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV


0x04
Q_x
Q_y
1
32 bytes
32 bytes
RIPEMD160(SHA256(1 32 bytes 32 bytes))
Mainnet 0x00
Testnet 0x6f
1
20 bytes
SHA256(SHA256(1 20 bytes))
4
28 bytes
1
20 bytes
4
Base58 conversion
16mQrYaGoDxscPF6rhDongfPwazt8ANqds

Building a Bitcoin address starting from the public key in the SEC uncompressed format



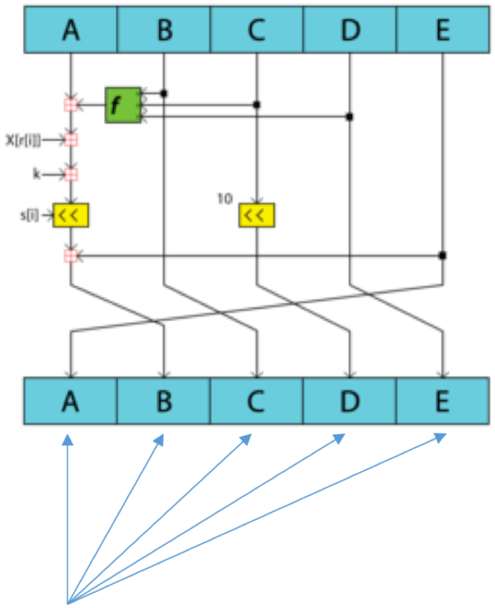
Conversion in the WIF format of a private key *k*

RIPEMD160

SHA256

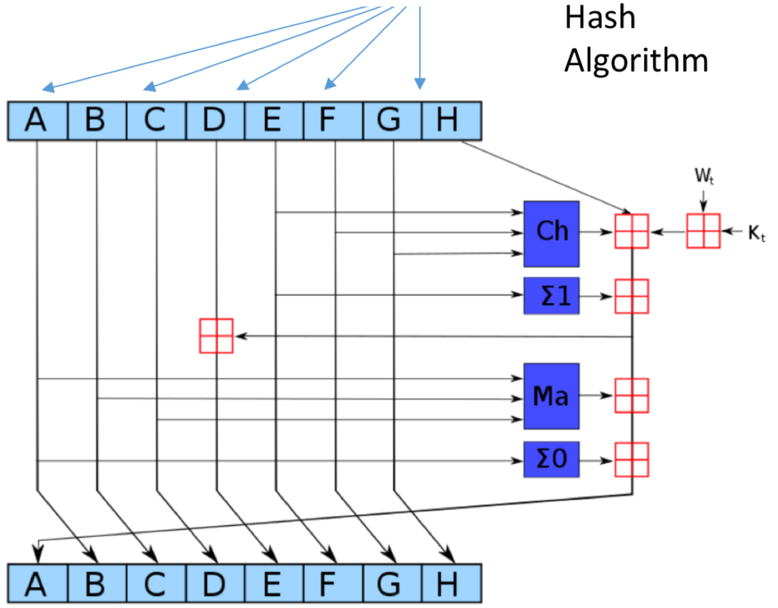
32 bit blocks

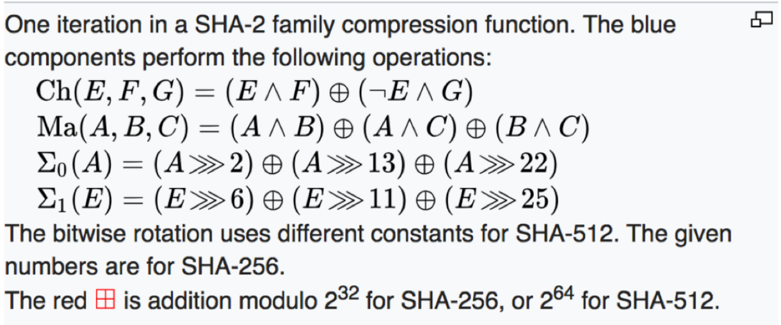
Secure
Hash
Algorithm



32 bit blocks

RACE Integrity Primitives
Evaluation Message Digest



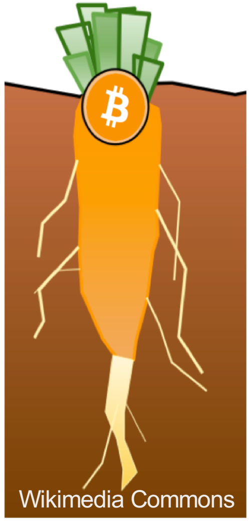

One iteration in a SHA-2 family compression function. The blue components perform the following operations:

$$\mathrm{Ch}(E,F,G) = (E \land F) \oplus (\neg E \land G)$$
$$\mathrm{Ma}(A,B,C) = (A \land B) \oplus (A \land C) \oplus (B \land C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256.

The red ⊞ is addition modulo 2^{32} for SHA-256, or 2^{64} for SHA-512.

Wikimedia Commons

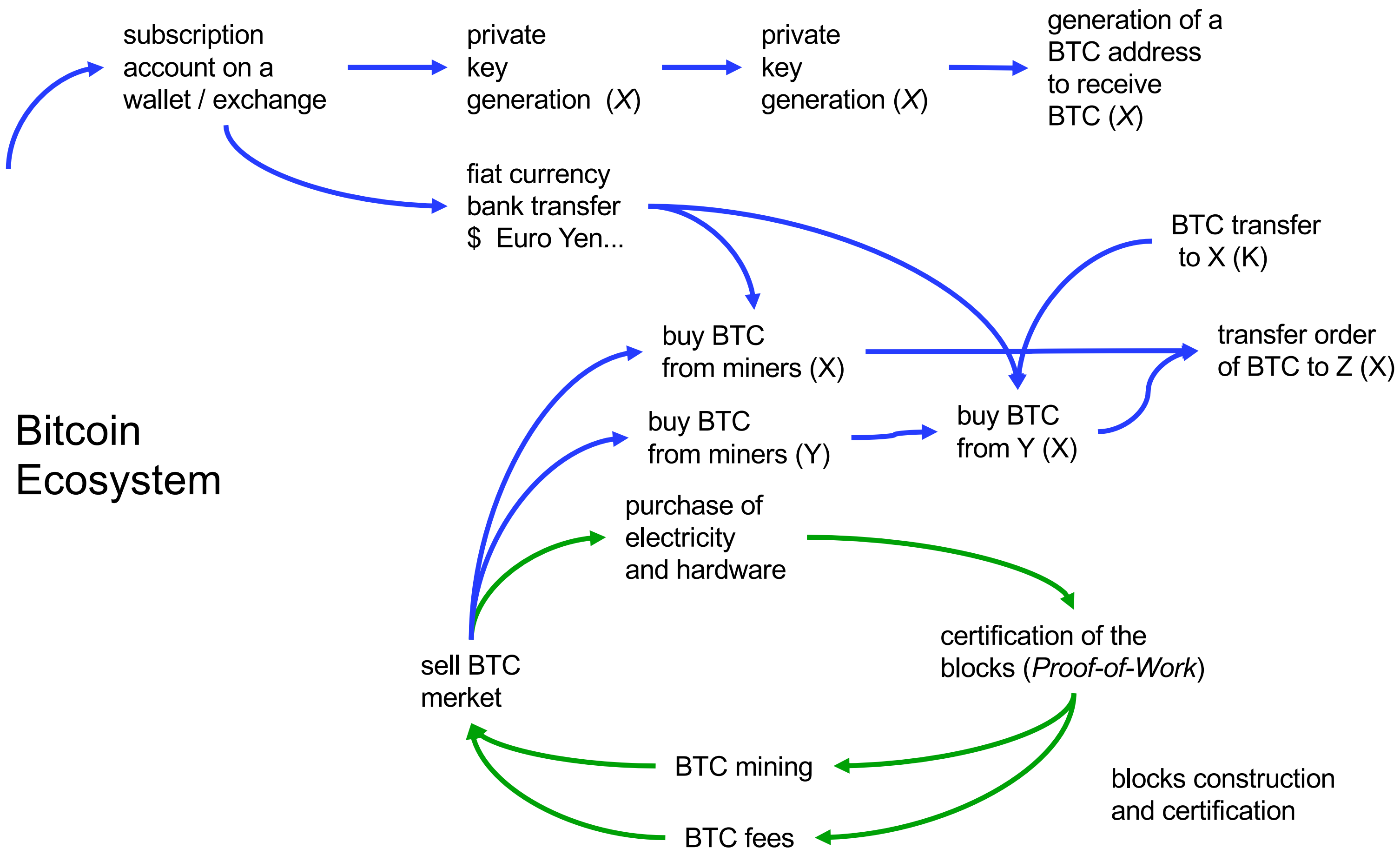

Wikimedia Commons

Taproot improvement (BIP 0341)

(adopted on 14th nov 2021, block 709632)

1. Adoption of a new numerical signature (Schnorr's signature)
2. Possibility of a joint signature between multiple users (different from the old Multisig)
3. Improved network scalability
4. Greater possibilities of use of smart contracts and De-Fi

Bitcoin Ecosystem



subscription account on a wallet / exchange

private key generation (*X*)

private key generation (*X*)

generation of a BTC address to receive BTC (*X*)

fiat currency bank transfer $ Euro Yen...

BTC transfer to X (K)

buy BTC from miners (X)

transfer order of BTC to Z (X)

buy BTC from miners (Y)

buy BTC from Y (X)

purchase of electricity and hardware

certification of the blocks (*Proof-of-Work*)

sell BTC merket

BTC mining

BTC fees

blocks construction and certification

II LEVEL OF ANALYSIS: THE OVERALL ECOSYSTEM

By forking from Bitcoin you get many other altcoins:

Soft-fork (it regards the software protocol)

1. Namecoin (2011 →)
2. Litecoin (2011 →)
3. Bitcoin XT (2015-2016)
4. Bitcoin Classic (2016-2017)
5. Bitcoin Unlimited (2018 →)

Hard-fork (*thin air generation of a new* cryptocurrency)

6. Bitcoin Cash (2017 →)
7. Bitcoin Gold (2018 →)
8. Bitcoin Private (2018 →)
9. Bitcoin SV (2018 →)

Vitaliy Bùterin obtains Ethereum (ETH) by gemmating from Bitcoin

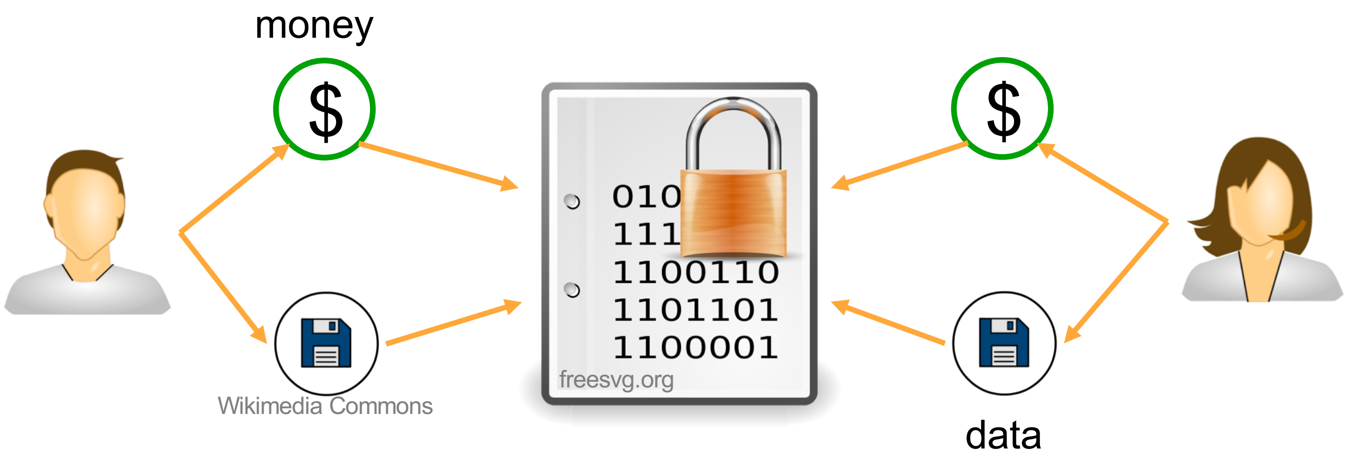
Виталий Дмитриевич Бутерин

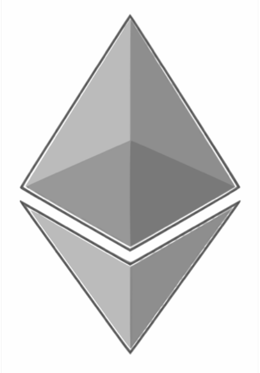
Wikimedia Commons

27 years

- in 2011, at the age of 17, Buterin knows Bitcoin from his father;
- in 2012, he gets a bronze medal in the International Olympics in Computer Science in Russia;
- in 2013 he published the Ethereum white paper.
- he enrolls and attends the University of Waterloo, but in 2014 wins a $ 100,000 scholarship from the Thiel foundation to drop out university and start working on Ethereum full time
- today 09/02/2022 Ethereum has a market value (capitalization) of approx. 484 B$
- his personal assets amount to 330 kETH, around 1 B$

Smart Contracts





freesvg.com

Ethereum: platform for *smart contracts*

1. The value transmitted over the Internet is that associated with smart contracts.
2. A smart contract is an IT protocol intended to facilitate, verify or digitally enforce the negotiation or execution of a contract.
3. Based on a blockchain
4. Smart contracts allow for credible, traceable, and irreversible transactions to be executed without third parties.
5. The goal of smart contracts is to provide greater security than traditional contract law and reduce the other transaction costs associated with bargaining.
6. Based on a **Turing-complete** language (Solidity)

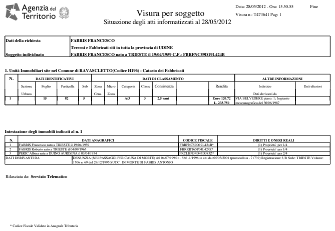
Digital mapping of the physical world and real estate

flickr.com

Via Nomentana 51
Sassari

visure.it

Cadastral map


Agenzia del Territorio

Visura per soggetto
Situazione degli atti informatizzati al 28/05/2012

Data: 28/05/2012 - Ora: 15.50.55 Fine
Visura n.: T473641 Pag: 1

Dati della richiesta	FABRIS FRANCESCO Terreni e Fabbricati siti in tutta la provincia di UDINE
Soggetto individuato	FABRIS FRANCESCO nato a TRIESTE il 19/04/1959 C.F.: FBRFNC59D19L424B

1. Unità Immobiliari site nel Comune di RAVASCLETTO(Codice H196) - Catasto dei Fabbricati

N.	DATI IDENTIFICATIVI				DATI DI CLASSAMENTO							ALTRE INFORMAZIONI	
	Sezione Urbana	Foglio	Particella	Sub	Zona Cens.	Micro Zona	Categoria	Classe	Consistenza		Rendita	Indirizzo Dati derivanti da	Dati ulteriori
1		15	82	5			A/3	3	2,5 vani		Euro 120,72 L. 233.750	VIA BELVEDERE piano: 1; Impianto meccanografico del 30/06/1987	

Intestazione degli immobili indicati al n. 1

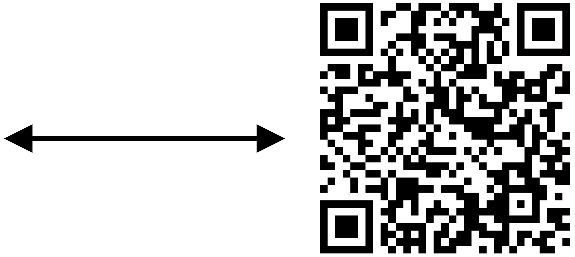
N.	DATI ANAGRAFICI	CODICE FISCALE	DIRITTI E ONERI REALI
1	FABRIS Francesco nato a TRIESTE il 19/04/1959	FBRFNC59D19L424B*	(1) Proprieta` per 1/4
2	FABRIS Roberto nato a TRIESTE il 04/09/1965	FBRRRT65P04L424Z*	(1) Proprieta` per 1/4
3	PERIC Albina nata a DUINO AURISINA il 03/04/1934	PRCLBN34D43D383Z*	(1) Proprieta` per 2/4
DATI DERIVANTI DA	DENUNZIA (NEI PASSAGGI PER CAUSA DI MORTE) del 04/07/1995 n . 566 .1/1996 in atti dal 05/03/2001 (protocollo n . 71739) Registrazione: UR Sede: TRIESTE Volume: 1506 n: 69 del 29/12/1995 SUCC . IN MORTE DI FABRIS ANTONIO		

Rilasciata da: **Servizio Telematico**

* Codice Fiscale Validato in Anagrafe Tributaria

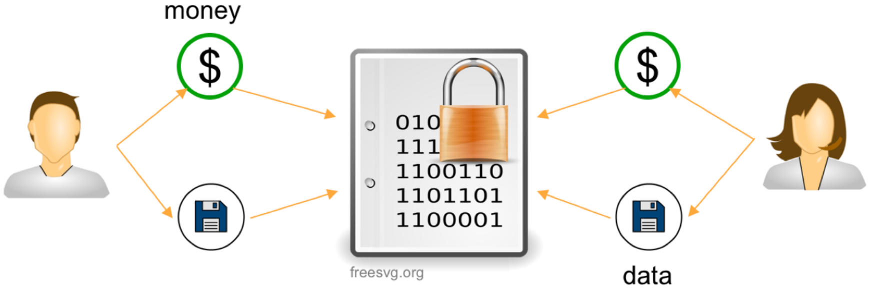
Cadastral data

Wikimedia Commons



Digitized projection
of the villa

trading through smart-contracts



freesvg.org

... presupposes a
land register on the blockchain

Advantages related to a trade on the blockchain

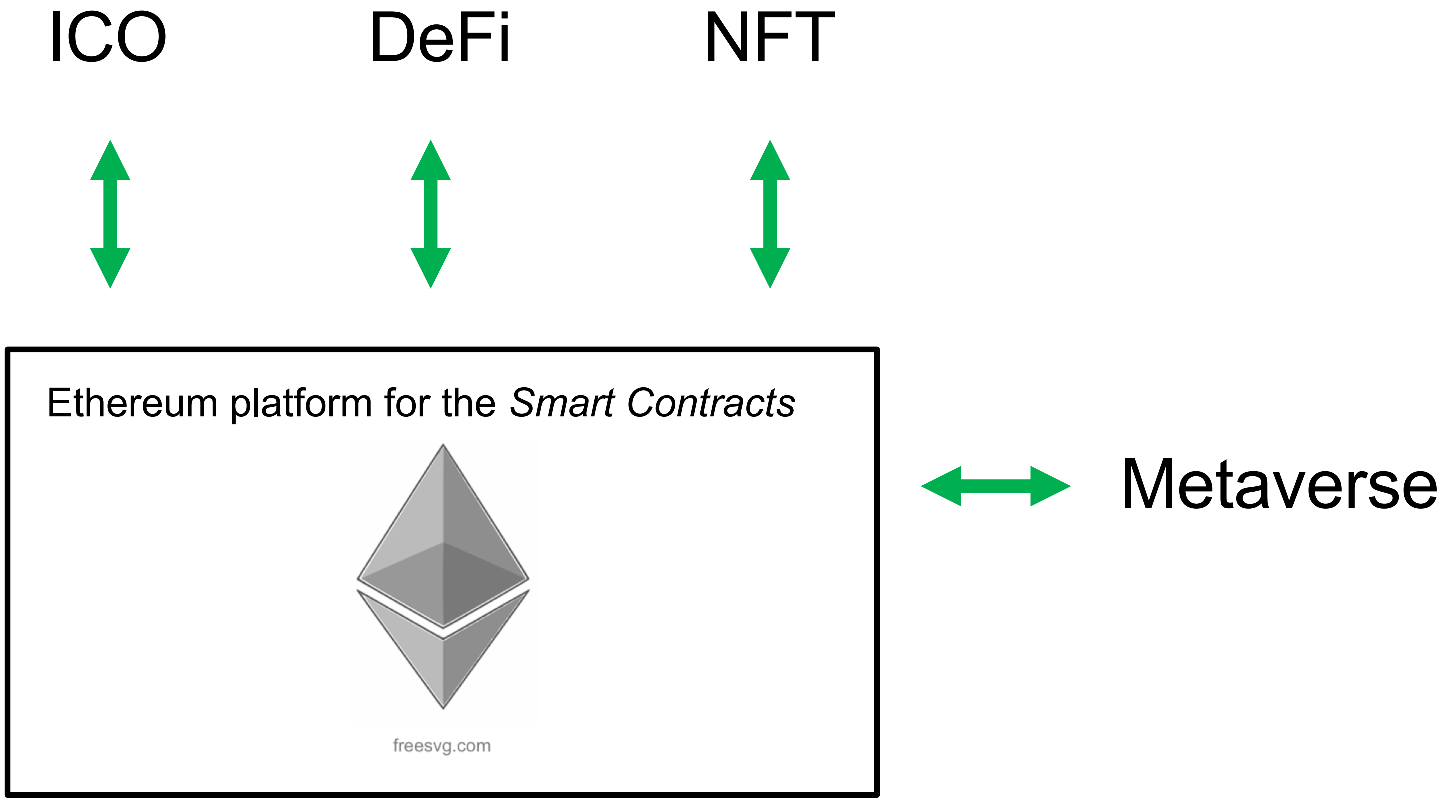
1. without mediation of the notary
2. cost reduction
3. instant
4. h 24/7/365
5. unmodifiable register
6. impossible to build false invoices

The underlying blockchain structure could be of nature private, but also authentically decentralized and otherwise controlled by any central authority.

By choosing a private blockchain, each entity (land registry, PRA, Revenue Agency, banks, insurance companies, ..., but also IMF, OECD, UN, ...) could have their own blockchain based on nodes which are the various servers scattered throughout the national or supranational territory.

By solving the trilemma problem, one could imagine a giant global blockchain, decentralized, unchangeable and not censurable, on which all the states and all the institutions, a bit of what we now have for the Internet

The ecosystems



ICO

DeFi

NFT

Ethereum platform for the *Smart Contracts*

freesvg.com

Metaverse

ICO (*Initial Coin Offering*)
crowdfunding based on smart contracts

Gram	$1.7 billion	10-13 july 2019	Encrypted Messaging & Blockchain Ecosystem
EOS	$4.1 billion	june 17-18	Smart Contracts
Dragon	$320 millions	feb-mar 2018	Decentralized Currency for Casinos
Huobi	$300 millions	jan-feb 2018	Cryptocurrency Exchange
Hdac	$258 millions	nov-dec 2017	IoT Contract & Payment Platform
Filecoin	$257 millions	ago-sept 2017	Decentralized Cloud Storage
Tezos	$232 millions	1-14 jul 2017	Self-Amending Distributed Ledger
Sirin Labs	$158 millions	16-26 dec 2017	Open-Source Blockchain Smartphone
Bancor	$153 millions	12 june 2017	Tokens conversion
DAO	$152 millions	01-28 may 2017	Decentralized VC
	.		
	.		

Altcoins

Today feb 9 2022 there are more than 17000 !

flickr.com

quoteinspector.com

openclipart.com

Platforms for which to exploit ICOs

Generation of altcoins (ERC-20 standard; over 1200 cryptocurrencies created so far)
250 working decentralized applications (DApps)
Cryptocurrencies pegged to fiat currencies
Cryptocurrencies anchored to gold
finance
internet-of-things
agriculture km.0
electricity supply and management
sport bets
digital signatures that guarantee the authenticity and proof of the existence of documents
smart locks
digital rights for music
platforms for forecasting financial markets
crowdfunding platforms
social media platforms
decentralized markets
online gambling
management of charging electric cars
systems for the certification of identity on the Internet
labor economy
video games
financial exchanges ...

Example

Wikimedia Commons

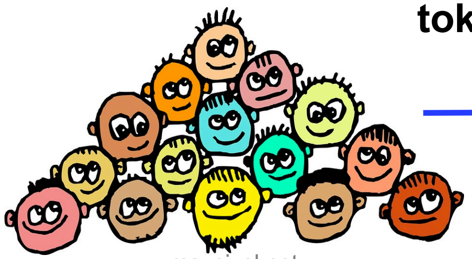
Autobus Trieste Trasporti
up to the train station

FFSS
train Trieste ➞ Venezia

Alitalia (ITA)
VCE ➞ FCO

Latam Airlines
FCO ➞ SCL

ICO



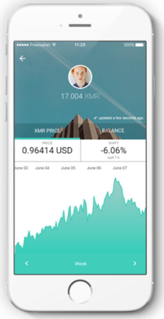
maxpixel.net

Generate the token AIR →

freesvg.org
Wikimedia Commons

AIR ↓

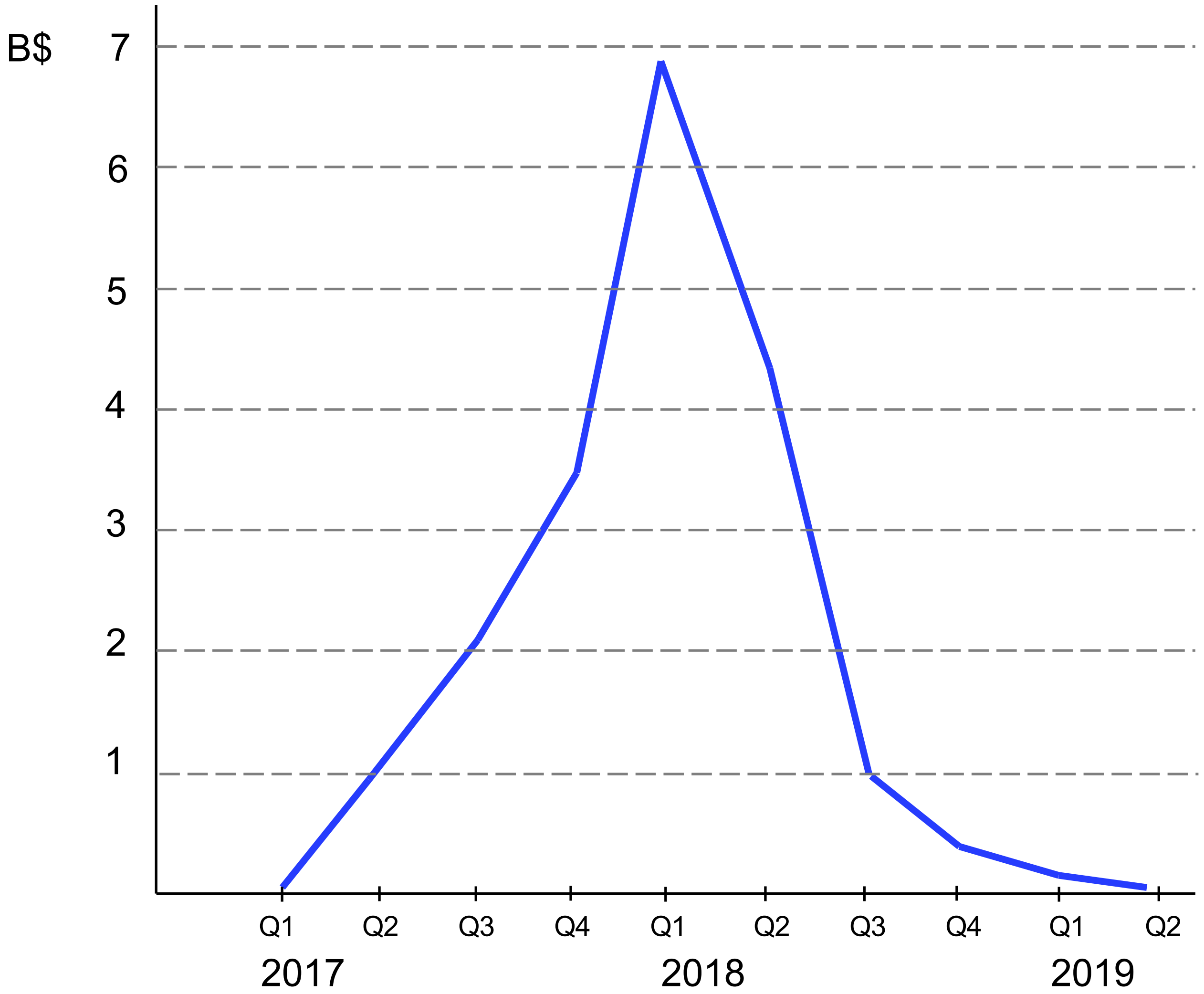
Build an app



Wikimedia Commons

← **Put on market the AIR token to get a quotation**

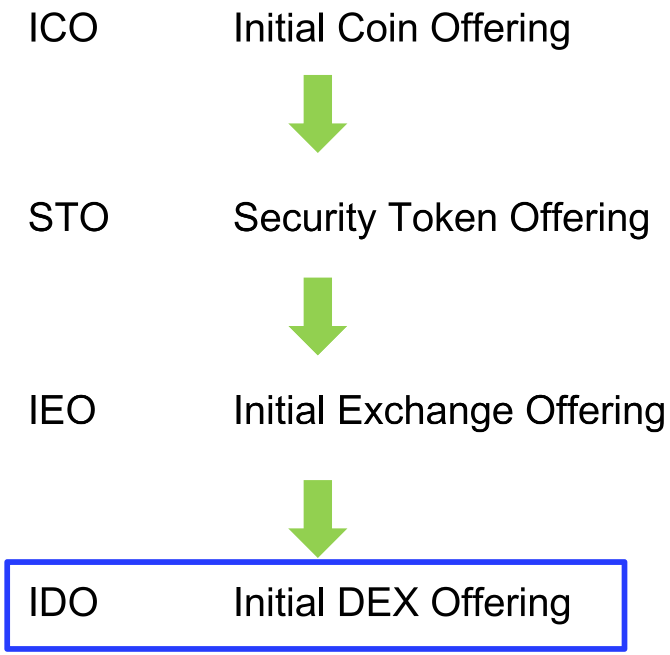
thefinalist.com



ICO raised funds

Source statista.com

Evolution of crowdfunding methods



ICO	Initial Coin Offering
STO	Security Token Offering
IEO	Initial Exchange Offering
IDO	Initial DEX Offering

BANCOR (BNT) offers a solution to the liquidity problem...

Bancor Network
Instantly convert over 120 tokens

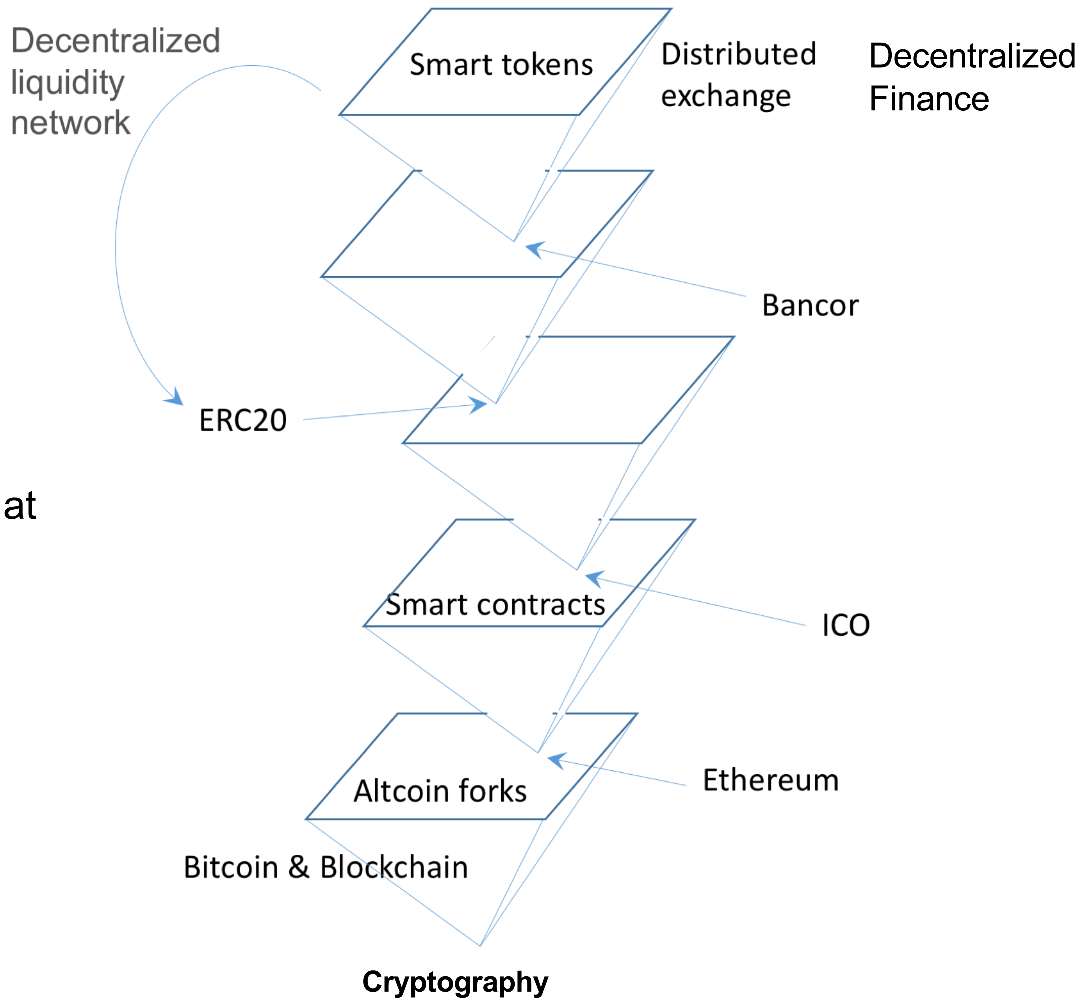
Bernard Lietaer

former Central Bank of Belgium,
one of the EURO architects

Author of three important books:

The Future of Money,
Money and Sustainability
New Money for a New World.

ICO



The genesis hierarchy of the Bancor token, aimed at improving liquidity in cryptocurrencies
with small capitalization

DeFi - *Decentralized Finance*

Objectives:

1. build an entire banking, stock exchange and financial system, h 24/7/365, decentralized, anonymous and uncensored;

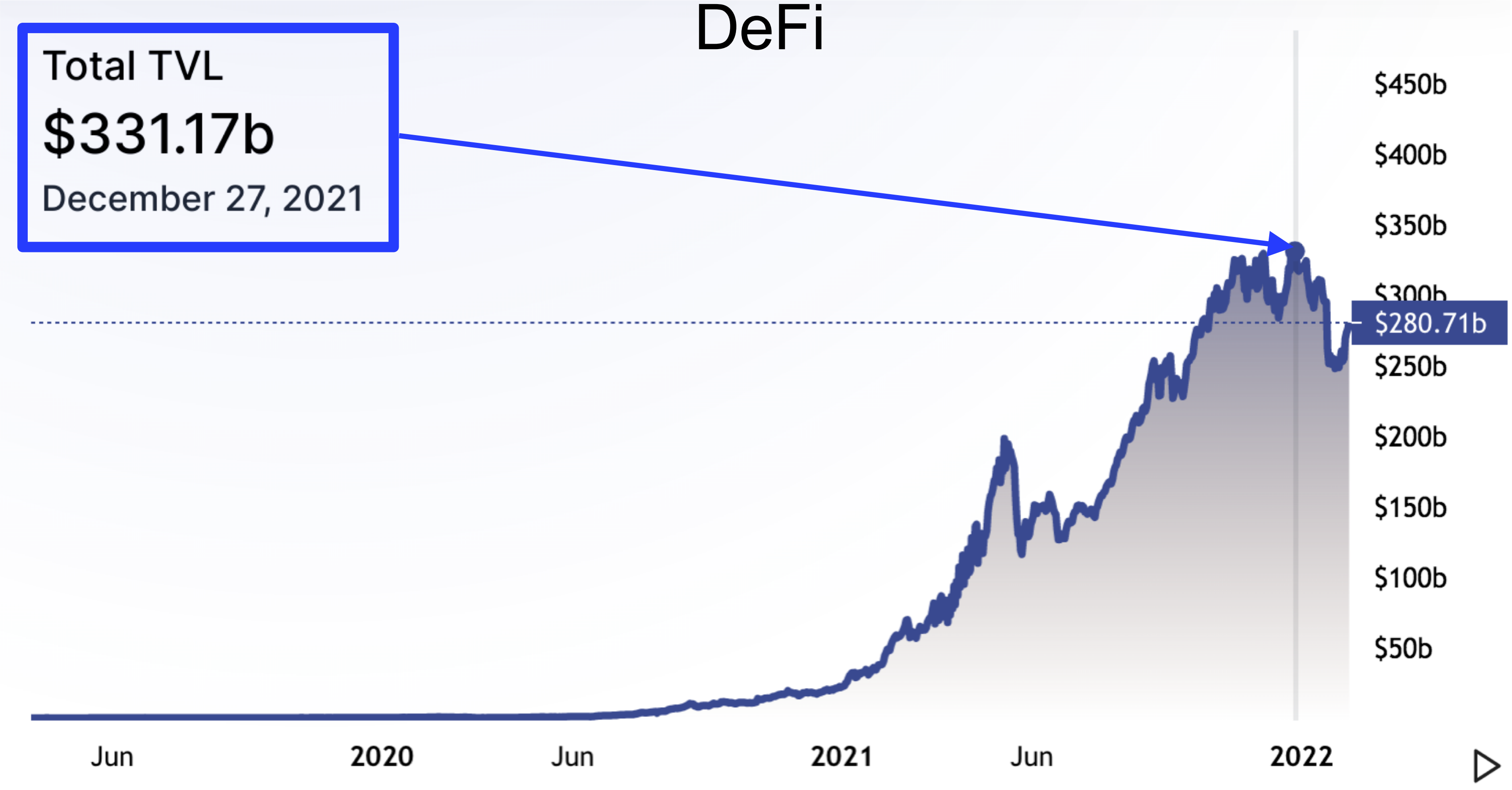
2. make this system available to people who for various reasons are excluded from banking/financial services

3. reduce banking/financial intermediation costs

DeFi - *Decentralized Finance*

Exchanges	decentralized cryptocurrency exchange
Lending	decentralized lending
Borrowing	decentralized application for loans
Staking	bond on cryptocurrencies finalized at the *Proof-of-Stake*
Liquidity Pooling	bond on couple of cryptocurrencies finalized to support DEX liquidity
Stablecoins	cryptocurrency pegged to the value of FIAT currencies ($, GBP, Yen, Yuan,...)
Asset sintetici	cryptocurrency pegged to the value of commodities (gold, silver, oil,...)

DeFi

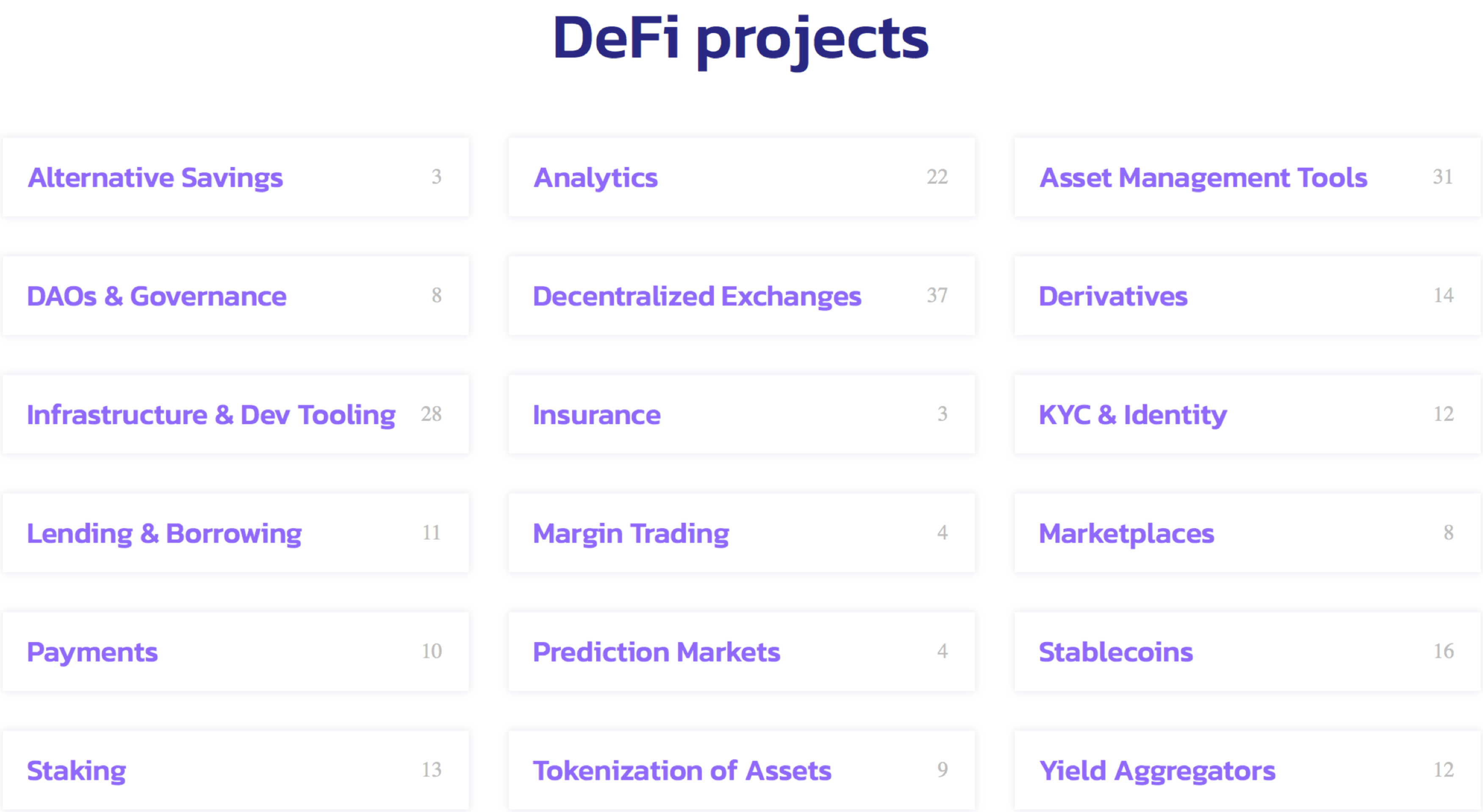


Total TVL

$331.17b

December 27, 2021

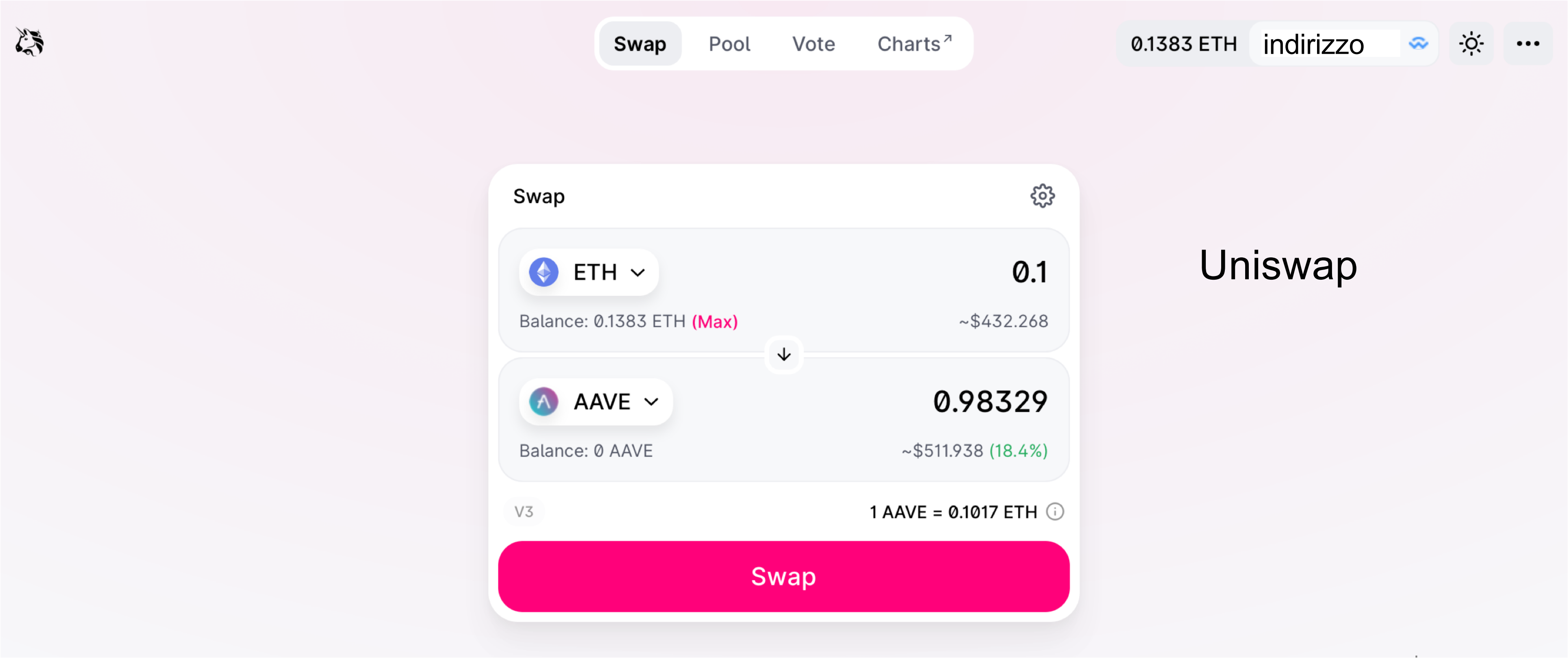
source
defillama.com/



DeFi projects

Alternative Savings	3	Analytics	22	Asset Management Tools	31
DAOs & Governance	8	Decentralized Exchanges	37	Derivatives	14
Infrastructure & Dev Tooling	28	Insurance	3	KYC & Identity	12
Lending & Borrowing	11	Margin Trading	4	Marketplaces	8
Payments	10	Prediction Markets	4	Stablecoins	16
Staking	13	Tokenization of Assets	9	Yield Aggregators	12

Decentralyzed EXchange - DEX



Swap

ETH 0.1

Balance: 0.1383 ETH (Max) ~$432.268

AAVE 0.98329

Balance: 0 AAVE ~$511.938 (18.4%)

V3 1 AAVE = 0.1017 ETH

Uniswap

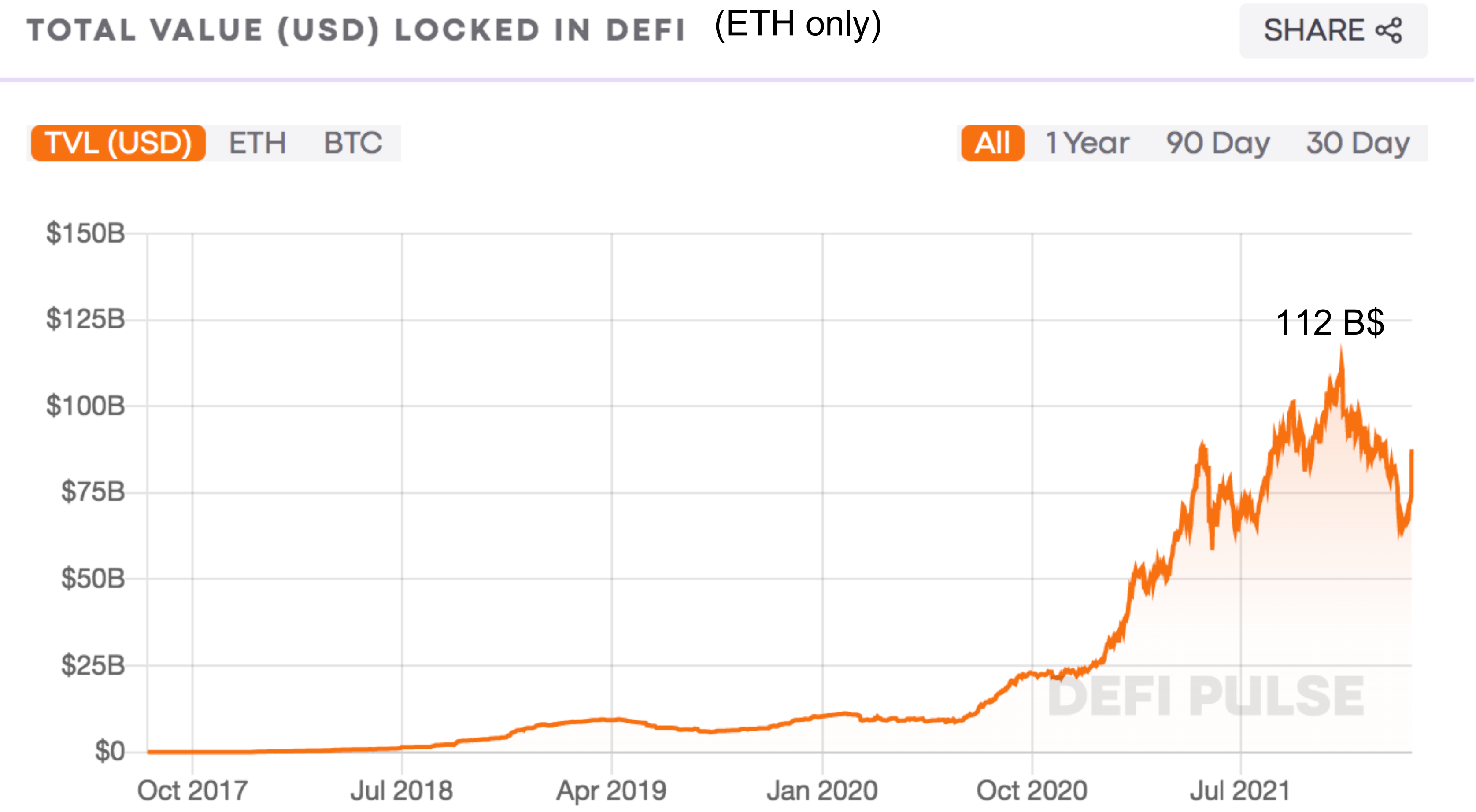
uniswap.org

Examples of DeFi projects

Decentralized derivatives	*Synthetics* *Mirror*	decentralized creation and marketing of synthetic derivatives linked to real world assets
Decentralized infrastructures	*Band* *Chainlink*	they acquire data from the real world (oracles) and transmit them on the various blockchains which support platform for smart-contracts
	0x	allows to market assets of various kinds on the Ethereum blockchain, including NFT

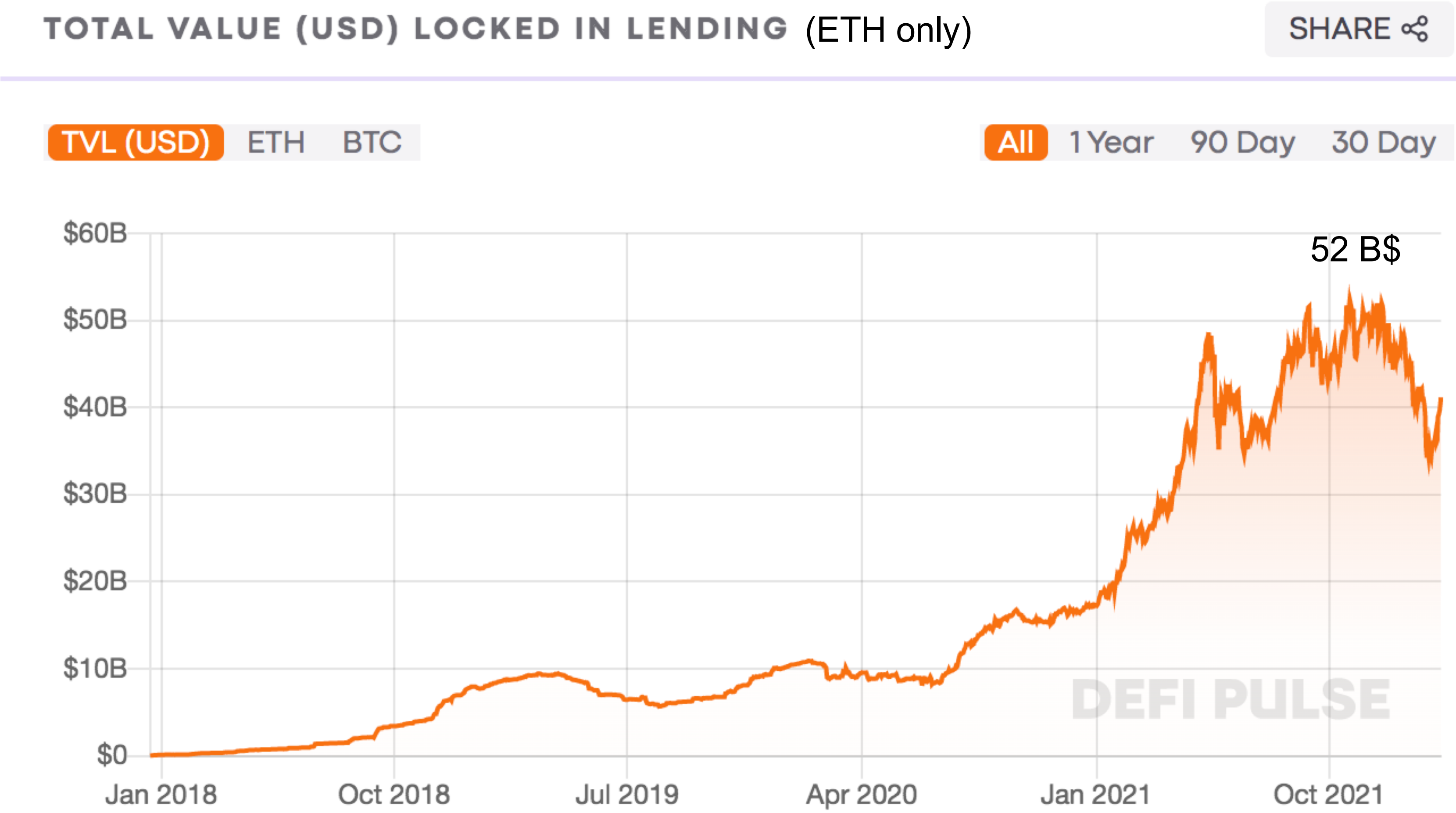
DAO (*Decentralized Autonomous Organizations*)	*Aragon*	platform to manage decentralyzed organizations
Prediction market	*Augur*	platform to manage bets on future events of any kind (value of a certain action in the future, who will win the next elections, what will the weather be like in a month, etc.)
Metaverso	*Decentraland*	platform for creating a virtual world, where you can buy land, goods, services, obtaining remuneration from interaction with other users.

DEX & Liquidity (Decentralized Exchanges)	*Uniswap* *Bancor* *Ren*	allow for decentralized exchanges, or the interoperability of cryptocurrencies *on different* blockchains
Marketplace	*District 0x*	allows you to launch your own decentralized platform governed by a DAO
Borrowing & Lending	*Aave* *Maker* *Compound*	acquisition and granting of credit



TOTAL VALUE (USD) LOCKED IN DEFI (ETH only)

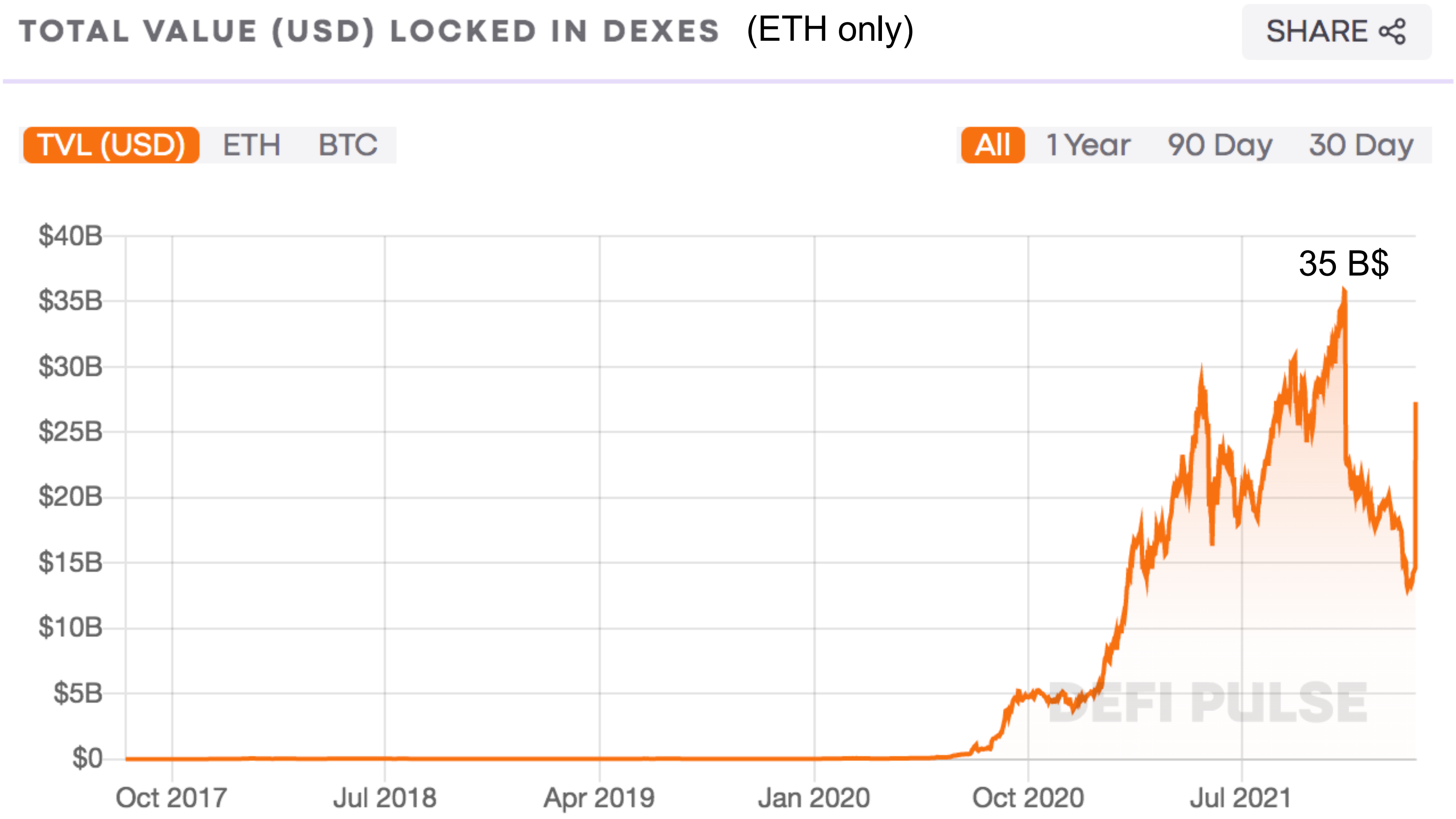
source
defipulse.com



TOTAL VALUE (USD) LOCKED IN LENDING (ETH only)

52 B$

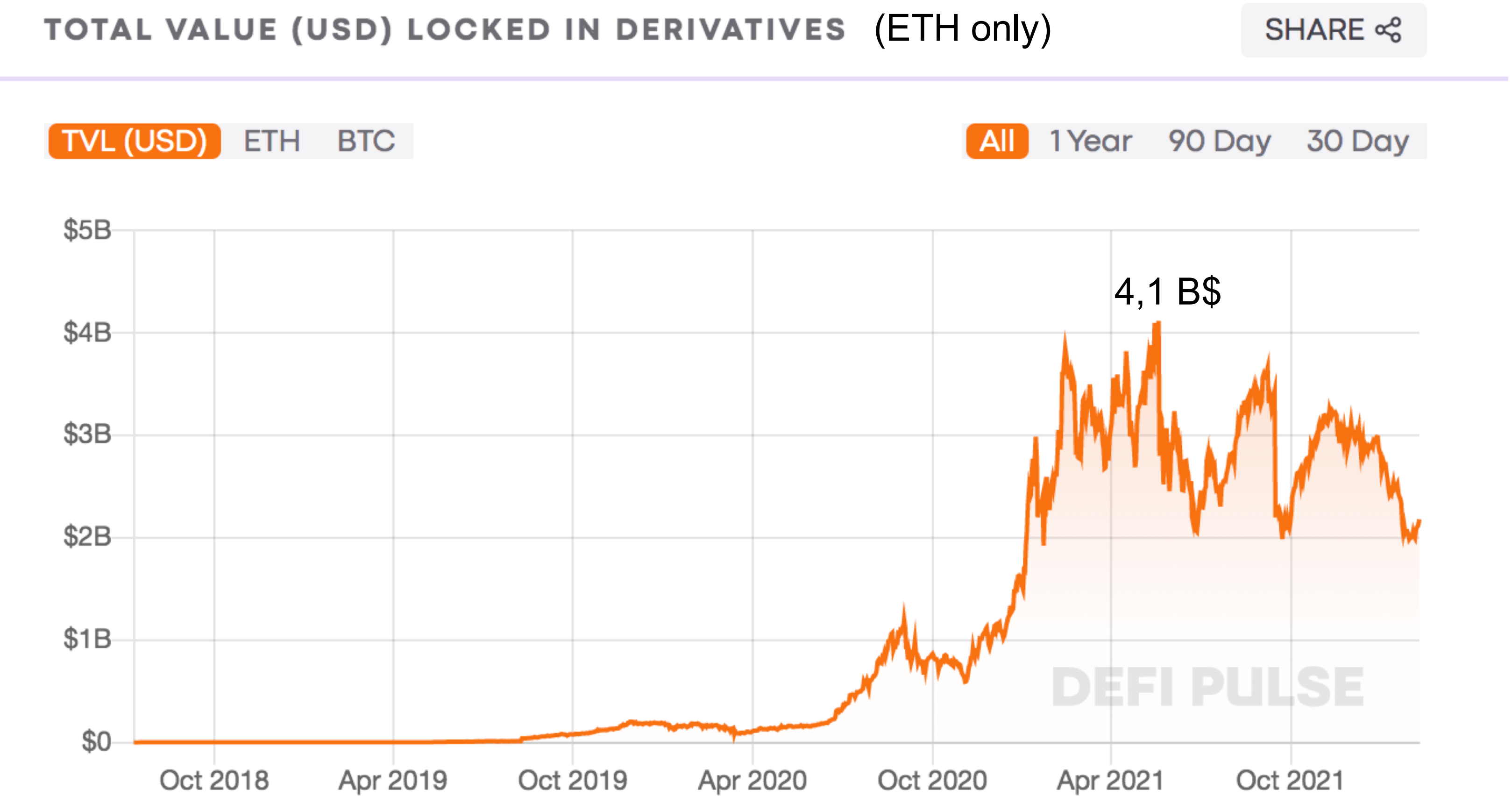
source
defipulse.com



TOTAL VALUE (USD) LOCKED IN DEXES (ETH only)

35 B$

source
defipulse.com

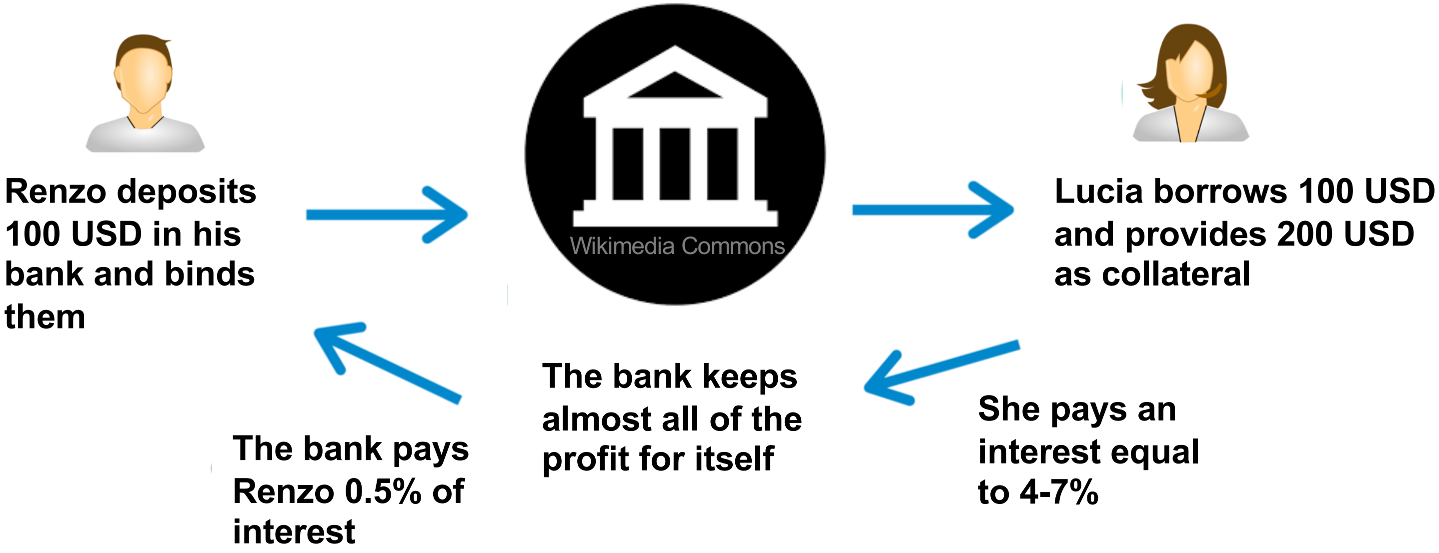


TOTAL VALUE (USD) LOCKED IN DERIVATIVES (ETH only)

4,1 B$

source
defipulse.com

Granting of a credit line in the traditional banking system



Renzo deposits 100 USD in his bank and binds them

Wikimedia Commons

Lucia borrows 100 USD and provides 200 USD as collateral

The bank pays Renzo 0.5% of interest

The bank keeps almost all of the profit for itself

She pays an interest equal to 4-7%

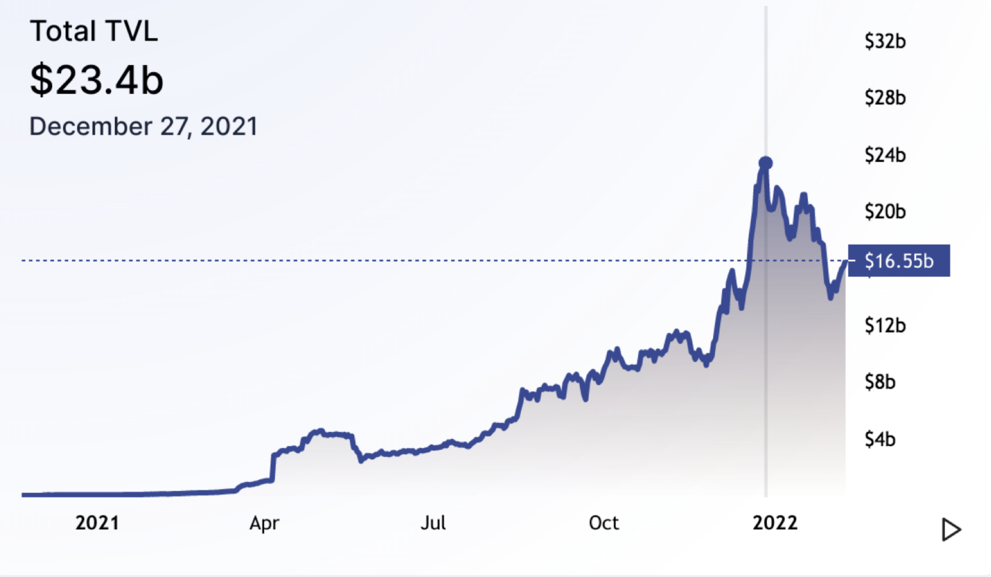
In DeFi there are two big innovations to increase liquidity:

1. by binding a cryptocurrency **XYZ**, one obtains in exchange another cryptocurrency, **nXYZ**, which is in turn negotiable

2. you get a return even when you ask for a loan that offsets, in part or in whole, the interest rate you pay

A DeFi case study: the TERRA (Luna) ecosystem

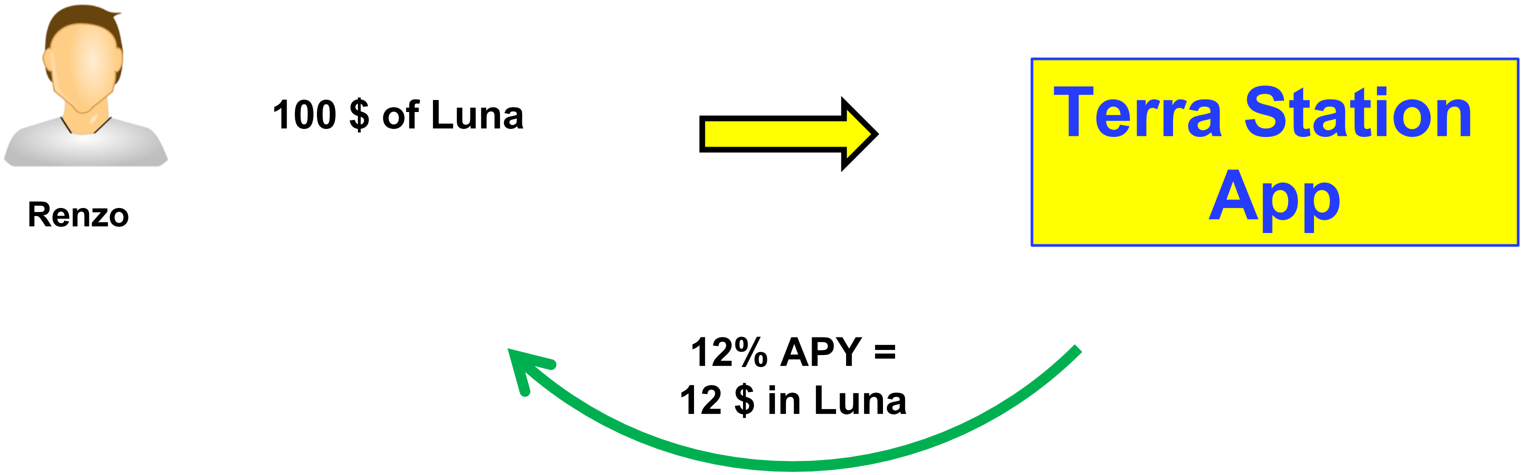
Luna	MarketCap	23 B$
UST (TerraUSD) (stablecoin)	MarketCap	11,2 B$



source
defillama.com/

Action n. 1 – Staking *Luna* on *Terra Station* App

aimed to support the functioning of the network



Renzo

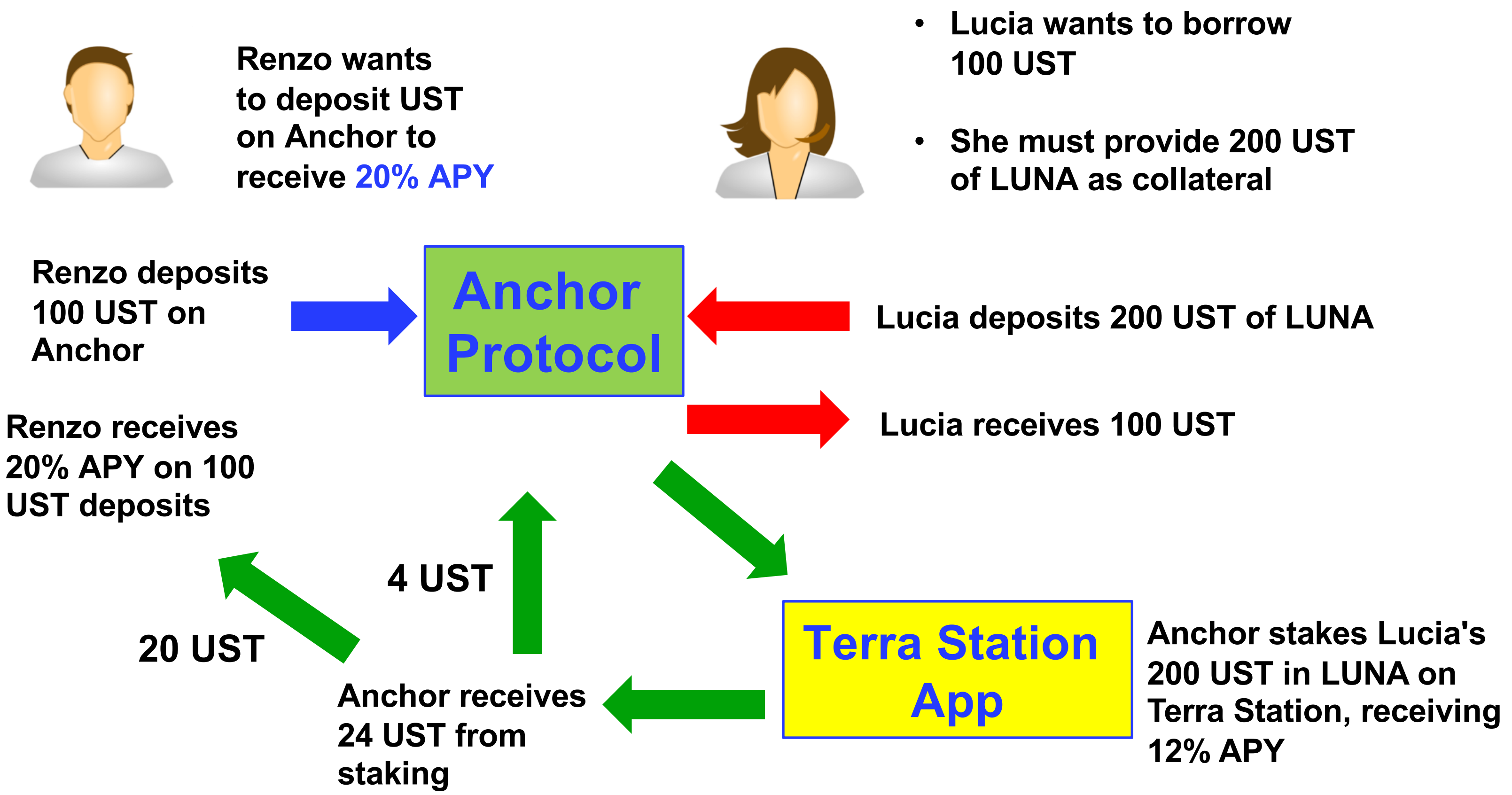
100 $ of Luna

Terra Station App

12% APY =
12 $ in Luna

Anyone who is staking Luna on the Terra Station platform receives 12% APY in Luna

Action n. 2 - Deposit and Loan



Renzo wants to deposit UST on Anchor to receive 20% APY

- Lucia wants to borrow 100 UST
- She must provide 200 UST of LUNA as collateral

Renzo deposits 100 UST on Anchor

Anchor Protocol

Lucia deposits 200 UST of LUNA

Lucia receives 100 UST

Renzo receives 20% APY on 100 UST deposits

4 UST

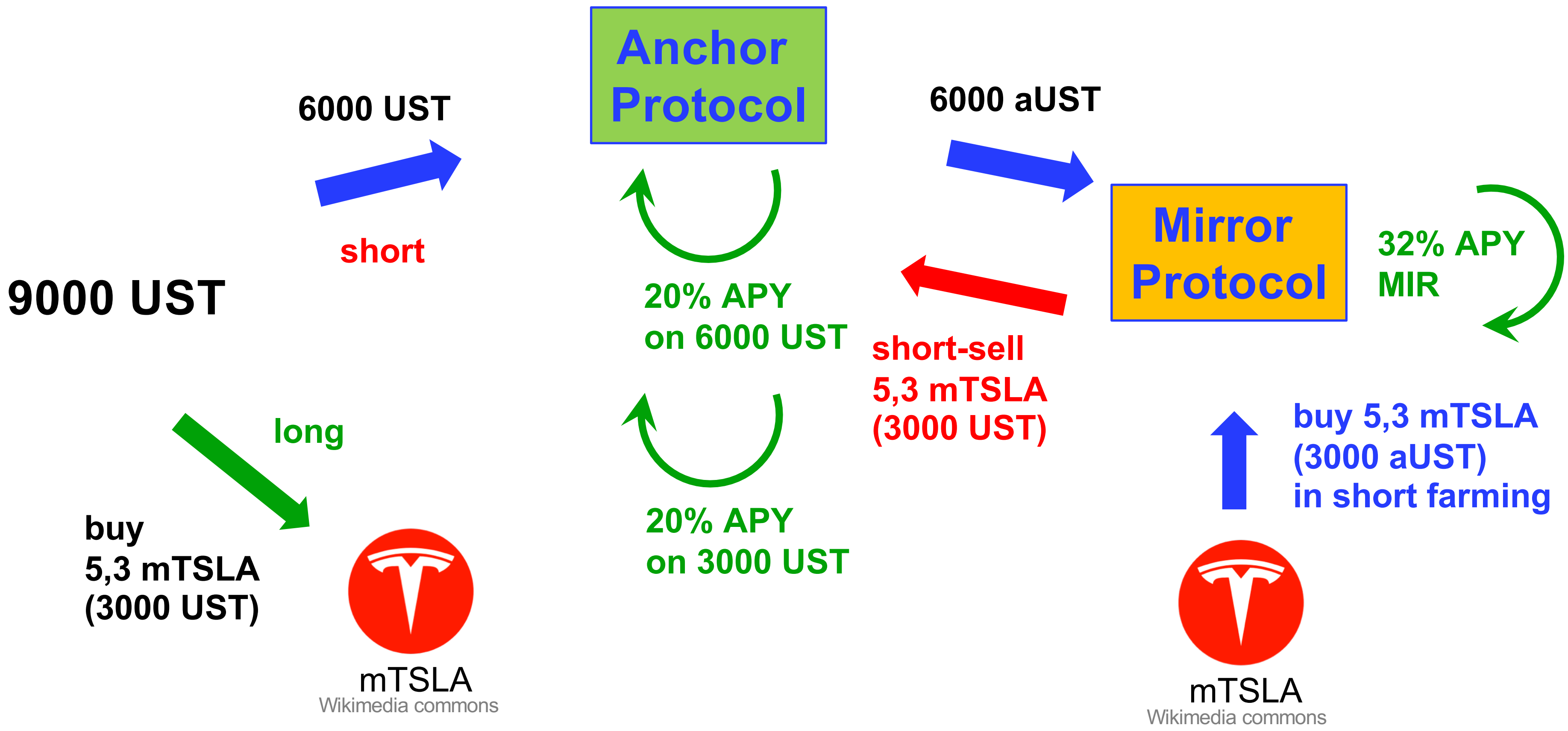
20 UST

Terra Station App

Anchor stakes Lucia's 200 UST in LUNA on Terra Station, receiving 12% APY

Anchor receives 24 UST from staking

Attività n.3 – Opening a *delta-neutral* position



9000 UST

6000 UST

short

Anchor Protocol

20% APY
on 6000 UST

6000 aUST

Mirror Protocol

32% APY
MIR

short-sell
5,3 mTSLA
(3000 UST)

long

buy
5,3 mTSLA
(3000 UST)

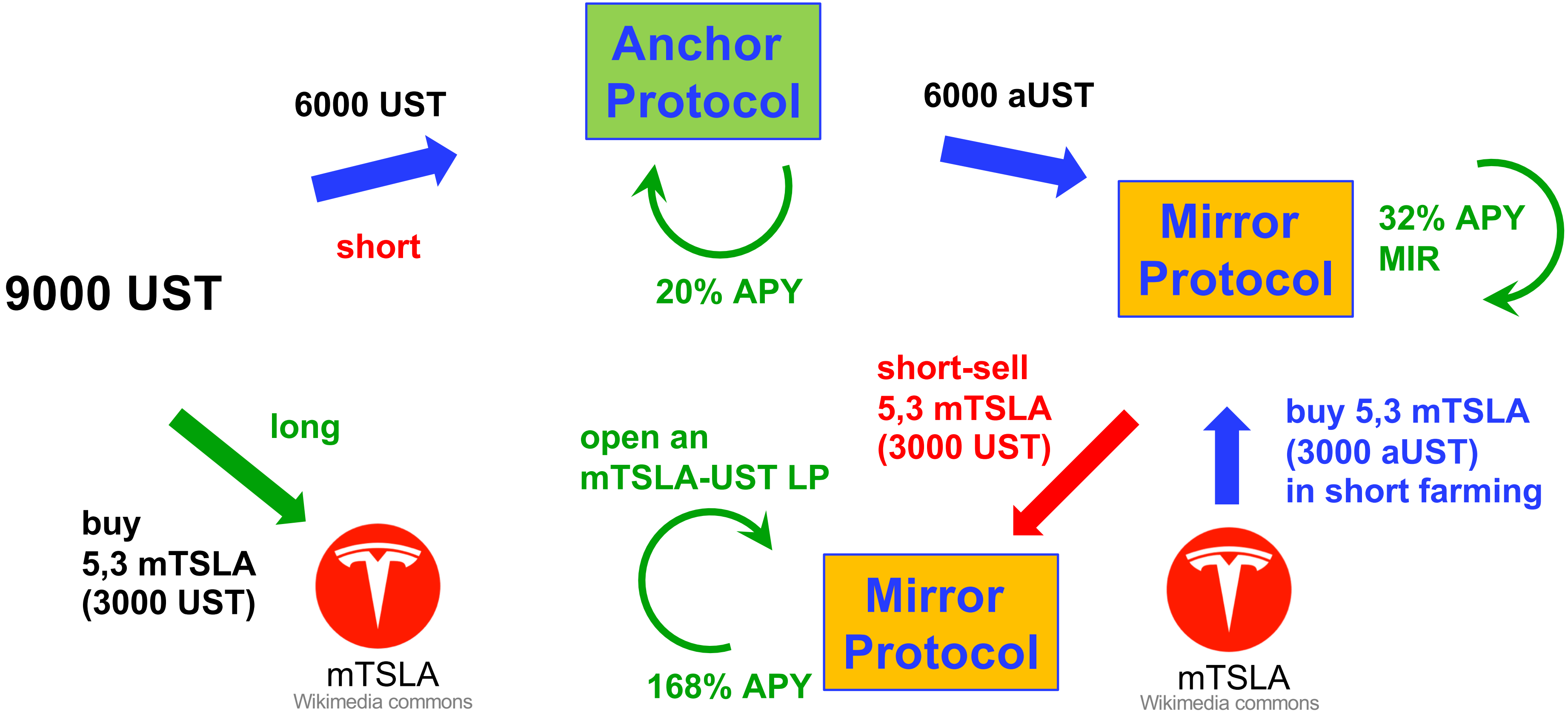
mTSLA
Wikimedia commons

20% APY
on 3000 UST

buy 5,3 mTSLA
(3000 aUST)
in short farming

mTSLA
Wikimedia commons

Attività n.3 – Apertura posizione *delta-neutral LP*



9000 UST

6000 UST

short

Anchor Protocol

20% APY

6000 aUST

Mirror Protocol

32% APY
MIR

long

buy
5,3 mTSLA
(3000 UST)

mTSLA
Wikimedia commons

open an
mTSLA-UST LP

168% APY

short-sell
5,3 mTSLA
(3000 UST)

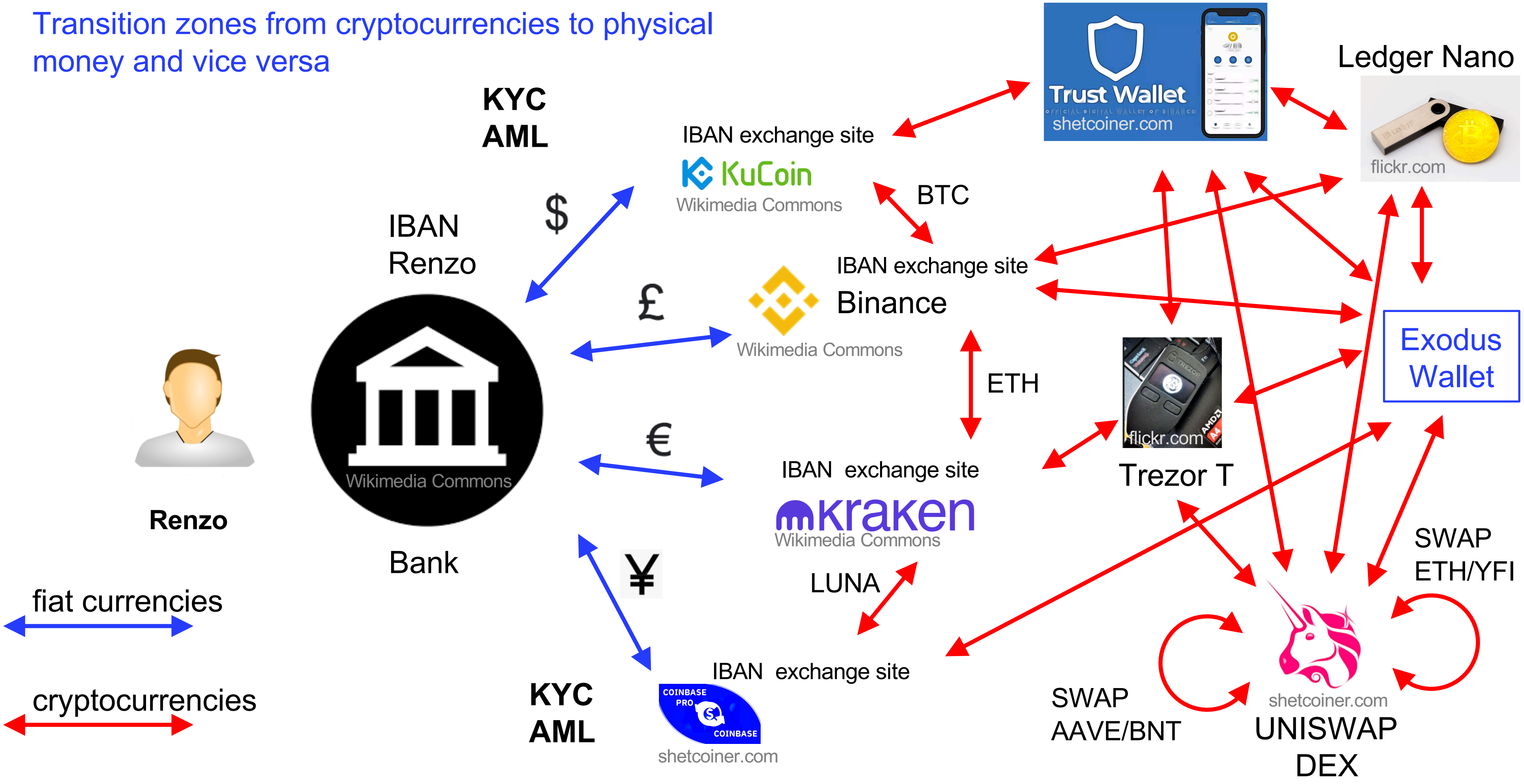
Mirror Protocol

buy 5,3 mTSLA
(3000 aUST)
in short farming

mTSLA
Wikimedia commons

De Fi

Transition zones from cryptocurrencies to physical money and vice versa



KYC
AML

IBAN exchange site
KuCoin
Wikimedia Commons

$

IBAN
Renzo

BTC

IBAN exchange site
Binance
Wikimedia Commons

£

Trust Wallet
shetcoiner.com

Ledger Nano
flickr.com

Exodus Wallet

Renzo

Wikimedia Commons

Bank

€

ETH

IBAN exchange site
kraken
Wikimedia Commons

flickr.com
Trezor T

¥

LUNA

SWAP
ETH/YFI

SWAP
AAVE/BNT

shetcoiner.com
UNISWAP
DEX

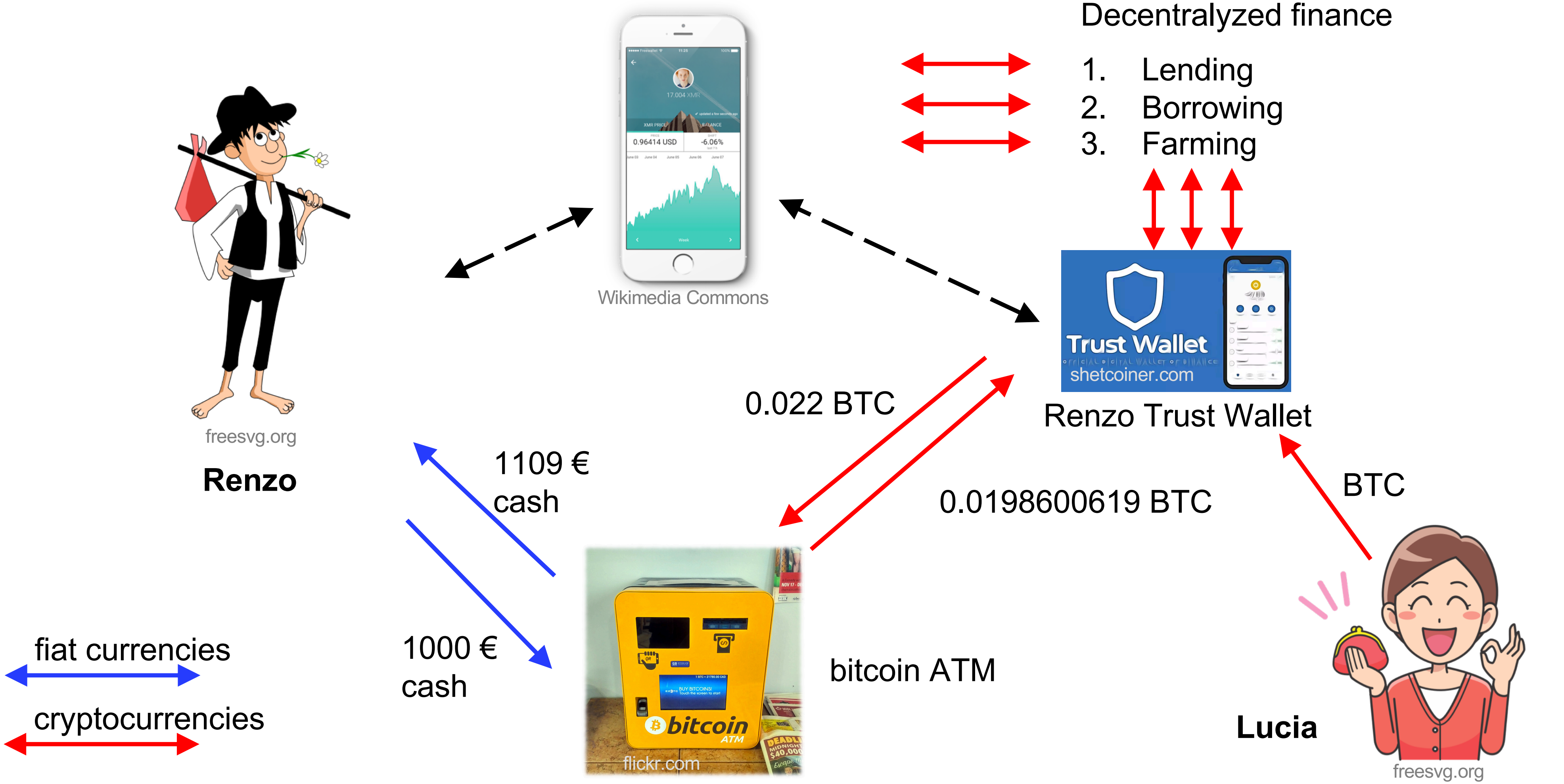
IBAN exchange site
COINBASE PRO
COINBASE
shetcoiner.com

KYC
AML

fiat currencies

cryptocurrencies

De Fi



Decentralyzed finance

1. Lending
2. Borrowing
3. Farming

Wikimedia Commons

Renzo Trust Wallet

0.022 BTC

0.0198600619 BTC

BTC

1109 € cash

1000 € cash

bitcoin ATM

flickr.com

freesvg.org

Renzo

freesvg.org

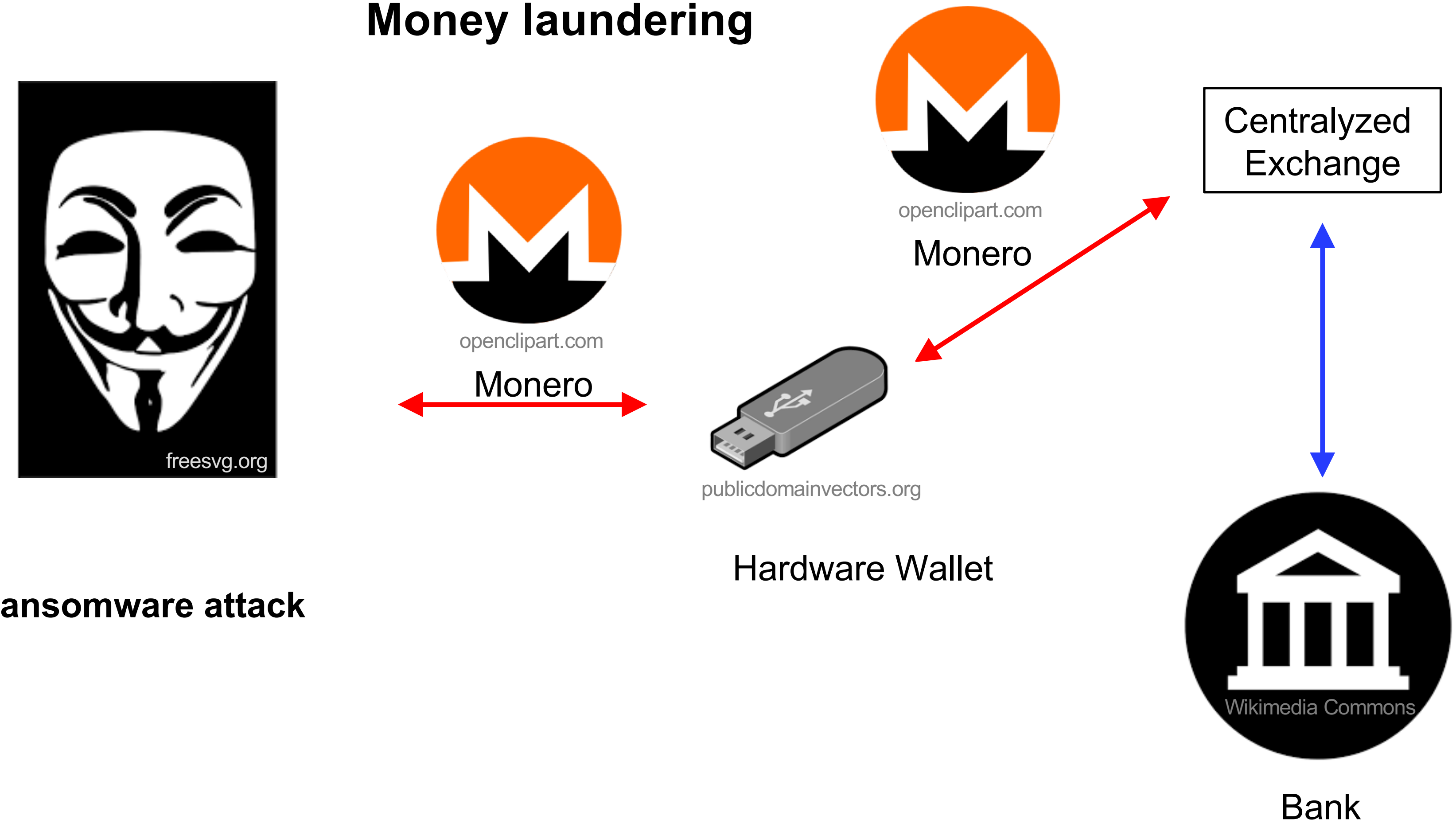
Lucia

fiat currencies

cryptocurrencies

De Fi

Money laundering



freesvg.org

Ransomware attack

openclipart.com

Monero

publicdomainvectors.org

Hardware Wallet

openclipart.com

Monero

Centralyzed Exchange

Wikimedia Commons

Bank

NFT - Non Fungible Tokens

Fungible and non fungible

flickr.com

=

flickr.com

Wikimedia Commons

??

Wikimedia Commons

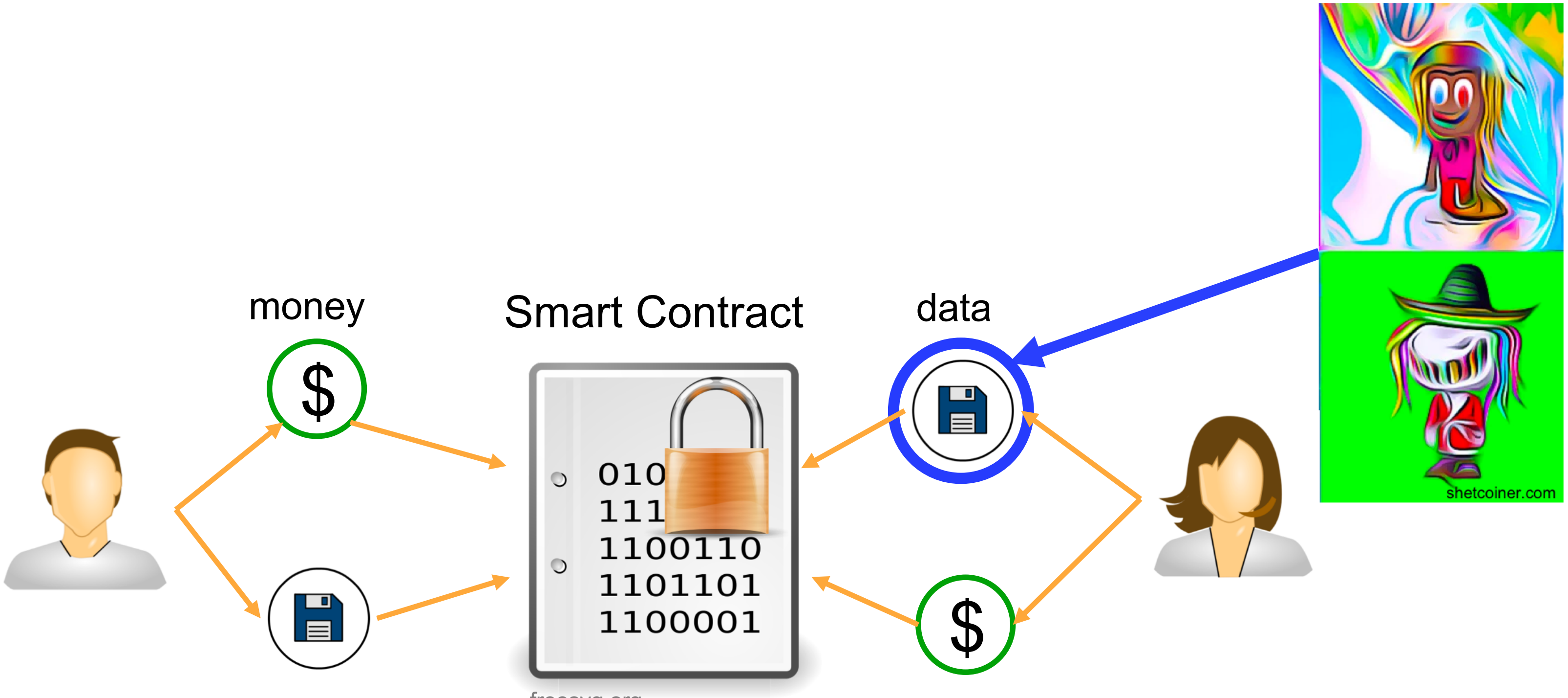
Beeple NFT picture sold for record-setting $69.3M at Christie’s Auction

Cryptopunks Sold for 16,9 m$ on Cristie’s

but also

NFT technology to protect copyrights in a decentralized way

NFT



freesvg.org

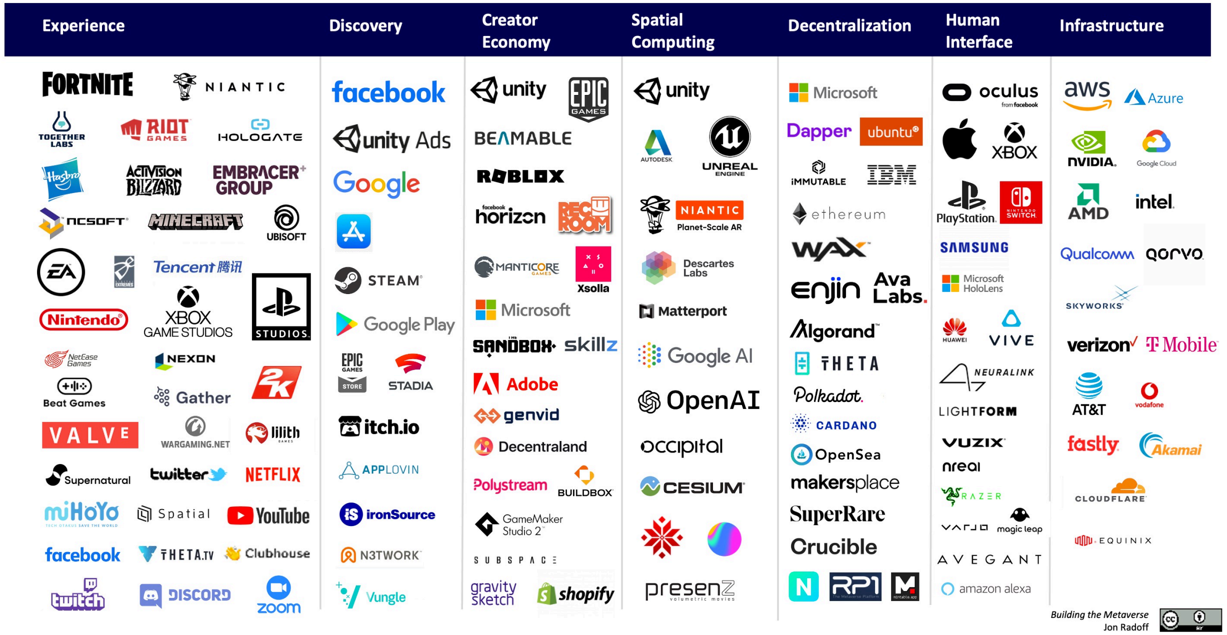
shetcoiner.com

Metaverse

Market Cap
$28,336,435,598
▾ 3.91%

source
coinmarketcap.com

Metaverse Market Map



Wikimedia Commons

A look into the future: Web 3.0 or the blockchain of blockchains?

Wikimedia Commons

Relay chain:
coordinates consensus and transactions among the various blockchains

Parachain:
autonomous constitutive blockchains, which manage their own transactions

Bridges:
connection bridges with external blockchains such as Ethereum

The adoption of cryptocurrencies now appears institutionalized

Pay Pal allows you to make payments using the main cryptocurrencies

ebay is considering doing the same

JP Morgan Chase will offer Bitcoin-based funds

Goldman Sachs has added trading on ETFs and BTC-based futures

Tesla own 42 kBTC (2,4 B$) as a strategic asset

Microstrategy own 125051 BTC (5,5 B$) as a strategic asset

Grayscale Investment own 654885 BTC (28,8 B$) as a strategic asset

Facebook-Meta wants to create Diem, its own cryptocurrency

Towards a *tokenization* of economy?

spacecoastdaily.com

So people talking about tokenization and having a token for everything is returning to the Stone Age. Even the Flinstones had a more sophisticated financial system than crypto. They [had] shell dollars and they were using them to avoid the barter, while you guys want to go back to the barter.
Nouriel Roubini
Professor of economics, New York University

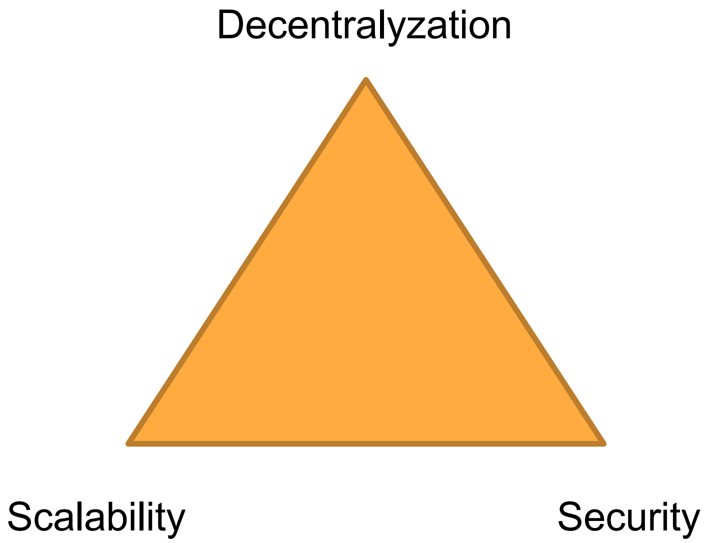
Bitcoin is an excellent idea. It fulfills the needs of the complex system, not because it is a cryptocurrency, but precisely because it has no owner, no authority that can decide on its fate. It is owned by the crowd, its users. And it has now a track record of several years, enough for it to be an animal in its own right.
Nassim Nicholas Taleb
Professor at the Tandon School of Engineering,
New York University

In summary, main characteristics are:

Censorship-resistance	outside the control of central banks, national and international institutions and governing bodies
Tamper-resistance	tampering and alteration resistant
Permissionless	they do not require the presence of a guarantor and guarantee free access to anyone

Problems and threaten of the cryptocurrency world

The Blockchain Trilemma



Problems and threaten of the cryptocurrency world

1) **value coupled** with a technology
2) trilemma of the blockchain
3) volatility of digital currencies
4) cryptocurrency regulation
5) hard forks
6) custody services for institutional investors
7) **scams, hacking and theft from** wallets and exchanges
8) **Halting problem and Rice theorem!!**
9) ...

Perspectives

1) cryptocurrencies as electronic cash
2) cryptocurrencies as a store of value
3) development of smart contracts (after digital mapping of the real world) within the legal system
4) **decentralized finance**
5) decentralized services
6) institutional adoption (banks, investment funds, pension funds, ...)
7) **Central Bank Digital Currencies**
8) programmability of money
9) economy tokenization

Accusations to the world of cryptocurrencies from economic and financial actors

1. they have **no intrinsic value**, as they do not have any underlying asset
2. cannot constitute a **reserve of value**, having regard to point 1.
3. they cannot be a **medium of exchange**, given the high volatility
4. they cannot be counted as a **unit of account**, due to high volatility

Accusations to the world of cryptocurrencies from the point of view their use and function

... but AML in the bank sector:
Deutsch Bank 1,3 T$
JP Morgan 514 B$
Bank of America 384 B$
...

not **AML** (*Anti Money Laundering*) money laundering

not **KYC** (*Know Your Customer*) exchange sites that do not ask for KYC

used to finance illegal activities

used for payments on the dark web

used as a means of tax evasion

used as a means of circumventing embargoes

Denigrators of cryptocurrencies

Nouriel Roubini

professor of economics,
New York University

«Crypto is the mother or father of all scams and bubbles»
Those who operate in the sector and who induce customers to buy cryptocurrencies are "cheaters, swindlers, criminals, charlatans"
«The Blockchain is the most overrated and least useful technology in human history; in practice it is nothing better than a spreadsheet or a glorified database "

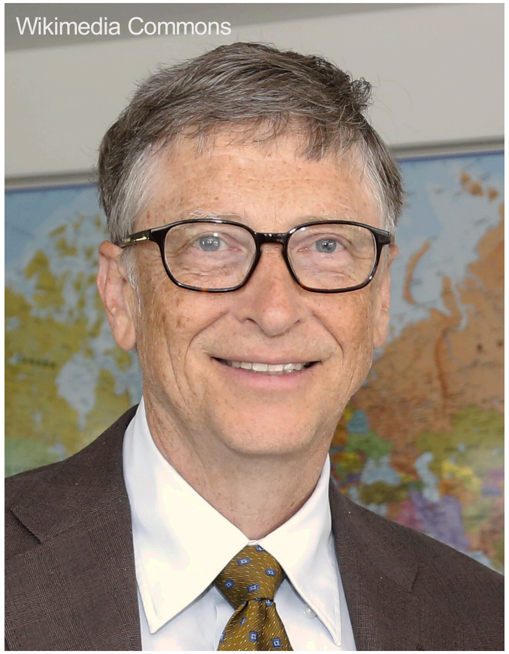
Warren Buffett

flickr.com

Warren Buffett
A Great American

American businessman and economist, one of the richest men in the world

«Bitcoin is rat poison squared»



Bill Gates

Founder of Microsoft

Bitcoin is one of the craziest and most speculative things

As an asset class, it's not producing anything and so you shouldn't expect it to rise in value

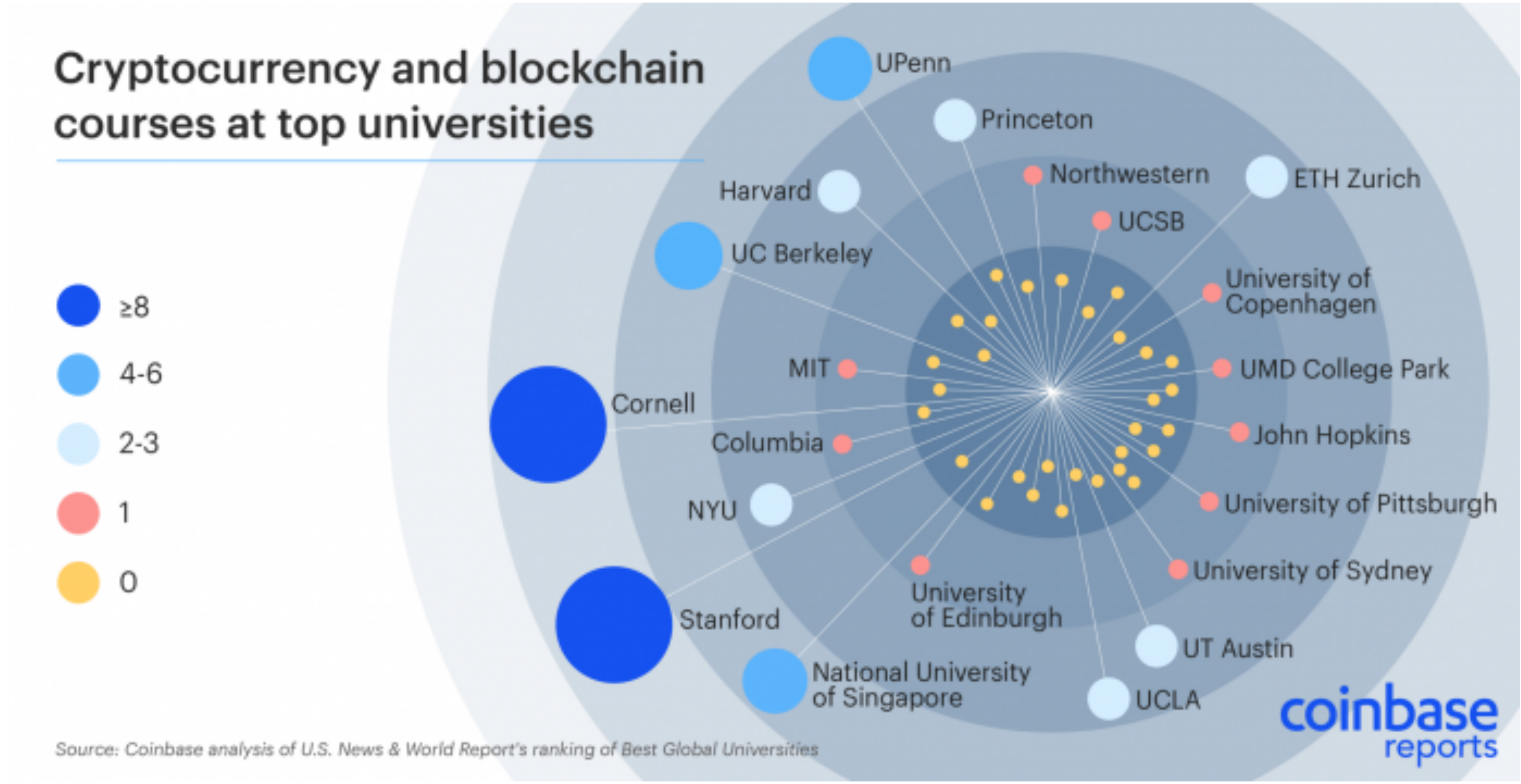
flickr.com

Bitcoin is a Ponzi Scheme, says former Israel Prime Minister *Ehud Barak* – (MD in engineering-economic systems)

Blockchain could easily become a decentralized alternative to the current centralized banking system – MIT *Sloan School of Management*, ex BCG consultant

Wikimedia Commons

Studies & Jobs

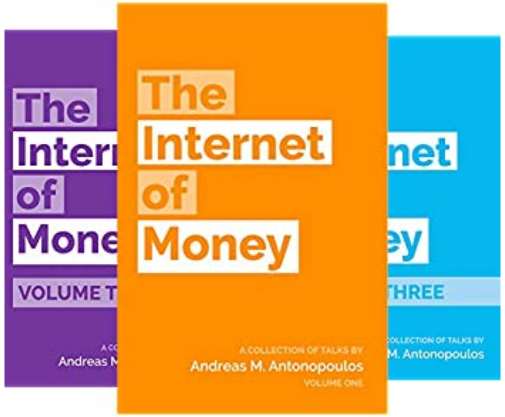


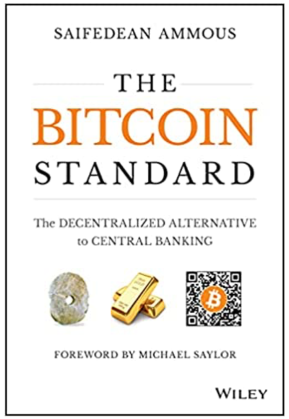
Cryptocurrency and blockchain courses at top universities

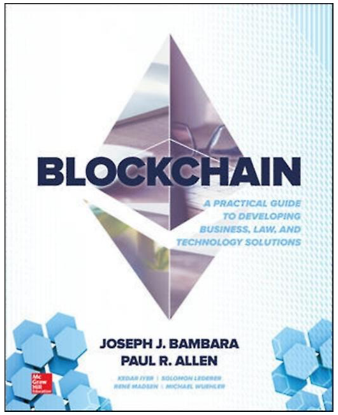
Source: Coinbase analysis of U.S. News & World Report's ranking of Best Global Universities

coinbase reports

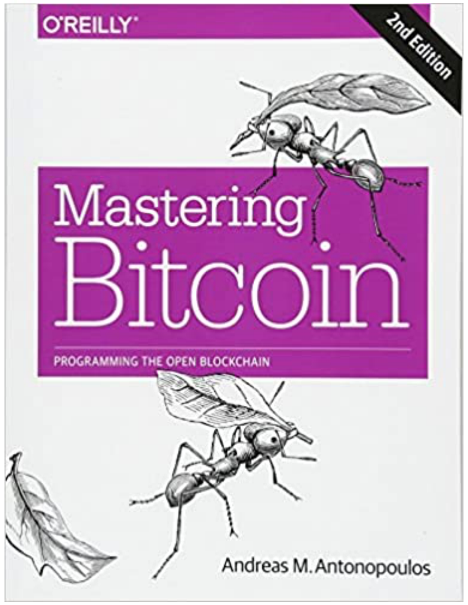
Books

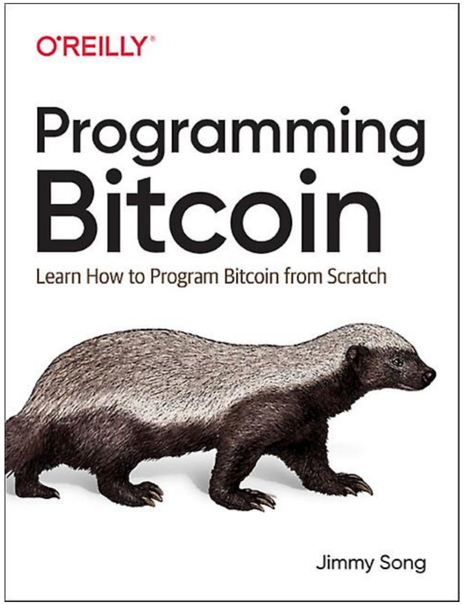



SAIFEDEAN AMMOUS
THE BITCOIN STANDARD
The DECENTRALIZED ALTERNATIVE to CENTRAL BANKING
FOREWORD BY MICHAEL SAYLOR
WILEY


BLOCKCHAIN
A PRACTICAL GUIDE TO DEVELOPING BUSINESS, LAW, AND TECHNOLOGY SOLUTIONS
JOSEPH J. BAMBARA
PAUL R. ALLEN

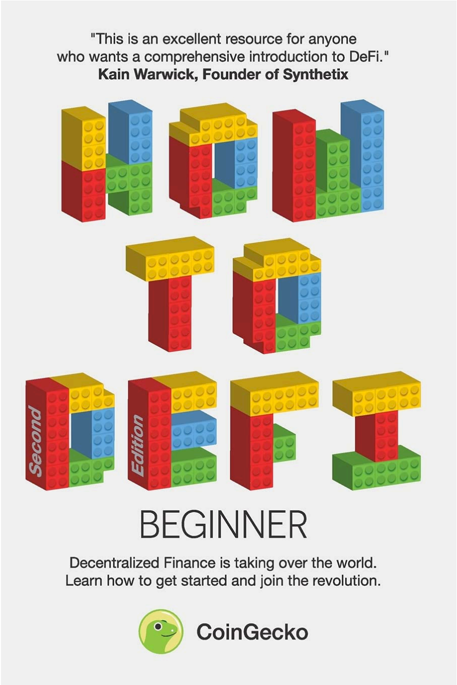
more general





more technical

DeFi

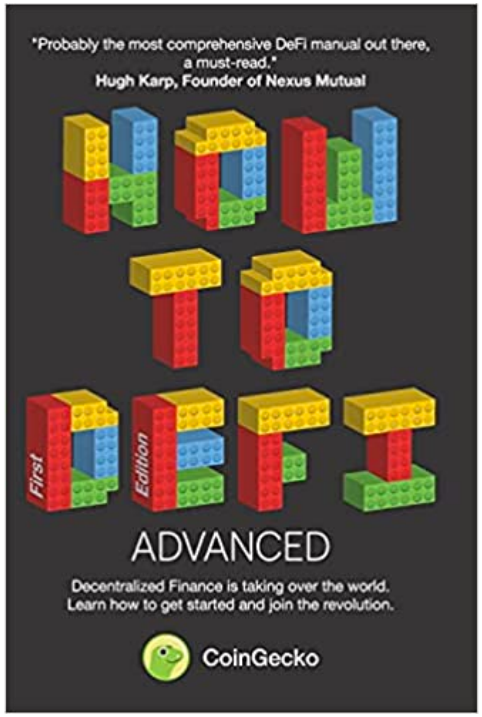


"This is an excellent resource for anyone who wants a comprehensive introduction to DeFi."
Kain Warwick, Founder of Synthetix

BEGINNER

Decentralized Finance is taking over the world.
Learn how to get started and join the revolution.

CoinGecko



"Probably the most comprehensive DeFi manual out there, a must-read."
Hugh Karp, Founder of Nexus Mutual

ADVANCED

Decentralized Finance is taking over the world.
Learn how to get started and join the revolution.

CoinGecko

In Italian

Gianluca Chiap Jacopo Ranalli Raffaele Bianchi
BLOCKCHAIN
TECNOLOGIA E APPLICAZIONI PER IL BUSINESS
Tutto ciò che serve per entrare nella nuova rivoluzione digitale
HOEPLI

UN APPROCCIO MULTIDISCIPLINARE
IL FUTURO DEL VALORE
BLOCKCHAIN, CRYPTOASSET E FINANZA DECENTRALIZZATA
SECONDA EDIZIONE
P. SORGENTONE

Operative DeFi

Crypto Gateaway

https://www.youtube.com/c/TheCryptoGatewayInvestireinCriptovaluteOfficial/videos

Crypto Ita

https://www.youtube.com/c/CryptoIta/videos