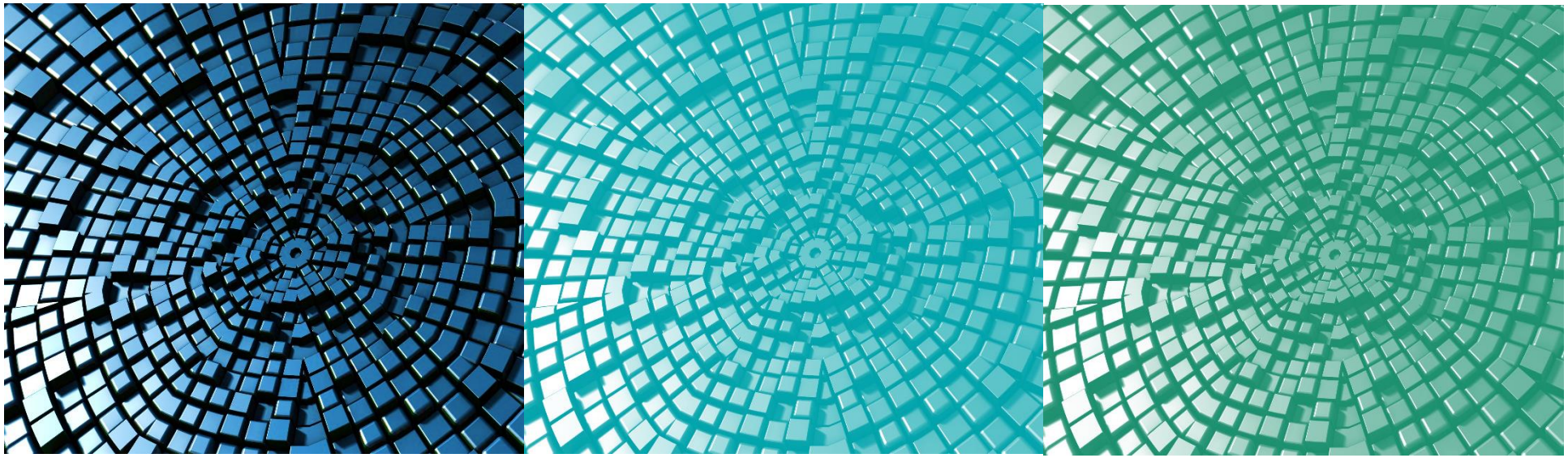
Blockchain Technology Overview

Keys, Addresses, Wallets

Lect. univ. dr. George Cirlig,
Ovidius University of Constanta



Blockchain for Entrepreneurs - a non-traditional Industry 4.0 curriculum for Higher Education - 2018-1-RO01-KA203-049510

Contents

- ✓ Blockchain and cryptography overview
- ✓ Bitcoin history and key concepts
- ✓ Cryptocurrency Wallets, Addresses, Public and Private Keys
- ✓ Practical Example: Installing a Hot Wallet
- ✓ Practical Example: Start mining in 60 seconds with NiceHash
- ✓ Practical Example: Start trading with Binance App

Why Should I Use Blockchain?

A simple analogy for understanding blockchain is a Google Document. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the document at the same time. No one is locked out awaiting changes from another party, while all modifications to the document are being recorded in real-time.

Of course, blockchain is more complicated, but the analogy illustrates three critical ideas of the technology: reduce risk, stamps out fraud and brings transparency.

The whole point of using a blockchain is to let people — in particular, people who don't trust one another — share valuable data in a secure, tamperproof way.

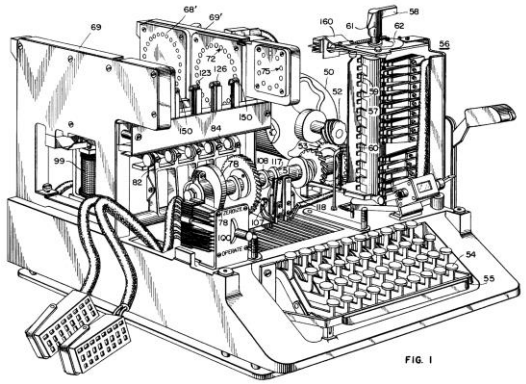
What is Blockchain?

To briefly define what the ***blockchain*** is we can say that "*a blockchain is a ledger that uses cryptography to record transactions in a tamper-evident way*".

This allows transactions between pseudo-anonymous parties without requiring a trusted intermediary.

Cryptography in the past

Ancient scytale



Military SIGABA machine

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère_square

Military Enigma machine

Modern cryptography

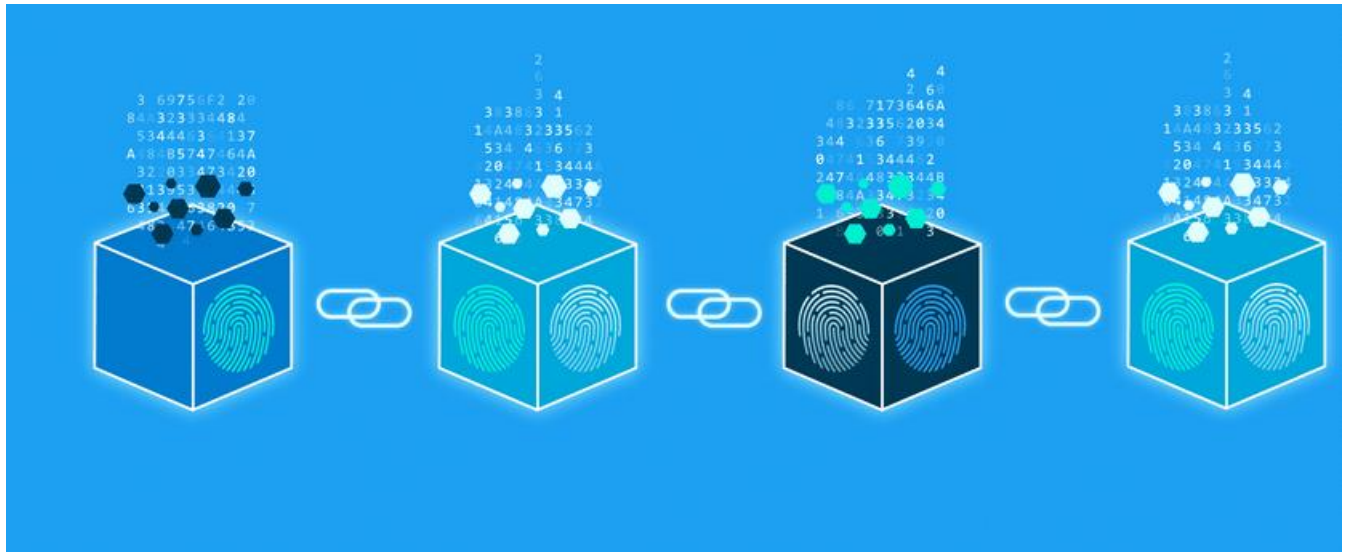
Hundreds of times a day we use cryptography in our life without even realizing it. For example, this happens when you:

- authenticated yourself by typing a password;
- remotely unlocking your car;
- withdraw cash from an ATM;
- purchased something by credit card over the Internet;
- downloaded a verified update for your operating system;

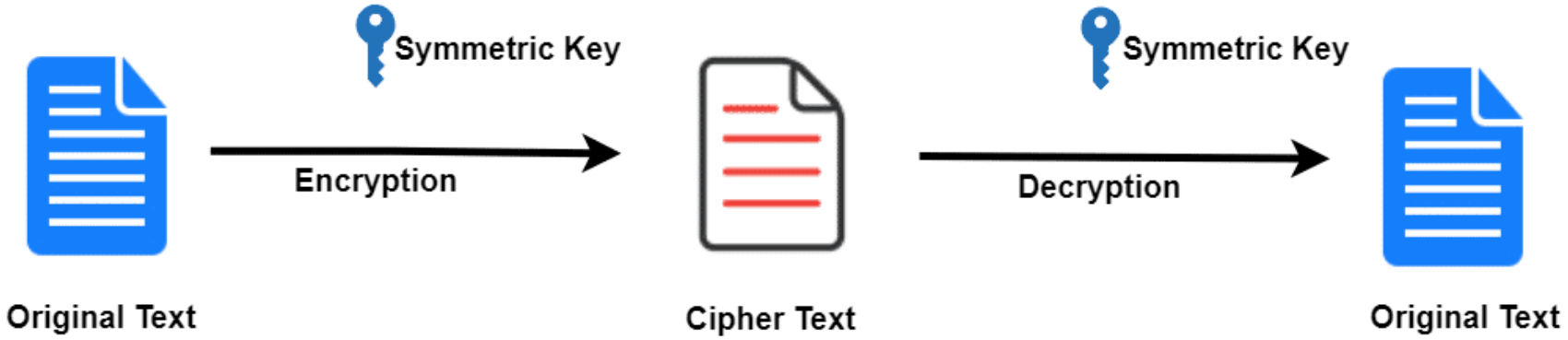
Cryptography's role in the Blockchain?

At its most basic level, the Blockchain is literally just a chain of *blocks*. Obvious not in the traditional sense of those words: *blocks* on the blockchain are made up of digital pieces of information.

Cryptography is the core of this technology, making blockchain unchanging and reliable. To achieve this, **asymmetric-key algorithms** and **hash functions** are used.

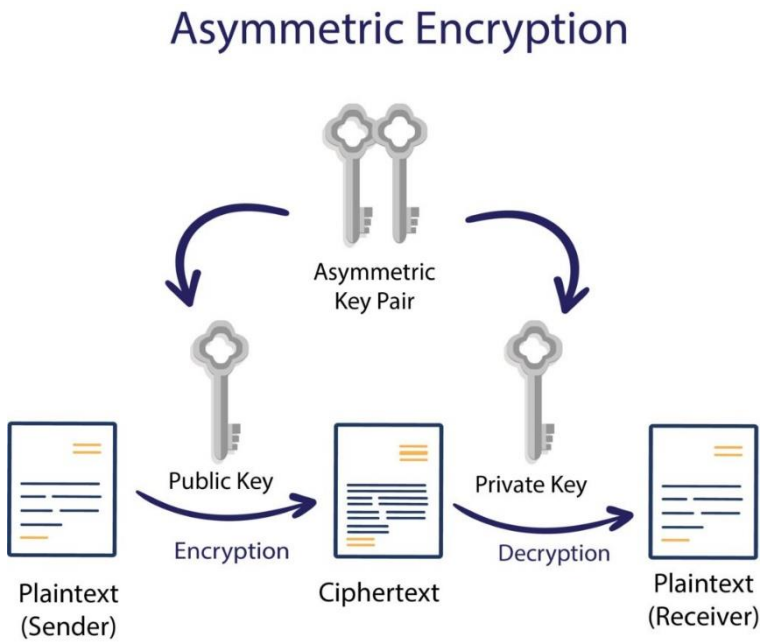


Symmetric encryption



The recipient of an encrypted message would use the same secret key to unscramble the message that the sender had used to scramble it.

Asymmetric Encryption



Bitcoin Whitepaper: 10/31/2008

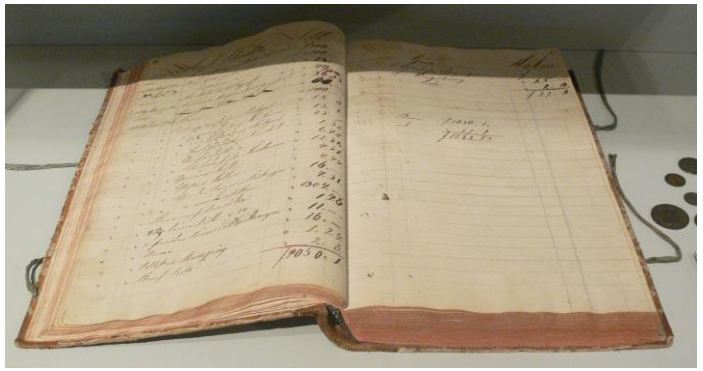
Bitcoin: A Peer-to-Peer Electronic Cash System

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

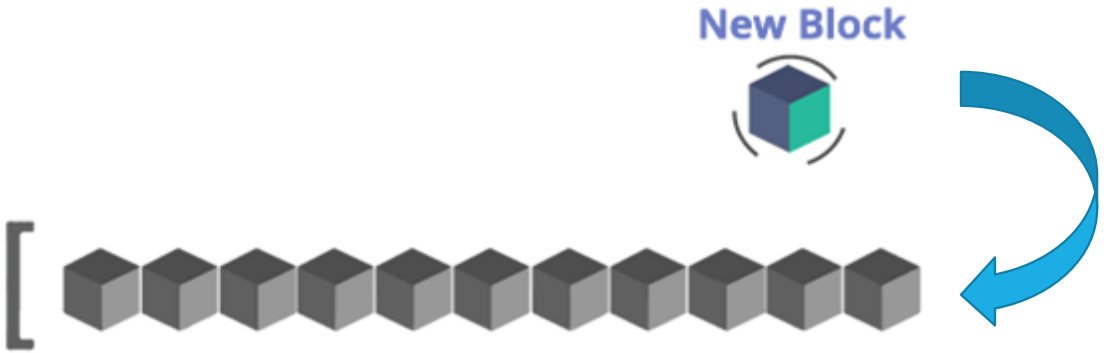
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

https://bitcoin.org/bitcoin.pdf

Classic ledger vs Blockchain ledger



A ledger from 1828



A growing list of data blocks that are linked together.

First conclusion:

Blockchain ≠ Bitcoin

Is the underlying data structure, which can be used for many things, including cryptocurrencies.

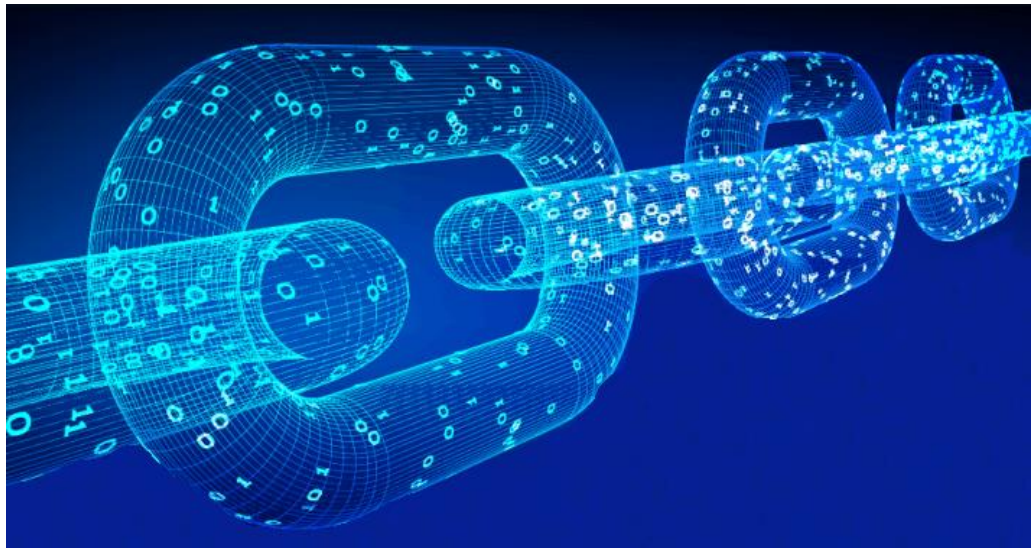
Is a virtual and decentralized currency that use the blockchain technology in order to transmit value among traders, without a third-party authority.

Nakamoto key concept: BLOCKS

Blocks – store information about transactions (date, time, sum, etc.);

Blocks store information about who is participating in transactions, but purchase is recorded without any identifying information using a unique *digital signature*.

Blocks store information that distinguishes them from other blocks.



Nakamoto key concept: MINERS

Miners - create new blocks on the chain through a process called mining.

Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash.

When a block is successfully mined, the change is accepted by all the nodes on the network and the miner is rewarded financially.

Source: Bitcoin.com

Nakamoto key concept: NODES

Nodes - one of the most important concepts in blockchain technology is decentralization. No one computer can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain;

Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning. Every node has its own copy of the blockchain;

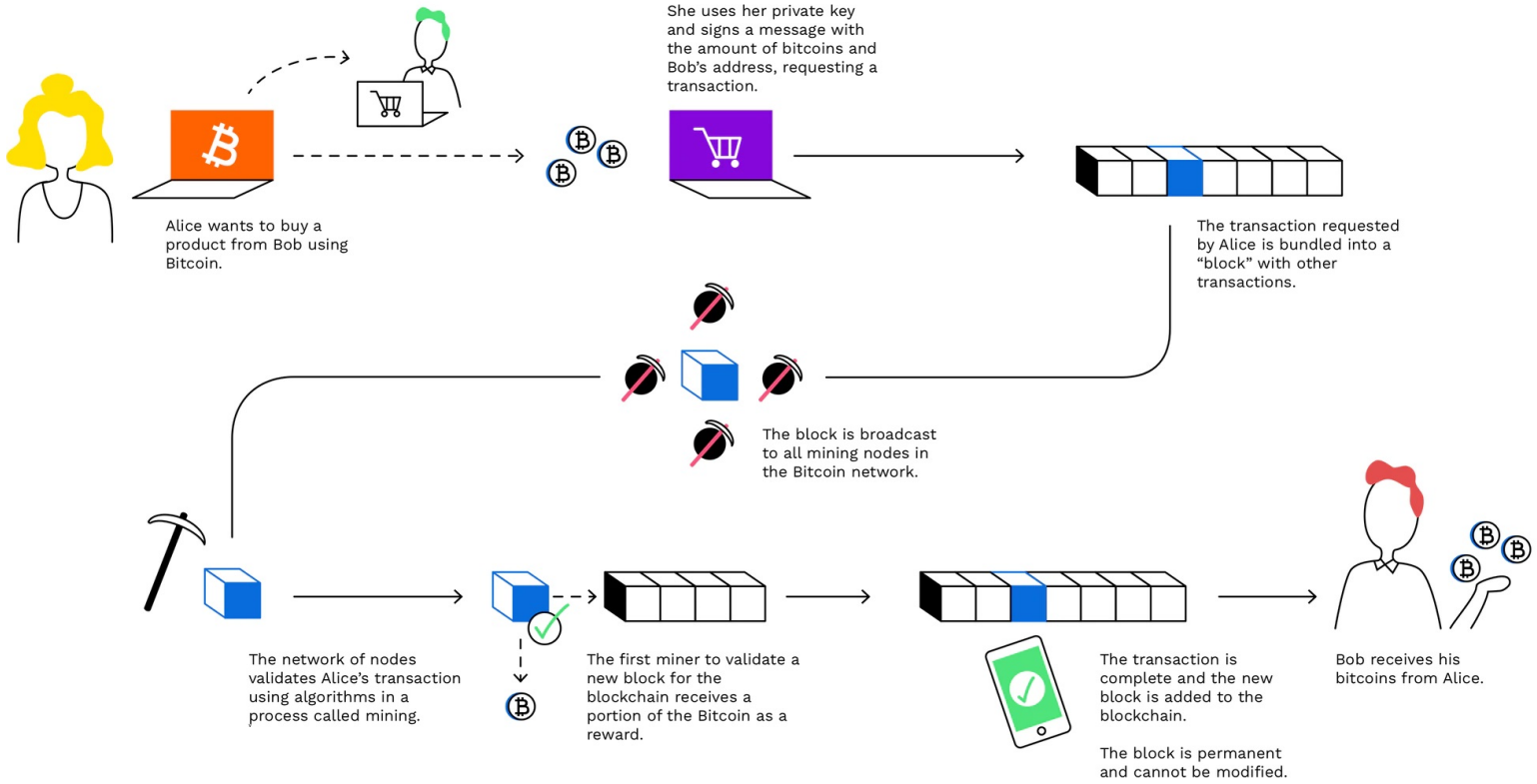
Since blockchains are transparent, every action in the ledger can be easily checked and viewed.

Nakamoto consensus

Bitcoin network use consensus by crypto-lottery:

1. Miners print their own “lottery tickets” by solving crypto-puzzle using brute-force (proof-of-work);
2. Winner add a new block to the blockchain and gets reward: e.g., print new money;
3. All miners gravitate to longest chain. Repeat.

A Bitcoin transaction diagram



Source: https://www.bitpanda.com/academy

Key Features

- ✓ Write-only, immutable, transparent data storage
- ✓ Decentralized, no need for intermediaries
- ✓ Resistant against malicious participants
- ✓ Open to everyone
- ✓ Consistent state across all participants
- ✓ Creating witnesses

Challenges

- ✓ Energy consumption (huge amount for proof of work);
- ✓ Transaction delay – *minimum* 10 min.
- ✓ Scalability
- ✓ Personal responsibility
- ✓ Money laundering

Important dates in the history of Bitcoin

Bitcoin was the first non-duplicable digital currency. This digital asset eliminated the need for transactions fees and other third-party controls, regulations, and restrictions typically associated with moving currency.

2008: A paper was published proposing a form of digital cash called *bitcoin*.

2009: Start of the Bitcoin Network

2010: First cryptocurrency stock exchange is launched; First purchase using Bitcoin - two Papa John's pizzas for just 10,000 BTC's (worth about $60 at the time and $500 millions today).

Important dates in the history of Bitcoin

2011: One Bitcoin equals one USD

2013: 1 Bitcoin equals 100 USD;

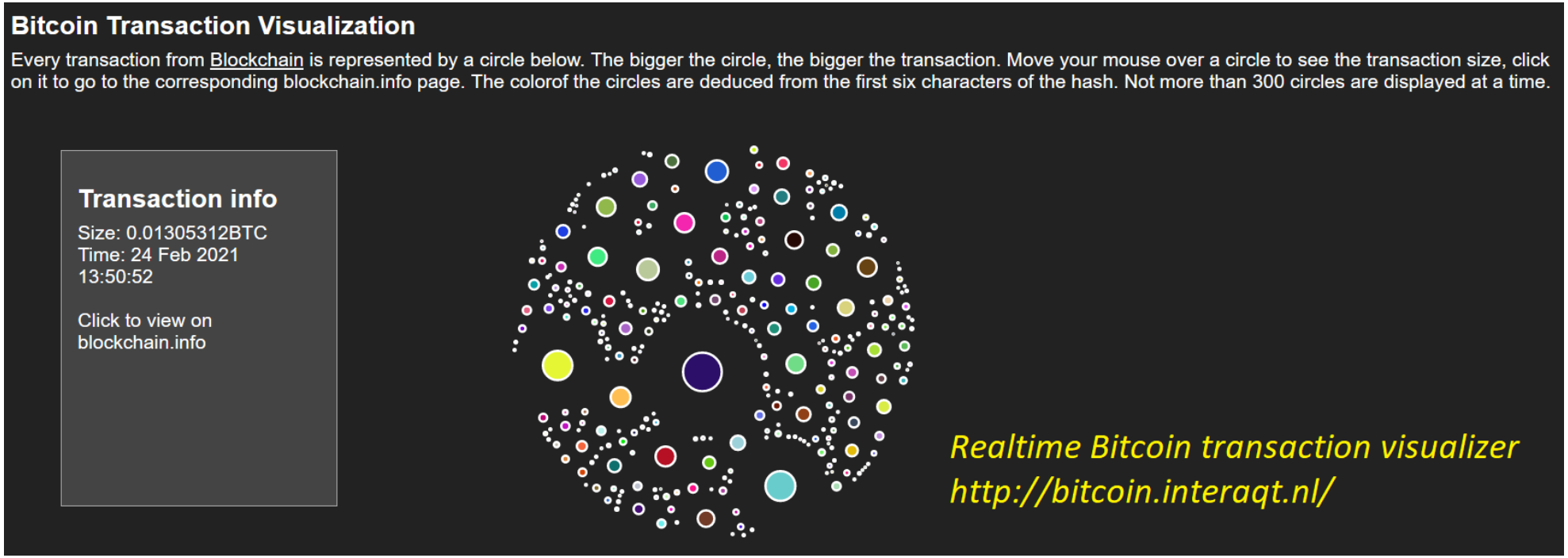
2014: Microsoft accepts Bitcoin, PayPal announces Bitcoin integration;

2017: 1 Bitcoin equals 10,000 USD;

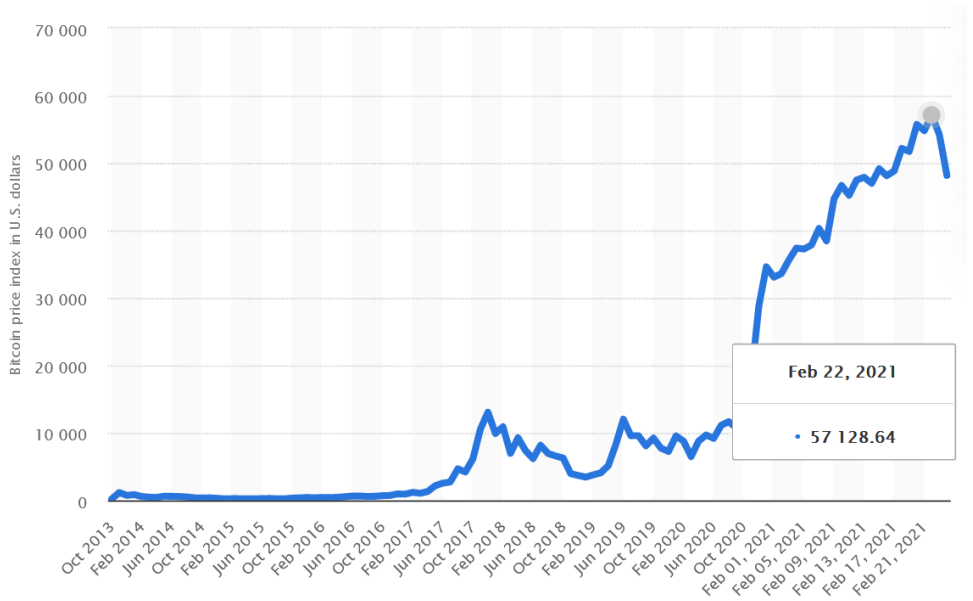
2018: IBM develops a blockchain-based banking platform with large banks like Citi and Barclays signing on.

2021: 1 Bitcoin equals 60,000 USD;

Bitcoin visualization



Bitcoin price evolution



Source: https://www.statista.com/statistics/326707/bitcoin-price-index/

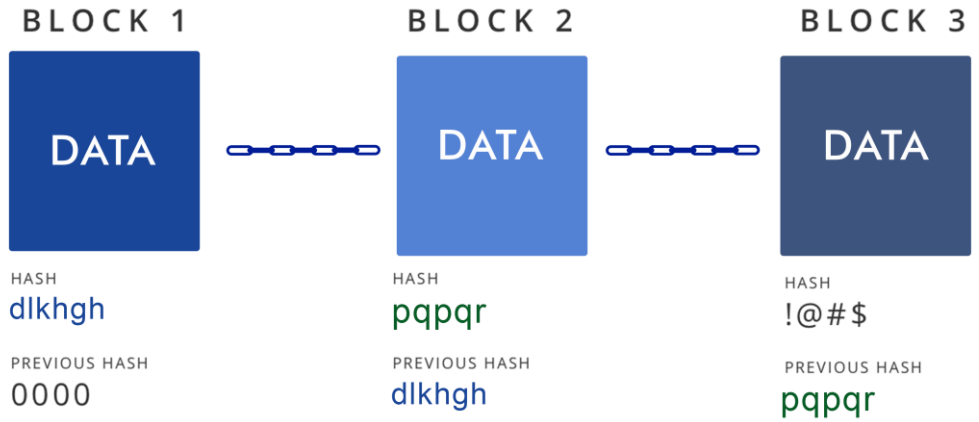
- The cryptocurrency market is still in its infancy, being supposed to a high volatility of the prices. It's still important to notice that the general financial uncertainty attract positive effects on the Bitcoin prices, following a pattern that is strongly correlated with the crisis periods.

- The cryptocurrency market is more exposed to bubbles and crashes, as a result of the strong contagion effect between different cryptocurrencies. In the same time, there is a clear request for the alternative money as we can notice from the growth in the Bitcoin trading volume and price.

Other Blockchain ledgers

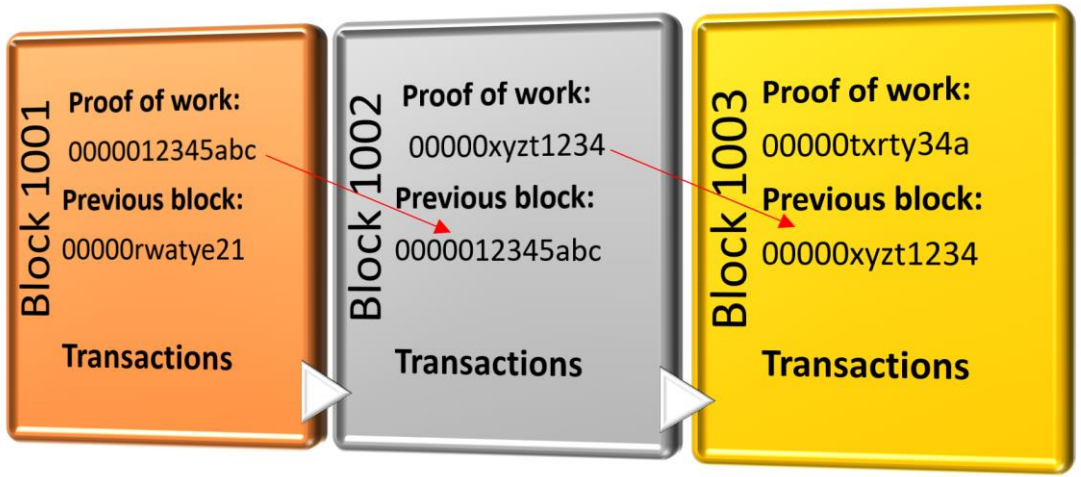
Nakamoto uses blockchain to transparently record a ledger of payments, but blockchain can be used to record any number of data points.

This could be in the form of transactions, votes in an election, product inventories, state identifications, and much more.



Conclusions so far:

- Blockchain is a system of recording information in a way that makes it difficult or even impossible to change or cheat the system.
- A **blockchain is essentially a digital ledger of transactions** that is duplicated and distributed across the entire network of computer systems on the blockchain.
- Most normal databases, such as an SQL database, have someone in charge who can change the entries. Blockchain is different because nobody is in charge; it's run by the people who use it.



Keys, Seeds, Addresses, Wallets

- Sometimes all the terminology and technical details related to blockchain are overwhelming.
- However, as a new user, you can get started with Bitcoin without understanding the technical details. Once you've installed a Bitcoin wallet it will generate your first Bitcoin address. You can disclose your addresses to your friends so that they can pay you.

A useful analogy!

Crypto Wallet

Home

What is a Private Key?

- **A private key proves to the Bitcoin network that you own bitcoin and allows you to spend your bitcoin.**
- A private key is essentially a random number between 0 and 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936. Pretty much, a 256-bit number.
- But it'd be difficult to use that every time you wanted to spend bitcoin, right? So developers created a **human-readable format** to derive private keys: the popular **seed phrase** format.

What is then a Seed Phrase?

- A seed phrase is simply **a representation of a random number. It's an ordered sequence of 12 or 24 words**, chosen from a list of 2048 words.

- Here's an example of a seed phrase:

  kit invite plastic dove lumber quote

  board young robust regular skull history

- Using cryptography, **your wallet can derive your private key using your seed phrase**. And with that private key, your wallet can spend your bitcoin.

Hash Functions

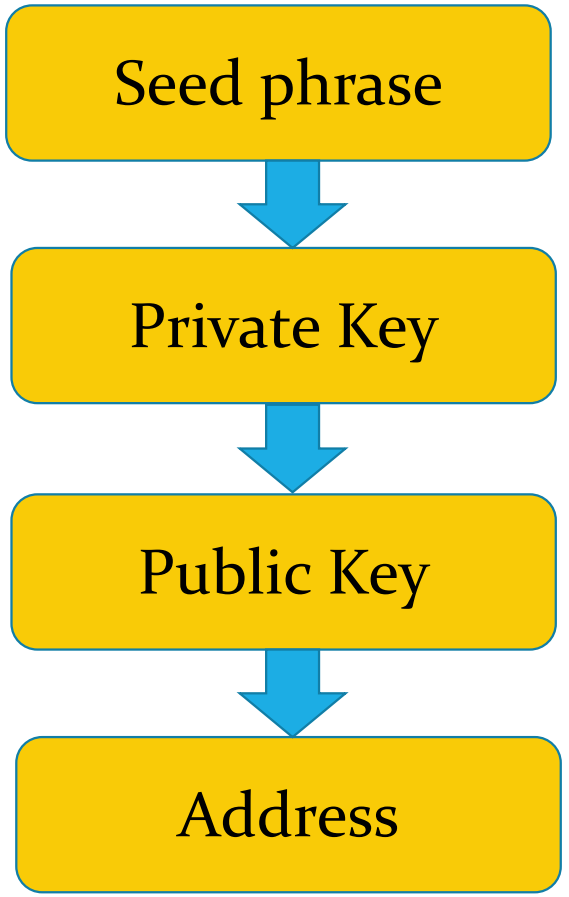
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

- The other aspect of a hash function is that it is "one way". It is very easy to put input into the hash function and get output, but it's basically impossible to get some hash output and determine from that what the input was.

What is an Address?

An address is a "**human-readable" form of its respective public key.** It's where you receive bitcoin.

So, a seed derives a private key. That private key generates its corresponding public key. That public key then generates its corresponding address.

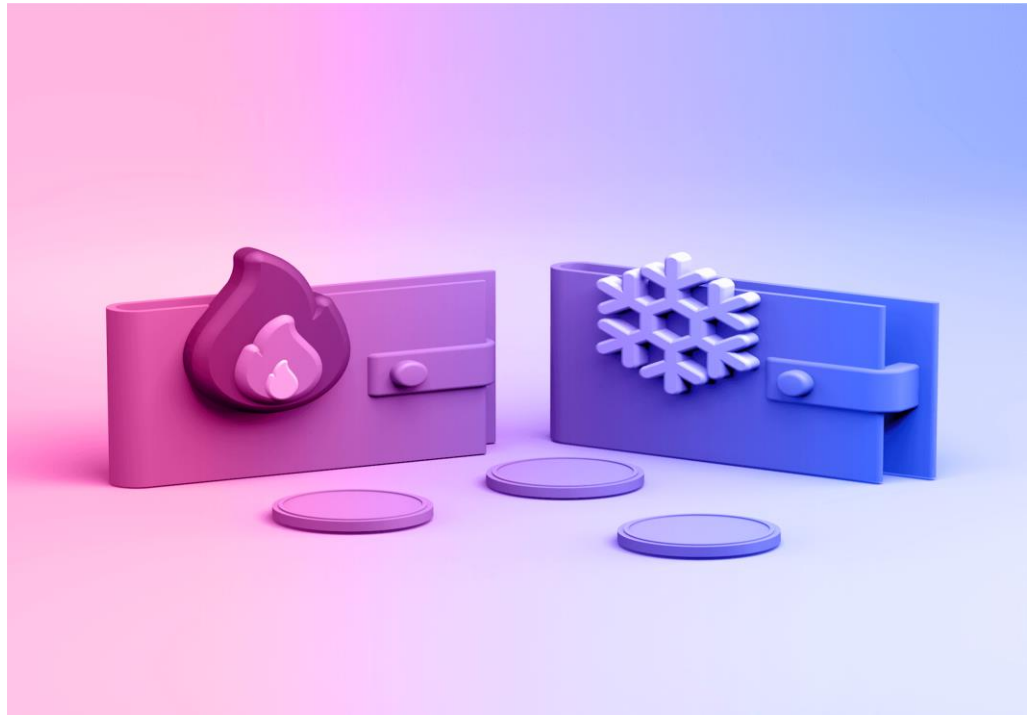


Cryptocurrency wallets

Cryptocurrency wallets provide users with a digital solution for securely storing and managing blockchain assets and cryptocurrencies.

They are one of the basic pieces of infrastructure that make it possible to send and receive funds through blockchain networks.

Hot vs Cold Wallets



Desktop wallets

- As the name implies, a desktop wallet is a software you download and execute locally on your computer. Unlike some web-based versions, desktop wallets give you full control over your keys and funds. When you generate a new desktop wallet, a file called "wallet.dat" will be stored locally on your computer. This file contains the private key information used to access your cryptocurrency addresses so you should encrypt it with a personal password.

- If you encrypt your desktop wallet, you will be required to provide your password every time you run the software so that it can read the wallet.dat file. If you lose this file or forget your password, you will most likely lose access to your funds.

- In general, desktop wallets may be considered safer than most web versions, but it's crucial to make sure your computer is clean of viruses and malware before setting up and using a cryptocurrency wallet.

Mobile wallets

- Mobile wallets function much like their desktop counterparts but designed specifically as smartphone applications. These are quite convenient as they allow you to send and receive cryptocurrencies through the use of QR codes.
- As such, mobile wallets are particularly suitable for performing daily transactions and payments, making them a viable option for spending Bitcoin, and other cryptocurrencies in the real world.
- Just as computers, however, mobile devices are vulnerable to malicious apps and malware infection. So it's recommended that you encrypt your mobile wallet with a password, and backup your private keys (or seed phrase) in case your smartphone gets lost or broken.

Hardware wallets

- Hardware wallets are physical, electronic devices that use a random number generator (RNG) to generate public and private keys. The keys are then stored in the device itself, which isn't connected to the Internet. As such, hardware storage constitutes a type of cold wallet and is deemed as one of the most secure alternatives.

- While these wallets offer higher levels of security against online attacks, they may present risks if the firmware implementation is not done properly. Also, hardware wallets tend to be less user-friendly, and the funds are more difficult to access when compared to hot wallets.

- You should consider using a hardware wallet if you plan to hold your crypto for a long time or if you're holding large amounts of cryptocurrency. Currently, most hardware wallets allow you to set up a PIN code to protect your device, as well as a recovery phrase – which can be used in case your wallet is lost.

Real world applications:

- Jaxx Wallet
- Nicehash miner
- Binance exchange

References

1. Antonopoulos, A., *Mastering Bitcoin*, O'Reilly Media, Inc., 2014
2. Katz, J., Lindell, Y., *Introduction to Modern Cryptography*, Chapman & Hall/CRC, 2008
3. https://arstechnica.com/tech-policy/2017/12/how-bitcoin-works/
4. https://bitcoin.org
5. https://blockgeeks.com/guides/cryptocurrency-wallet-guide/
6. https://blockgeeks.com/guides/what-is-hashing/
7. https://crushcrypto.com/cryptography-in-blockchain/
8. https://www.blockchain.com/explorer
9. https://www.coindesk.com/math-behind-bitcoin
10. https://www.euromoney.com/learning/blockchain-explained
11. https://www.facebook.com/ProjectBLOCKS/
12. https://www.investopedia.com/terms/b/blockchain.asp
13. http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

CONTACT: cgeorge@univ-ovidius.ro

BLOCKS

GRAB A BLOCK OF COFFEE UNTIL 15:00