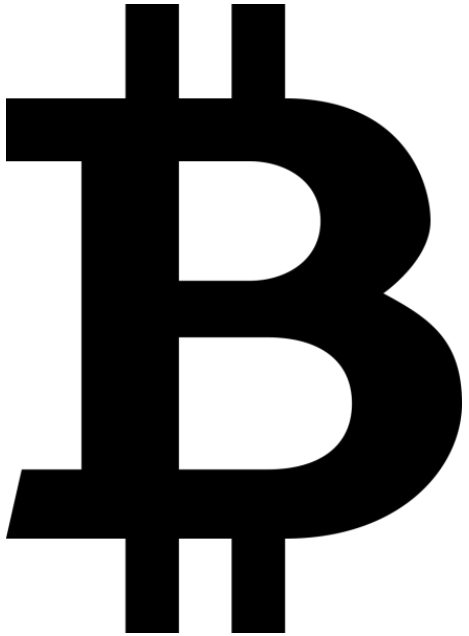
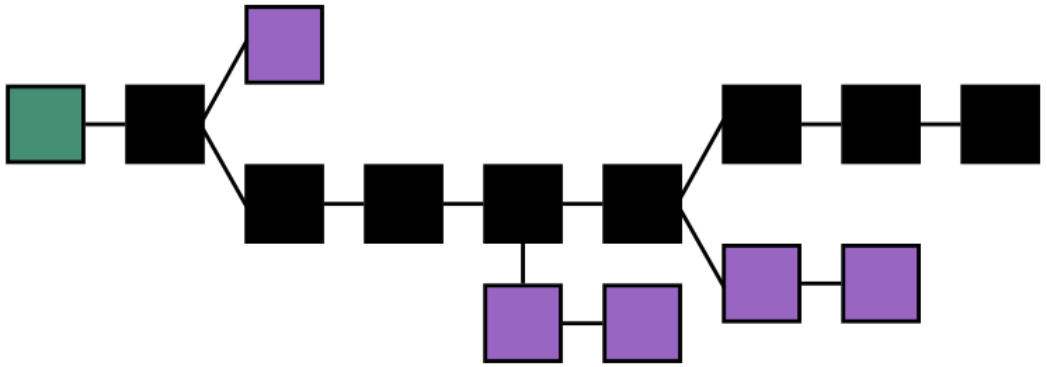
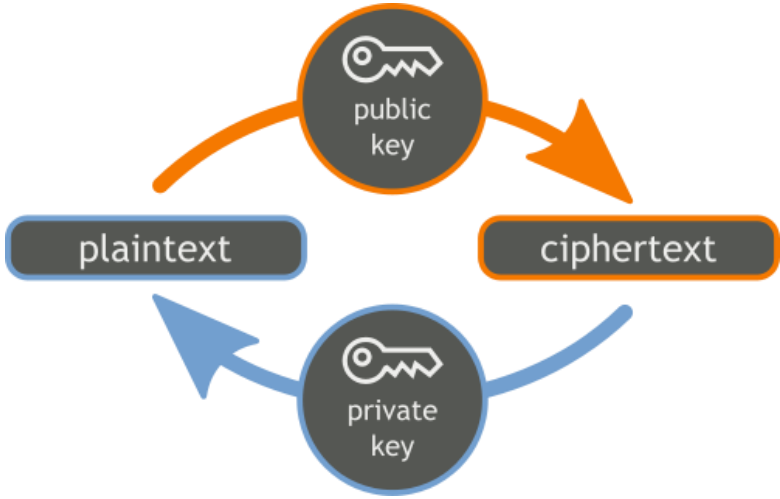
Bitcoin, Blockchain, and Cryptocurrencies

Mika Mäntylä <mika.mantyla@oulu.fi>, M3S, University of Oulu

Contributions by Adrian Santos, M3S, University of Oulu







Essay – Bitcoin, Blockchain, Cryptocurrencies

- Explain: a) Commodity money, b) Gold standard (money), c) Fiat Money, d) Cryptocurrencies
  - Why people trust Fiat money? Are there any examples of Fiat money problems?
  - Are cryptocurrencies a, b, or c?
- How does bitcoin solve double spending problem in a network without central authority?
- What is bitcoin mining? How are nonce and hash functions related to bitcoin mining?
- Electricity consumption of bitcoin mining. What are the consequences?
- Is mining bitcoin mining profitable?
- What are smart contracts?
- How do you see the future cryptocurrencies and smart contracts?

Cryptocurrencies

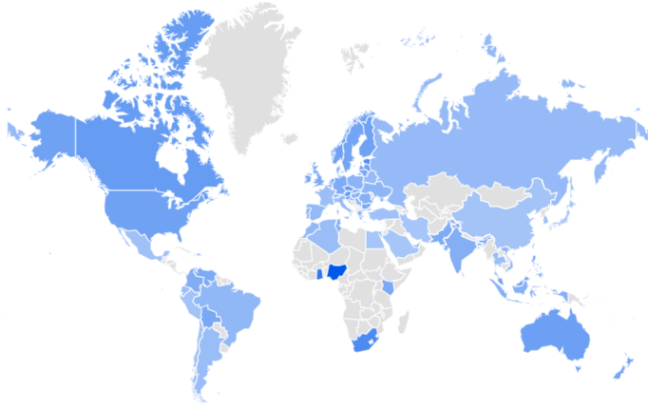
- “A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange using cryptography to
  1. secure the transactions
  2. control the creation of additional units of the currency” <wikipedia>
- Cryptography Originally used to secure communication
  - kryptós, "hidden, secret";
  - graphein, "writing",

Bitcoin popularity

Hakumäärät ajan mittaan

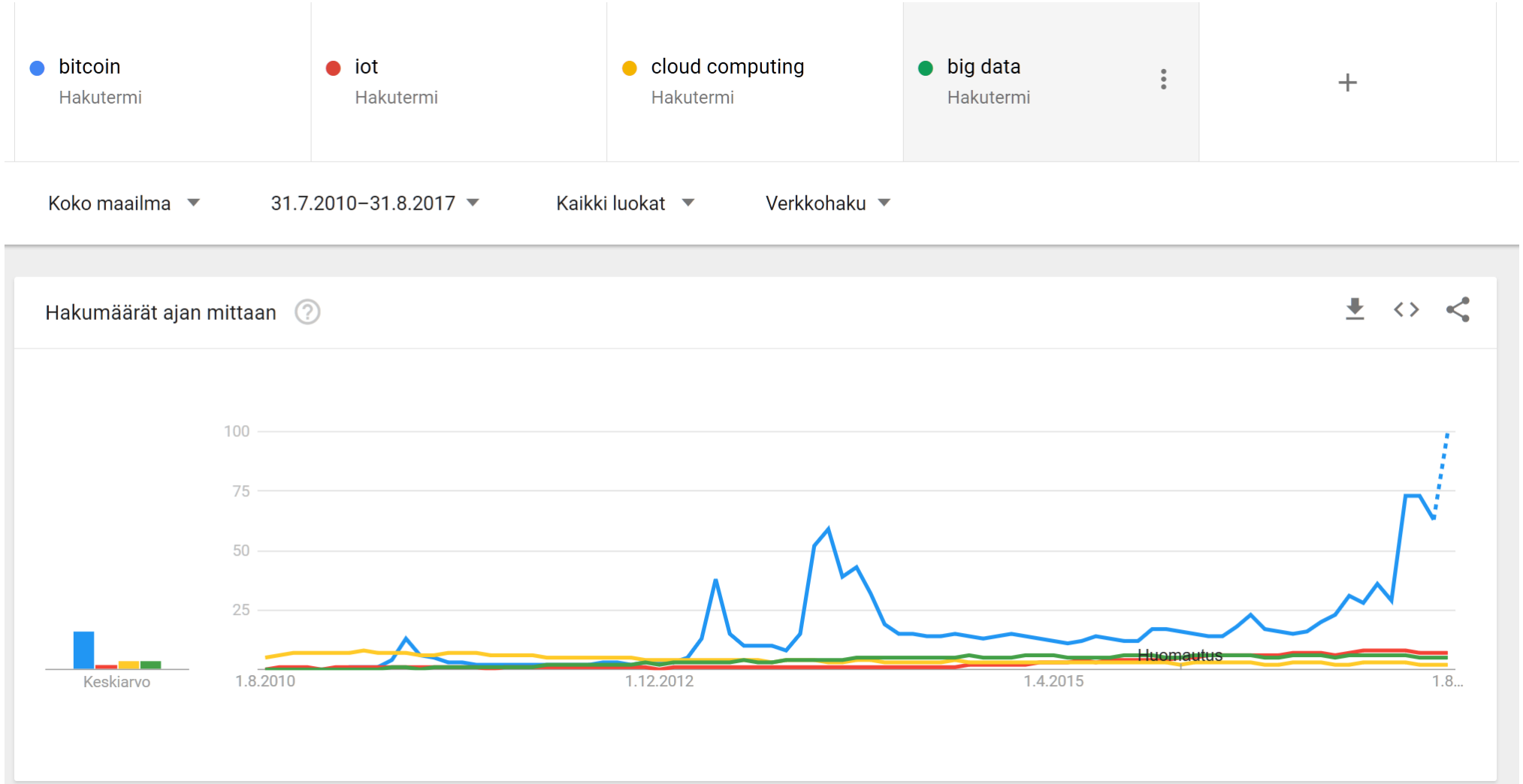
Kiinnostus alueittain

Alue

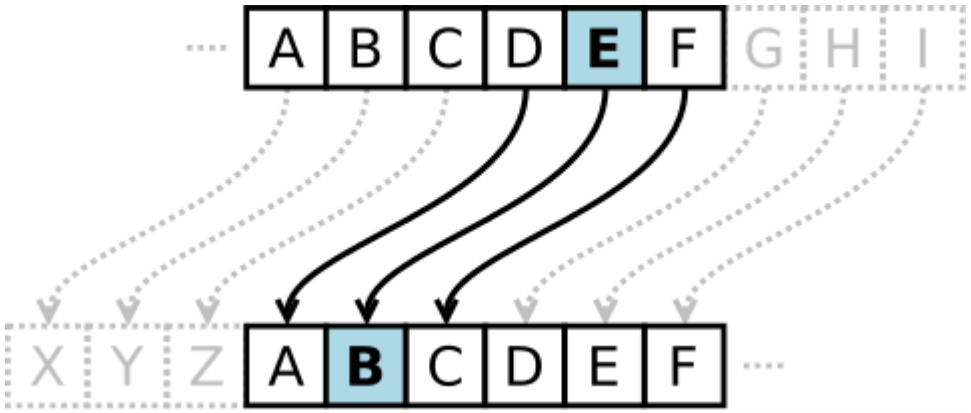


1	Nigeria	100
2	Ghana	73
3	Etelä-Afrikka	56
4	Viro	54
5	Slovenia	53

Bitcoin popular than IoT, Cloud Computing, Big Data



How do we get from Cryptography



Caesar cipher

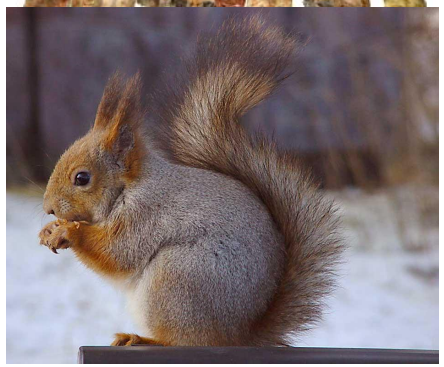
Navajo language

By Alessandro Nassiri - Museo della Scienza e della Tecnologia "Leonardo da Vinci", CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=47910919

Enigma encryption machine

http://summersidemakerspace.ca/projects/enigma-machine/

To Money



What is money?

- Money is an item or record accepted as payment in a particular country or socio-economic context
- Every well functioning society needs money
  - For example, making payments for this lecture via exchange would be difficult
    - Students would bring lunches as payment?

Exercise - Money – Discuss with a pair

- Why is one note worthless (on the right) while the other (on the left) has value?
- How could the worthless note become valuable and accepted?
- Students:
  - Convention and Agreement
  - Some piece of paper represents a certain amount of gold
  - Money has value because people believe it has value
  - Rare

Commodity money

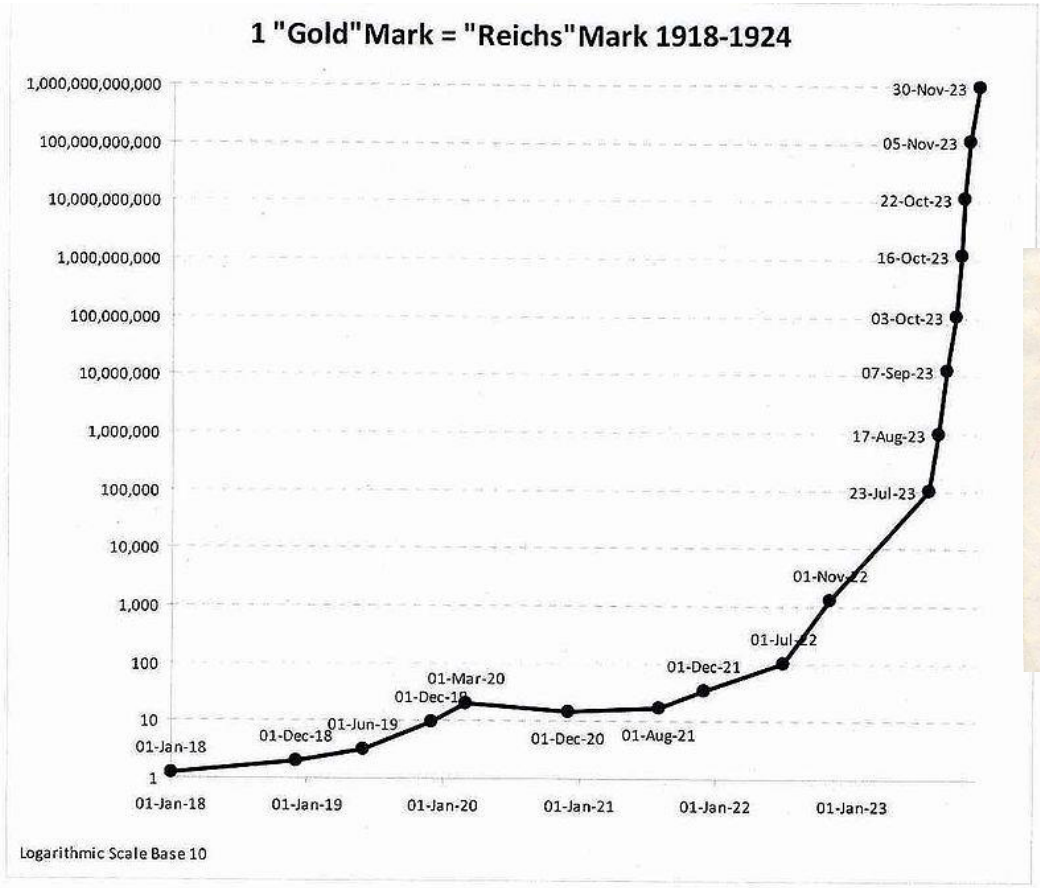
- Commodity money may be used for some purpose
  - Finland – Squirrel skins can be used for fur clothing during winter
  - Prisoner Of War camps – Cigarette currency
  - Others: Gold, silver, spices, tea, etc.

Gold standard to Fiat money

- Fiat money has no value other than the one given by a country or socio-economic context.
  - Fiat (latin) etymology => "let it become", "it will become"
  - Fiat uses => Authorization, permission or (official) sanction, e.g. “a government fiat”
- Why? Commodity money is inconvenient to transfer, transport, or store.
- Way to pure Fiat money was created via Gold Standard
- Gold Standard – For every money unit the government holds a fixed amount of gold, e.g. in Fort Knox

From gold standard to pure fiat -> Hyperinflations

By John Alan Elson - see http://www.3dham.com/scancoins/index.html, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=30681800



Note: 1 "Gold"Mark value in grammes of fine gold (1913) = 0.35842g;
"Reichs"Mark = Currency not tied to the goldstandard in 1918 to 1924.

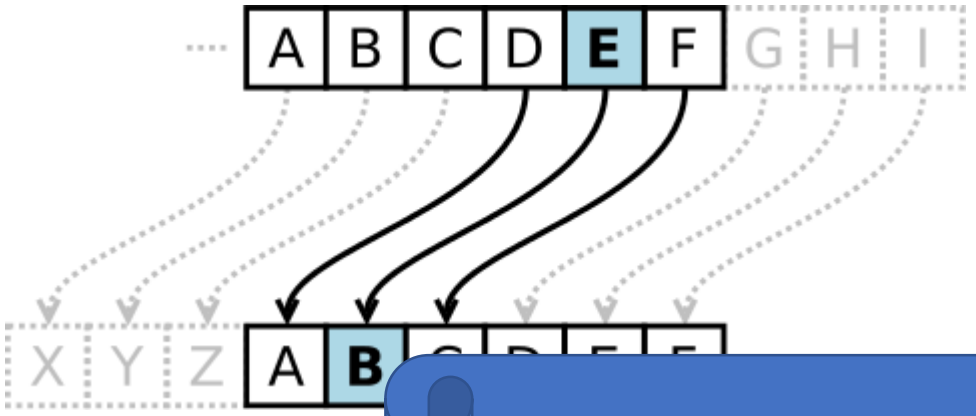
Source: Law about the Revaluation of Mortgages and other Claims (Revaluation Act 1925), issued the 16th of July, 1925 (Aufwertungsgesetz, Reichsgesetzblatt, Teil I, 1925, p.133-135) and Author's calculations.

By Wolfgang Chr. Fischer - Template:Wolfgang Chr. Fischer, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=11013489

End of Bretton Woods - Birth of the current fiat money

- After WWII Bretton Woods agreement fixed that a gold ounce was worth $35 (pegged rate)
- 1970's due to financial troubles U.S. and western countries could not protect the pegged rate
  - Market valued gold more than US dollars
  - US had lost lot of gold and was in financial trouble

How do we get from Cryptography



Caesar

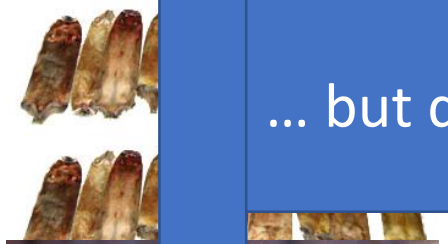
n machine

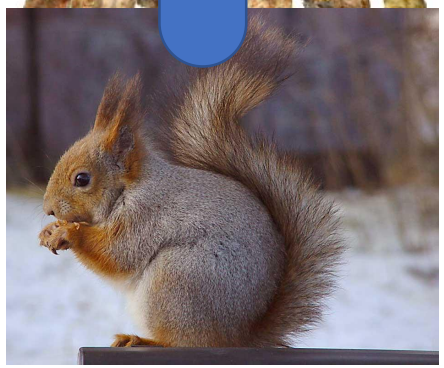
projects/enigma-machine/

To Mone

1st obstacle cleared. Money already prior to crypto money was Fiat money (not based on anything expect to the fact that we trust the government, state, the economy and politicians…

… but do we really





Majority of money is electronic,
- just numbers inside a computer
- software runs banks and credit card companies

FIRST BANK OF WIKI
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

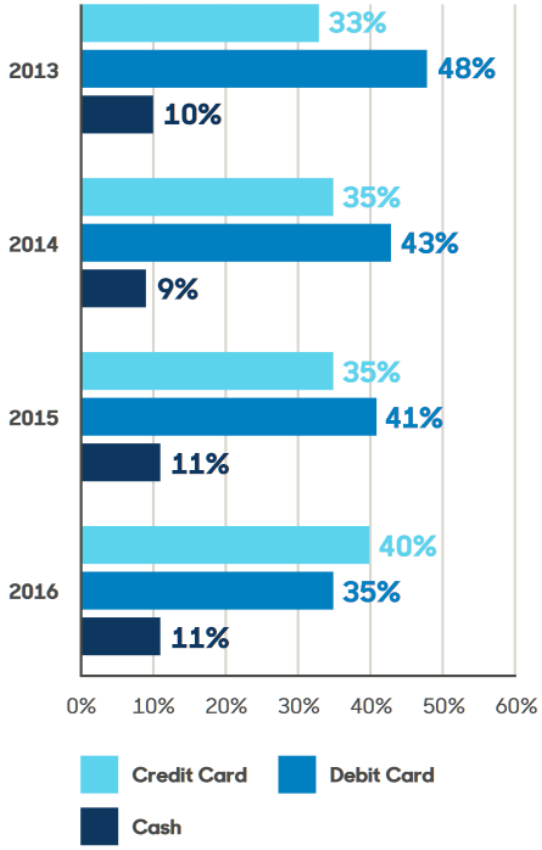
CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	00005-123-456-7

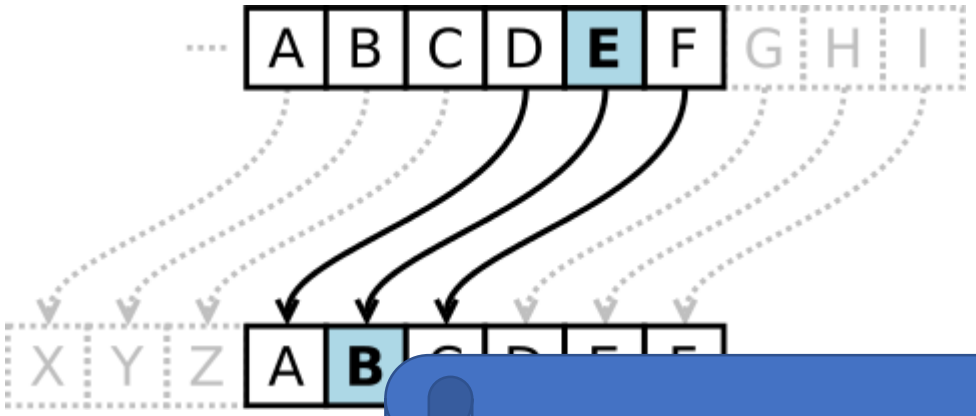
Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47
	*** Totals ***		1,515.63	1,442.61	

Exhibit 4:
Most Preferred Payment Type



http://www.tsys.com/Assets/TSYS/downloads/rs_2016-us-consumer-payment-study.pdf

How do we get from Cryptography



Caesar

logia "Leonardo da Vinci", CC BY-SA 4.0,
10919

n machine

projects/enigma-machine/

To Mone

2nd obstacle cleared. Money already prior to crypto money was Electronic controlled by Software

Any currency needs mechanism to

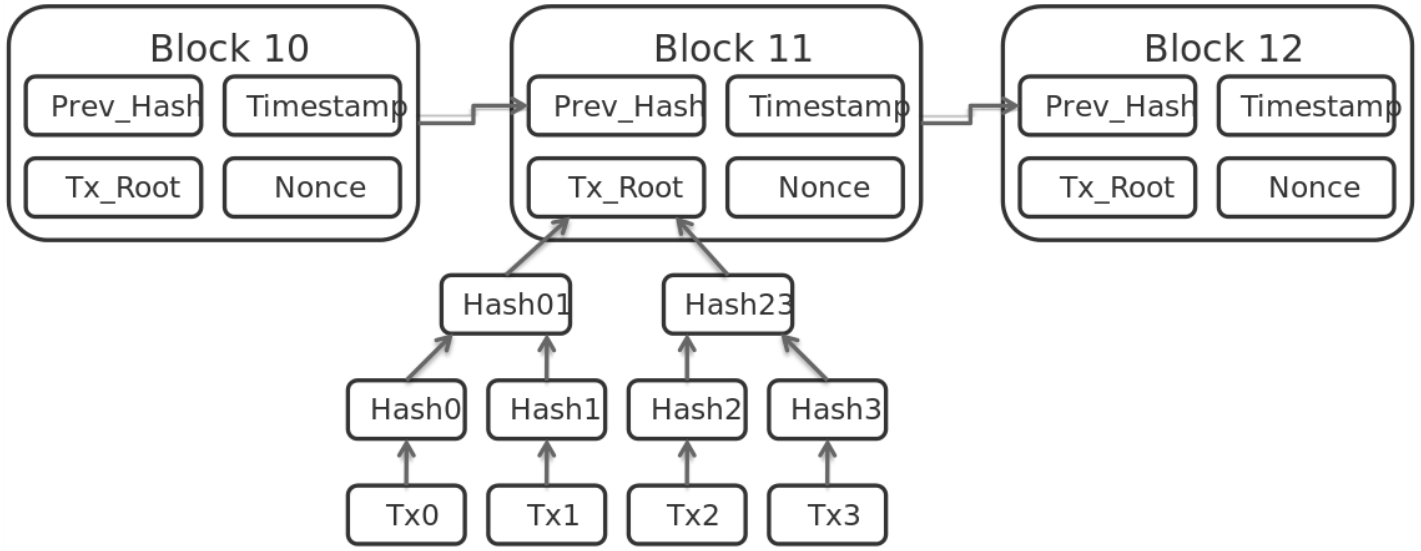
- Secure the transactions
  - Cash: Trust (in handing over) and security personnel if large amounts
  - Electronic traditional money: 3rd party (bank, or credit card company)
  - Cryptocurrencies: Block chain (p2p network, pki, hash)
- Control the creation of additional units of the currency
  - Cash / Electronic traditional: Central bank (remember currently all pure Fiat money without gold standard)
  - Cryptocurrencies: Cryptocurrency scheme (max amount of Bitcoins is 21 million)

Original Bitcoin Paper - Arguments from 2008

- All electronic commerce runs on trusted based system (trusted 3rd party)
  - There is no way to do direct “cash” like payment online wo trusted 3rd party
- Need: “Electronic payment system based on cryptographic proof instead of trust”
- Double spending -> Same money can be spent more than once
  - I have 10 euro and I send it to two person A and B simultaneously
  - Like cash it has to go to one or the other
- Solution only take the transaction that is first but how to decide what is first
- Use trusted 3rd party that decides
- Wo 3rd party
  - All transactions must be public
  - System (nodes) must agree an a single **valid** transaction file with order
  - Agreement – the group with most CPU power decides which transaction A or B becomes valid
    - A group that first produces valid bitcoin block (proof-of-work)
  - Faking transaction file requires a lot of CPU power
- Bitcoin “is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”
- “If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins thaneveryone else combined, than to undermine the system and the validity of his own wealth.”

Block chain – Technology that runs crypto currencies

- Blockchain enables: “an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way”[1]
- Ledger (Tilikirja / Reskontra) – A way to keep track of money transactions

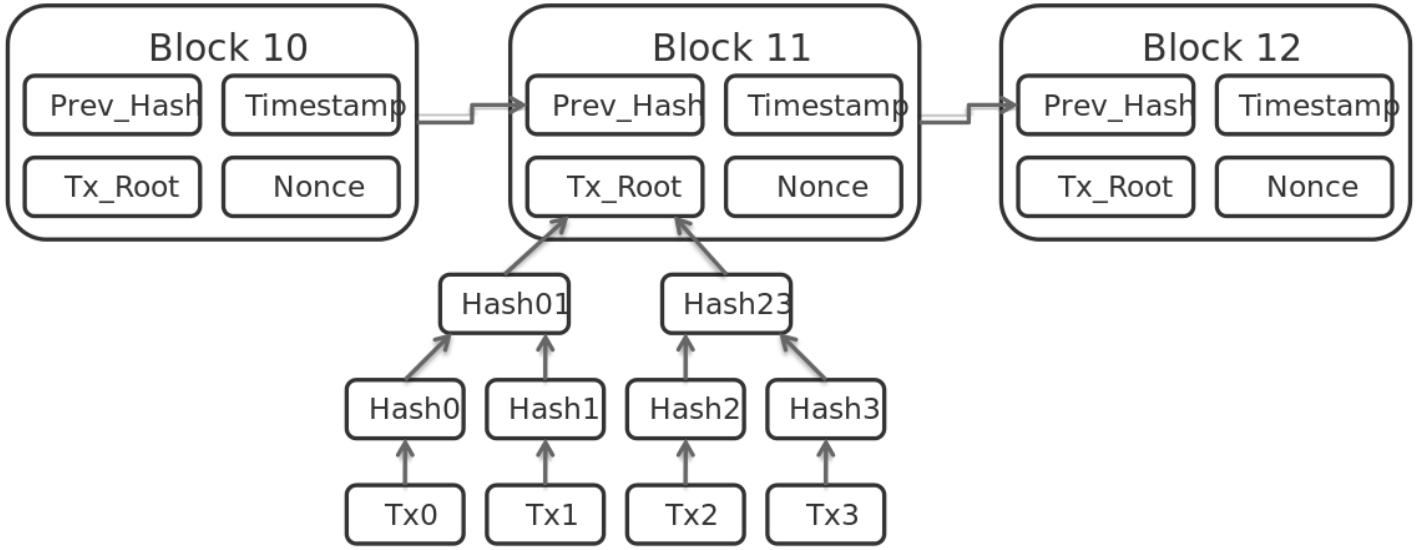


By Matthäus Wander, CC BY-SA 3.0, https://en.wikipedia.org/wiki/File:Bitcoin_Block_Data.svg

[1] Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University.

Block chain – Tx_Root (Transactions Root)

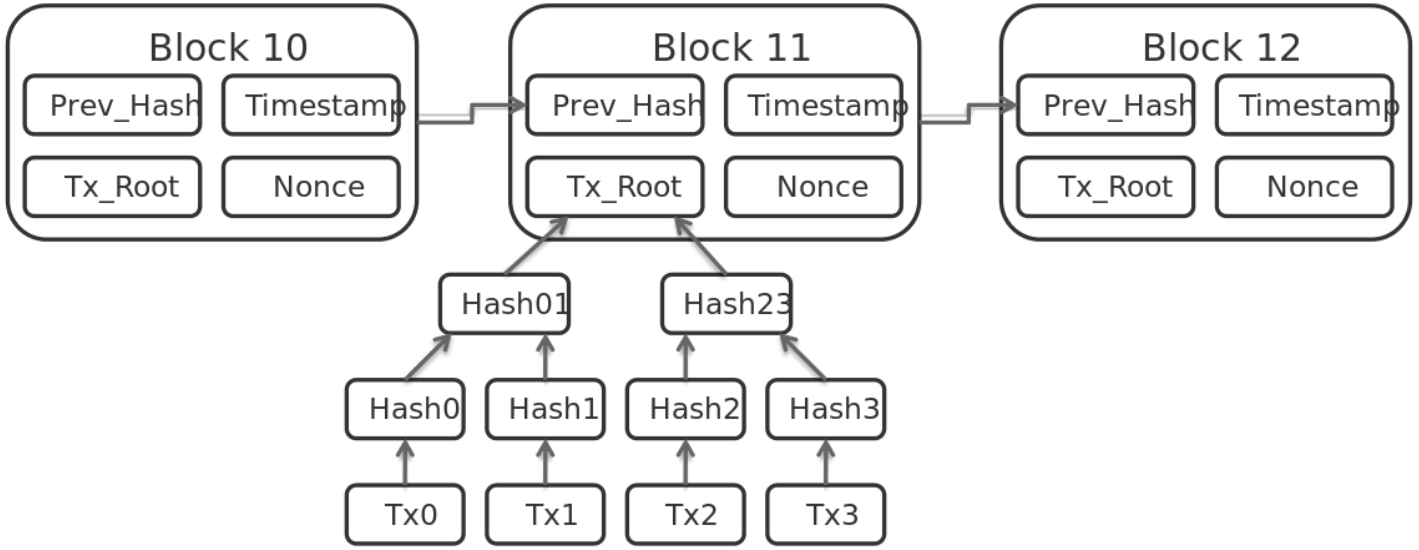
- Tx_Root is hash tree of all transactions that occurred at a particular time intervall
- Tx0-TxN are transactions (leaf nodes) which are hashed -> Hash0-Hash3
- Transaction hash values are again hassed to form Hash01 and Hash23
- Hash values make transaction difficult / nearly impossible to alter



By Matthäus Wander, CC BY-SA 3.0, https://en.wikipedia.org/wiki/File:Bitcoin_Block_Data.svg

Block chain – Timestamp & Nonce

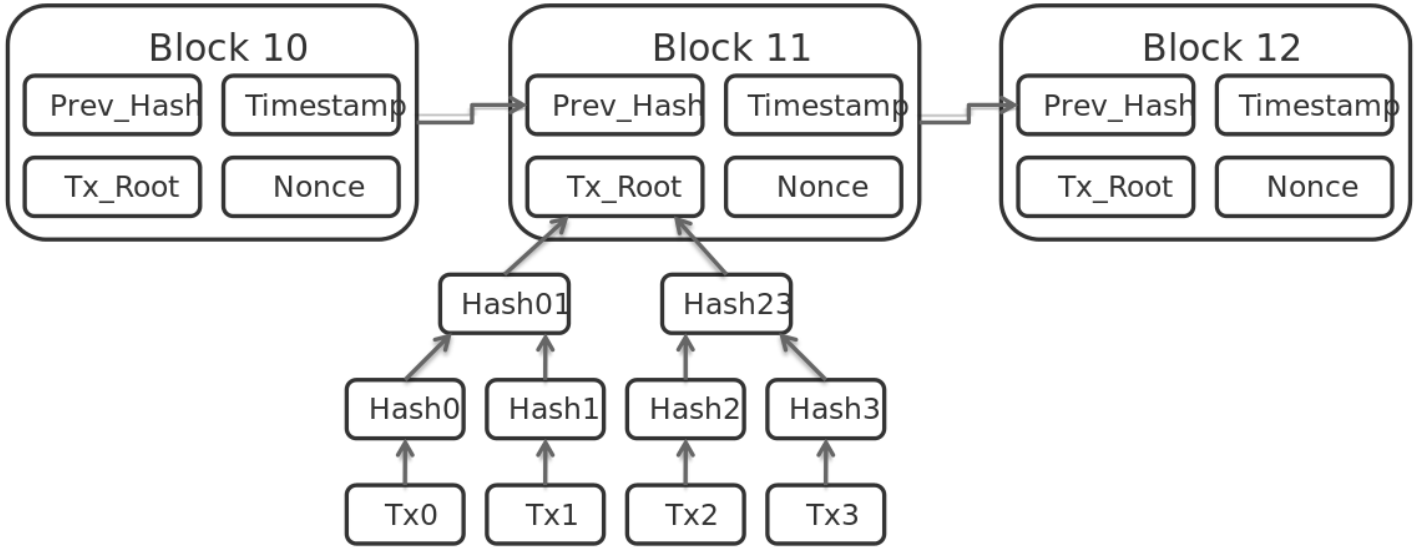
- Timestamp time when transactions were processed
- Nonce is random number searched for each block by the Bitcoint proof-of-work system



By Matthäus Wander, CC BY-SA 3.0, https://en.wikipedia.org/wiki/File:Bitcoin_Block_Data.svg

Block chain – Hash functions

- Prev_Hash = Hash value of previous block. Links all values together
- Hash function takes in data and computes fixed length output
- Even small modifications of input result in large changes in output
- http://onlinemd5.com/
- Hash functions are one way!
- Brute force attack needed to reversing - > What input generates a particular hash
- Since input space is larger there are collisions -> two inputs create same hash value but they are very rare
  - In SHA 256 they happen every 2^256 hash values.

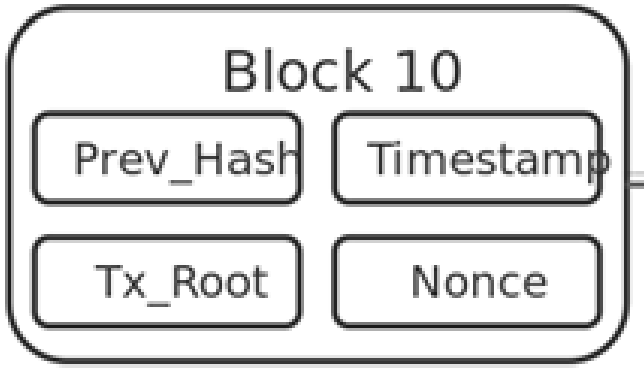


By Matthäus Wander, CC BY-SA 3.0, https://en.wikipedia.org/wiki/File:Bitcoin_Block_Data.svg

File	Checksum (SHA256)
Mist-linux32-0-9-0.deb	5ad1aa5723c7ecf63bcb3066df354b40232082c9768b62f600d48bd11e3639d5
Mist-linux32-0-9-0.zip	a4824c185e1353eebe727515d69ef34a79e953b8c925b355b33849e5b81caddc

Nonce searing -> Mining Bitcoins –> Proof of work schemes

- Proof of work – A computational puzzle that takes significant effort to compute but are easy to check
- For example create a message that produces SHA256 hash value starting with 0x000. Try it at http://onlinemd5.com/
- Bitcoin mining -> modify Nonce so that a given block has a hash value under threshold.
  - Bitcoin started with easy: 0x00000000FFFF<missing trailing zeros>
  - Current target is more difficifult 0x0000000000404CB<missing trailing zeros>
- Once such Nonce is found
  - the finder is awarded with bitcoins,
  - the block with the correct nonce is added to the block chain
  - the bit coin work moves to mine next block

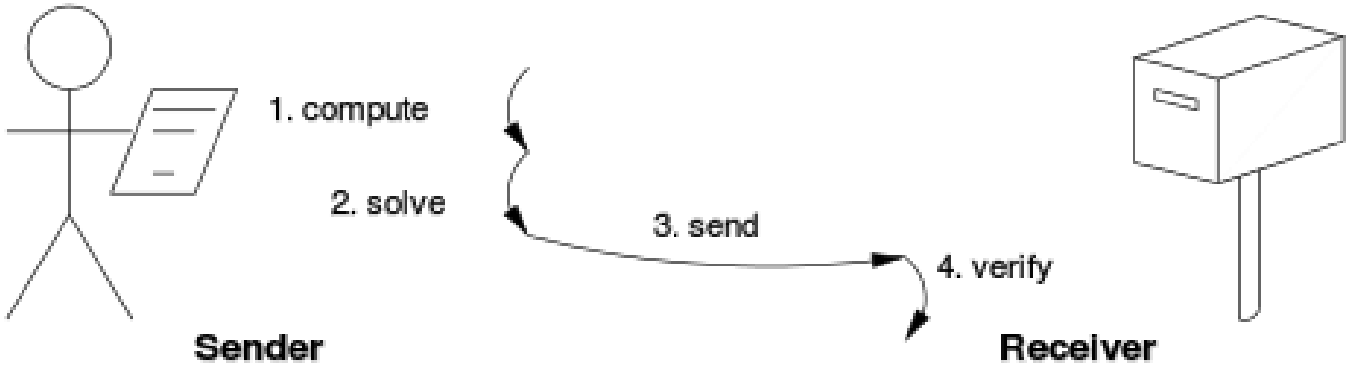


Results of our ”Bitcoin mining example ” http://onlinemd5.com/

- Previos: 850834FF678EFB27D0DAD2778A36EBD4D4794CF398197B3DA48B0069A92BBD09
- Tx_Root: From Mika to Student support foundation 1 bitcoin.
- Timestamp: 9:16, 5.10.2017
- Nonce: 00000000000000000000000000000000000000000000000000000000000000000

Proof of work schemes

- In all such schemes we want to limit the requester by making things unnecessarily difficult
- Things? Add transaction to the ledger for example
- This could be used to fight spam -> require each message to contain SHA256 hash.
  - If sending one message requires 10s of computational power this is not a problem for honest people but it is a problem for spammers.
- In cryptocurrencies proof of work ensures that creating a malicious block or entire ledger is too costly (e.g. a ledger where attacker has more money than in the real one)
  - Without proof of work creating fake blocks and entire ledgers would be too cheap



Majority of effort to mine bitcoins is purposeless, i.e. only needed to provide trust

- In perfectly altruistic and honest world cryptocurrencies would not need such proof of effort
- “a protocol which does not impose costs on its users invite abuse” [1]
- Handicap principle explains incentive for honest communication (between animals) by making bluffing too expensive
  - “Tail of a peacock makes the peacock more vulnerable to predators -> “I have survived in spite of this huge tail; hence I am fitter and more attractive than others” [2]
- “The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.” [3]

By Jatin Sindhu - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=49736189

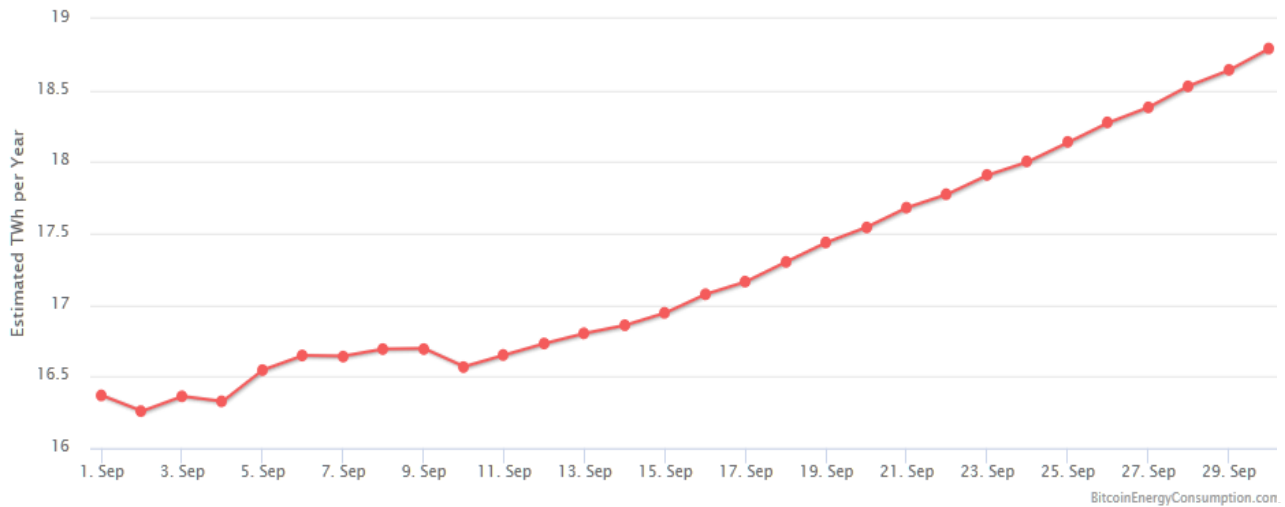
[1] http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/#selection-239.555-239.619
[2] https://en.wikipedia.org/wiki/Handicap_principle
[3] https://bitcoin.org/bitcoin.pdf

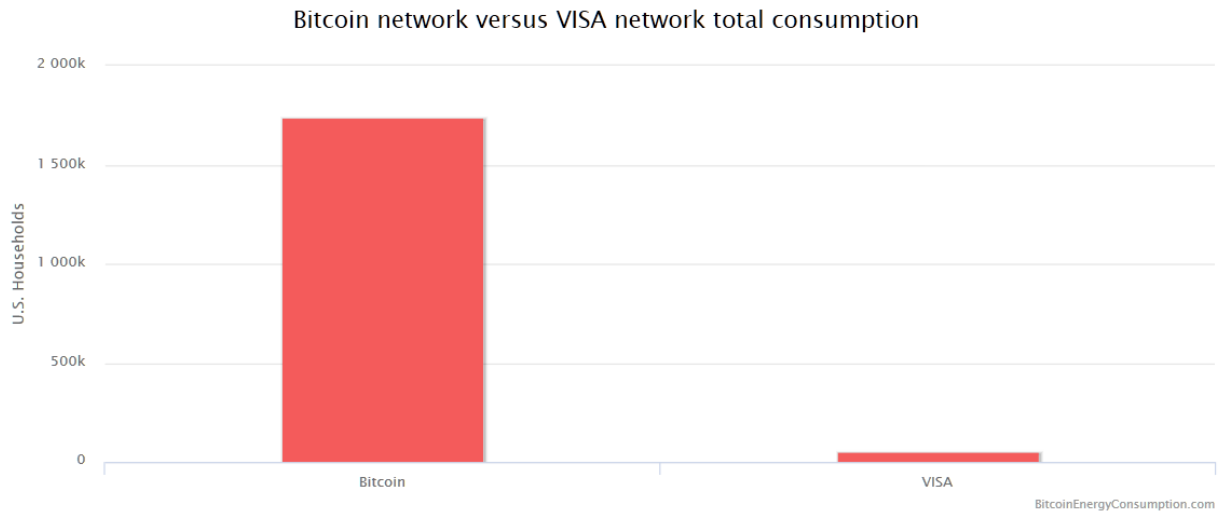
Exercise - Trust – Discuss with a pair?

- Trusted 3rd party and proof-of work schemes. Are there any other ways to establish trust?
- Try to find an input that start with two zeros in
  - http://onlinemd5.com/
- How does finding a particular input helps to establish trust.
- YOUR ANSWERS here

Bitcoin Electricity consumption is not sustainable

- Share of world electricity consumption 0.09%
- Bitcoin consumption 18.79TWh
  - Finland electricity production 66.2 TWh (2016)
- Bitcoin vs. Visa energy consumption
  - Visa processes far greater amount of transaction with fraction of energy use
- For updated number see https://digiconomist.net/bitcoin-energy-consumption





Can I make money by mining bitcoins?

- Can you get your electricity free? If yes then maybe
- Free or nearly free electricity, e.g. 1) dessert + solar panels 2) Houses heated with electricity, 3) Vulcanic activity, 4) Water ways
- Note: Investing in Bitcoin mining hardware is zero sum game
  - New block is release every 10 minutes
  - If computing power in network increases / decreases then nonce difficulty is adjusted so new blocks still come out every ten minutes.

Smart contracts

- A smart contract is a **computer protocol** intended to facilitate, verify, or enforce the **negotiation or performance of a contract**. (Wikipedia)
- Simple Example: Automated payments from a bank account
  - Rent that you setup as recurring payment (fixed amount each month)
  - Electricity bill that you set as auto-pay via “e-lasku” allowes fluctuating amounts to get auto-charged.
    - ”Sinulle on saapunut uusi e-lasku, Fortum Asiakaspalvelu Oy
      Summa 73,11 eur eräpv 29.09.2017
      Olet asettanut tämän laskun automaattiseen maksatukseen, ja se veloitetaan tililtäsi eräpäivänä. “
- Complex smart contracts allow more if-then-else mechanisms
- Smart contracts are immutable like cryptocurrency transactions
- Can be automatically executed even after hundreds of years
- Rent contract can be a smart contract. Both parties digitally sign
  - Every amount a rent contract is automatically charged
  - Contract can auto-lock the rental hourse door
- Employment contracts can be smart contracts.
- Contract for buying a house can be a smart contract
- Insurance contracts
- Smart contract can work together
  - Think a smart contract as a object in OO programming
- More: https://www.youtube.com/watch?v=w9WLo33KfCY

Smart contracts – Putting your money where your mouth is

https://www.reddit.com/r/ethereum/comments/73sddu/smartbillions_just_put_45113717_1500_eth_to_their/

SmartBillions just put $451,137.17 (1500 ETH) to their smart contract for the hackathon. If you break their contract you get 450K self.ethereum

Lisätty 23 tuntia sitten, lisännyt ChopterChopter

To prove the SmartBillions lottery smart contract comprehensive security, the development team has placed 1500 ETH in the smart contract address

The 1500 ETH hackaton prize has been sent to the smart contract address: https://etherscan.io/address/0x5acE17f87c7391E5792a7683069A8025B83bbd85

The prize awaits hacker who will be able to find a way to break into the smart contract and withdraw the stored funds. As we can see, the SmartBillions Team was very serious about guaranteeing Investors' protection.

This is the first time in a history, that Hackaton is held to prove the self-amending, smart contract quality and security. The development team is so sure about their product and its security, that they will risk their own - significant funds (1500 ETH), to prove its safety. The success of Hackaton will prove the smart contract's stability and security. It will also indisputably guarantee, that the Investors' funds will be well protected.

If the funds remain intact, The SmartBillions ICO will start on October 16th.

https://smartbillions.com/

155 kommenttia jaa ilmianna

Final notes

- + No trusted 3rd party
  - lower transaction costs?
- +/- People with mining farms have all the power in Proof of Work. They become defacto trusted 3rd but with less authority (as they still have to follow more strict transaction rules than trusted 3rd party)
- +/- We cannot make more money when we feel like it
  - Overspending politicians are in trouble
- +/- Fiat is an inflationary currency (loses value), Bitcoin is a deflationary currency (increase in value)
  - Deflationary -> Does not encourage spending -> Bad for economic growth?
  - Deflationary -> Does not encourage spending -> Good for the environment?

Final notes

- +/- No rollback of transactions
- + Technological advances (smart contracts)
- +/- Anonymity (Less Orwell good / Criminals can also hide their activies)
- - You are = Your private key file and the password that protects it. If you lose those your account is lost. Forever! If someone steals those they can take all of your money transfer it and you have no way of knowing who the person is.
- - Quantum computers /
- - Unknown crypto attacks (matchematical backdoors)
- - Someone has more than 50% of computing power
  - This could be supplemented with custom made worm attack (similar to Stuxnet) to honest mining rigs

Future considerations

- From PoW (Proof of Work) to PoS (Proof of Stake) -> "Central banks" as we know them already start to appear in cryptocurrencies.
  - POS Another mechanism to achieve distributed consensus
  - POS -> the creator of the next block is chosen with weighted random lottery
  - The wealth of each individual determines the chance of being selected
- Addressing Block chain issues Scalability, Latency, Lower Transactions costs etc.
  - Blockchain off-line https://raiden.network/