Hani Mebar, **Assignment 4**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
24/11/2022

H4 BitCoin Intro

x) Read/watch and summarize

> Nakamoto, Satoshi 2008: Bitcoin: A Peer-to-Peer Electronic Cash System. (A colored HTML version. This is the paper that defined and introduced BitCoin. You can skip "11. Calculations" if you don't like sigma symbols (or just read the code instead of maths if you're a coder). URL and email address on top of the website version seem unbeliveable and added by third party.
>
> Felten et al 2015: Bitcoin and Cryptocurrency Technologies, videos Week 1 (about 1 hour). Requires free registration. If you find it easy to follow, you can also optionally look at week 2 (1,5 h).

a) Really Black Friday. How much is one BitCoin (BTC) worth now? Using historical BTC course, show that you could have lost a lot of money investing in BTC. Also show that you could have won a lot of money with BTC.

b) What's a block chain? Give a simple but detailed explanation. (Feel free to use the most narrow and simple definition of blockchain - no need to consider a whole cryptocurrency).

c) Not BitCoin. Give examples of some AltCoins, crypto currencies compiting with BitCoin. For each AltCoin: how does it differ, what's it's claim for fame?

h) Voluntary: Really black Friday. Buy some BitCoin - it's on discount. If you're new to this, don't risk a lot of money.

i) Voluntary: When do you have to pay taxes for BitCoin in Finland? (If you want, you can instead check taxation in another country)

j) Voluntary: Describe a simple cryptocurrency (you can invent one yourself or use an existing toy example).

k) Voluntary: Secret or public? Find some transactions on a BitCoin account that is related to a case that has had publicity.

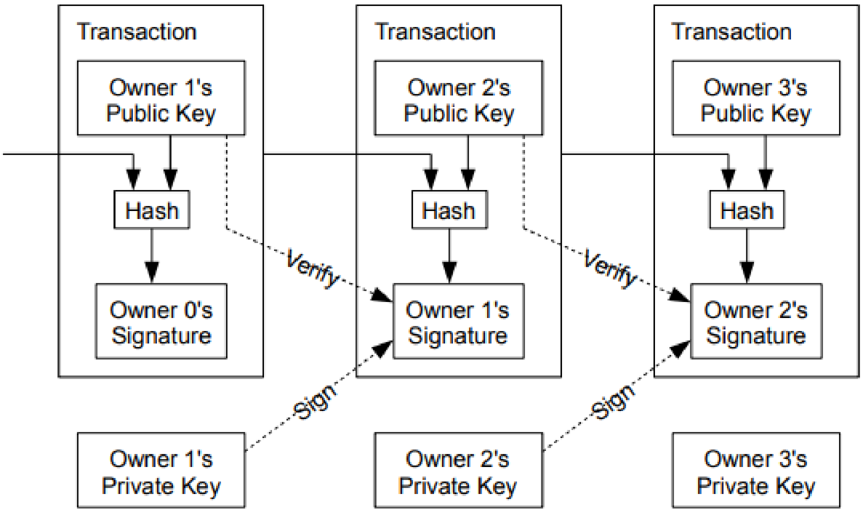
Answers

x) Summary/Notes on Satoshi Nakamoto's paper about BitCoin.

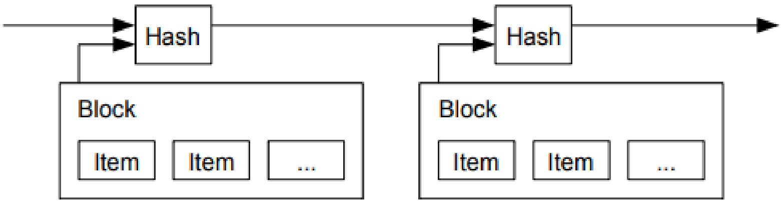
- A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.
- a solution to the double-spending problem using a peer-to-peer network.

Hani Mebar, **Assignment 4**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
24/11/2022

- Transactions costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.
- Crypto currencies are an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.
- an electronic coin is a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



- The challenge with the above model is that it's difficult to verify the previous owner didn't double spend. (Double-spending is the risk that a cryptocurrency can be used twice or more. Transaction information within a blockchain can be altered if specific conditions are met. The conditions allow modified blocks to enter the blockchain; if this happens, the person that initiated the alteration can reclaim spent coins.)
- The solution proposed by Nakamoto begins with a timestamp server. (A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post).
- Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



- Nakamoto provided a proof-of-work. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The block (as pictured previously) cannot be changed without redoing the work. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it.

- The Network and how to run it.
    1. New transactions are broadcast to all nodes.
    2. Each node collects new transactions into a block.
    3. Each node works on finding a difficult proof-of-work for its block.
    4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
    5. Nodes accept the block only if all transactions in it are valid and not already spent.
    6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
- To keep creating more coins and thus new nodes to support the network, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. The incentive may help encourage nodes to stay honest
- Saving diskspace without breaking the previous block's hashes (or breaking the chain) 'transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored'.
- A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in.
- To allow value to be split and combined, transactions contain multiple inputs and outputs. there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.
- privacy can still be maintained by breaking the flow of information by keeping public keys anonymous. Ie The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.

Video from Coursera

- Hash properties, hashes must be collision-free, can be hidden, and are puzzle-friendly.
- Collisions do exist, but the idea is to make sure they cannot be found.
- For hiding, you need to make it impossible to find the hash value by due to making it is a very high distribution of values. (High min-entropy means that the distribution is "very spread out", so that no particular value is chosen with more than negligible probability.
- Puzzle-friendly: For every possible output value y, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x such that H(k I x) = y. (so if part of the input is chosen in a randomized way then it needs to be very difficult to find another value that hits exactly that target.
    - Build a search puzzle which means that you must build a mathematical problem which requires searching a very large space in order to find the solution.

  - And where there are no shortcuts
- Hash pointer: pointer to where some info is stored and cryptographic hash of the info. With a hash point we can ask to get the info back and verify that it hasn't changed (much like what Nakamoto's paper about ecurrency discusses). The idea is that you can build data structures with hash pointers.
- Decentralized identity management: anybody can make a new identity at any time. You can make as many as you want! no central point of coordination - these identities are called "addresses" in Bitcoin (ie a public key or hash of a public key)
- When it comes to privacy, Addresses are not directly connected to real-world identity. But observers can link together an address's activity over time, make inferences.

(a) Bitcoin price as of 12:16 on 23/11/2022 $16 529,30. I will use my own friend's experience. Just after the pandemic hit, my high school friend used some of his profit from selling his house to purchase 10 BTC when they dropped from 16k to below 5k some time in march 2020. He bought 10 BTC on March 13 at $5183 a coin (so roughly $52k). He never sold them but I could say he has been crying to that he 'lost' from the peak of $64k. (so, theoretically he has lost 10*$64k = $640k, vs current 10* $16,5k = $165k, hence 165-640 = $-475k. (but I always remind him that he is still up from $52k, +$113k).

I have a better story. One of our first CEOs either purchased or mined BTC – I don't remember which – but might be both. Because at a dinner we learned that he invested around $1,250,000 in 2013 for about $120 (around 10,416 coins). He sold it all in 2017 in bits and pieces from $9000 to $16000 netting $130-$135m over the course of a few months or weeks. He lives in Singapore now and works as a private business consultant to only C-suite and board members for no less than $8000 per hour, while owning a building that he rents out apartments and shops.

(b) A Block chain in my own summarising and simplest form is a verified, secured, unchangeable transaction between nodes (or people) that is hashed then secured with public keys and private keys as they move forward. It's like a contract or document that cannot be altered no matter how far back you go.

(c) The most popular altcoin is Ethereum. Its claim to fame is that it focuses on smart contracts (self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code.)[i] and it is actually a code programmed with its own language whereas Bitcoin is only a ledger that records transactions in common coding language. Ethereum can also be an executable file. Ethereum also has a much faster execution time (seconds) vs Bitcoin which can take minutes. Finally, recently Ethereum to proof-of-stake (a set of interconnected upgrades that will make Ethereum more secure and sustainable)[ii] vs Bitcoins' proof-of-work which is highly energy intensive and thus not supportive of sustainable agenda.

Hani Mebar, **Assignment 4**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
24/11/2022

[i] Frankenfield, Jake March 24, 2022, Investopedia, URL: https://www.investopedia.com/terms/s/smart-contracts.asp, accessed 23/11/2022

[ii] Reiff, Nathan, Oct 04, 2022, Investopedia, URL: https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp, accessed 23/11/2022