Hani Mebar, **Assignment 5**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
01/12/2022

H5 Detective CoinBit

x Read/watch and summarize. (Some bullets is enough)

- Felten et al 2015: Bitcoin and Cryptocurrency Technologies, videos Week 2 (about 1 hour 20 min). Requires free registration. If you find it easy to follow, you can also optionally look at week 3 which goes to detail about blocks and networks you had some questions about.

a) Detective Coinbit. Find and analyse a BitCoin transaction. Voluntary bonus: what else have the related parties done?

b) Dashboard of Doom. Look at and comment Miko Hirvelä's crypto mining dashboard. Explain the current state of cryptocurrency mining. Relate your explanation to Miko's presentation and dashboard. What possible scenarios do you see for cryptocurrencies in the future?

Answers

x) Centralization and Decentralization of Bitcoin

Technical aspects of Bitcoin's decentralization

- Who maintains this ledger of transactions?
- Who has authority over which transactions are valid?
- Who creates new Bitcoins?
- Who determines how the rules of the system change?
- And how do Bitcoins acquire exchange value?

Even though the underlying protocol is decentralized, services that develop on top of it may be centralized or decentralized to varying degrees.

Three different aspects of Bitcoin and where they fall on the centralization, decentralization spectrum.

1. Peer to peer network is the closest thing to purely decentralized. Because anybody can run a Bitcoin node, and there's a low barrier to entry.
2. Bitcoin mining, which is not quite as decentralized because there has been a high centralization or a concentration of power in the Bitcoin mining ecosystem.
3. Updates to the software. A Bitcoin node will look at the Bitcoin specification, and some might even create their own software, so this encourages a purely decentralized system.

Distributed consensus is the key puzzle that must be solved to build a distributed e-cash system. The main challenge is reliability in distributed systems because there may be 1000s or millions of servers and if one fails, then the data is impossible to retrieve due to inconsistency in the database. But if they all fail to receive that data at the same time, then it would ask the user to try again; in the former example the user would have no idea. So this is the main reason for the need or existence of distributed consensus.

Hani Mebar, **Assignment 5**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
01/12/2022

Altcoins are systems built on Bitcoin-like principle but with different goals (could be currency system, could be digital contracts, etc)

Goal is for consensus to be on
1) which transactions were broadcasted, and
2) the order in which these transactions happened.

How consensus could work in Bitcoin is if all the nodes in the peer-to-peer network had a sequence of blocks of transactions that have reached consensus.

This is not exactly how Bitcoin works because it is a really hard technical problem, for a variety of reasons.

- Nodes might crash
- nodes might be malicious.
- the network is highly imperfect in a peer-to-peer system.
- Not all pairs of nodes are connected to each other.
- There could be faults in the network because of poor Internet connectivity and so on.
- A lot of latency in the system, because all of these things happen over the Internet.

A difference from how traditional distributive consensus algorithms operate is that nodes in Bitcoin do not have long term identities. Reason is it's more pragmatic and is much more secure. When in a unregulated decentralized model, there is no central authority that verifies identities or ensure that nodes aren't being created at will, hence this is the most secure way to carry on.

Sybil attack: Sybils are copies of nodes that a malicious adversary can create to look like there are a lot of different participants, when in fact, all those pseudo participants are really controlled by the same adversary.

Implicit consensus: as there is no consensus algorithm or vote between nodes, then a node unilaterally proposes what the next block in the chain is going to be, thus it is implicit and other blocks will have to either accept it or reject it. (accepting means they just add a new block, rejecting means they will start from the block before it).

Malicious attackers will attempt to:

- Steal bitcoins – which is very very difficult to do.
- Deny service to a user by not including their node/block in any of their transactions and thus end try to "orphan" that node/block.
- Double-spend attack, what an attacker is able to transfer coins to another address also controlled by the attacker instead of to the person who's services are being purchased and if the long-term consensus chain ends up including it the malicious spend. But if it doesn't getin the long-term consensus chain then the double-spend probability decreases exponentially with the number of confirmations.

Can we give nodes an incentive for behaving honestly? can we reward the nodes that created all these blocks that did end up on the long-term consensus chain?

- Not really, because nodes don't have an identity. So to get more nodes, we need to create an incentive and in this case that incentive is currency, or bitcoin which is also the distributed consensus process.

Hani Mebar, **Assignment 5**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
01/12/2022

Block Reward (the incentive): the node that creates each block gets to include a special transaction in that block; the special transaction is a coin creation transaction.

- How to provide incentive for honest behaviour? by ensuring validity only occurs when the block ends up on the consensus chain

- There is a finite amount of Bitcoin that will be created: only 21million, and currently it's expected to reach this goal by 2140.

- What is a transaction fee? A person can choose to make the output value of a coin less than the input value.Whoever creates the block that first puts that transaction into the block chain gets to collect that transaction fee; it is voluntary.

- So what is Proof of Work? Each block is created by solving puzzles. As the hashes get larger and more complicated you need more computing power to solve the puzzles, each solution is a proof of work and thus generates a block (which contains the new hash, old hash and all old transactions, and this string gets ever longer). 6 blocks further in the consensus chain is the commonly used heuristic that makes a bitcoin 'legit'.

- The mining reward that the miner gets is in terms of the block reward and transaction received fees vs what it costs them to create this block (which is typically the cost of electricity and the hardware setup). Costs can also come from the ratio of the power of the miners hardware to the rate at which they find blocks. And also the exchange rates .

- The truth within Bitcoin : the Bitcoin peer to peer network as recorded in the block chain, considers
- me the sum total of all my addresses to own a certain number of bitcoins. Ownership of Bitcoins is nothing more than other nodes thinking that I own a certain number of Bitcoins.

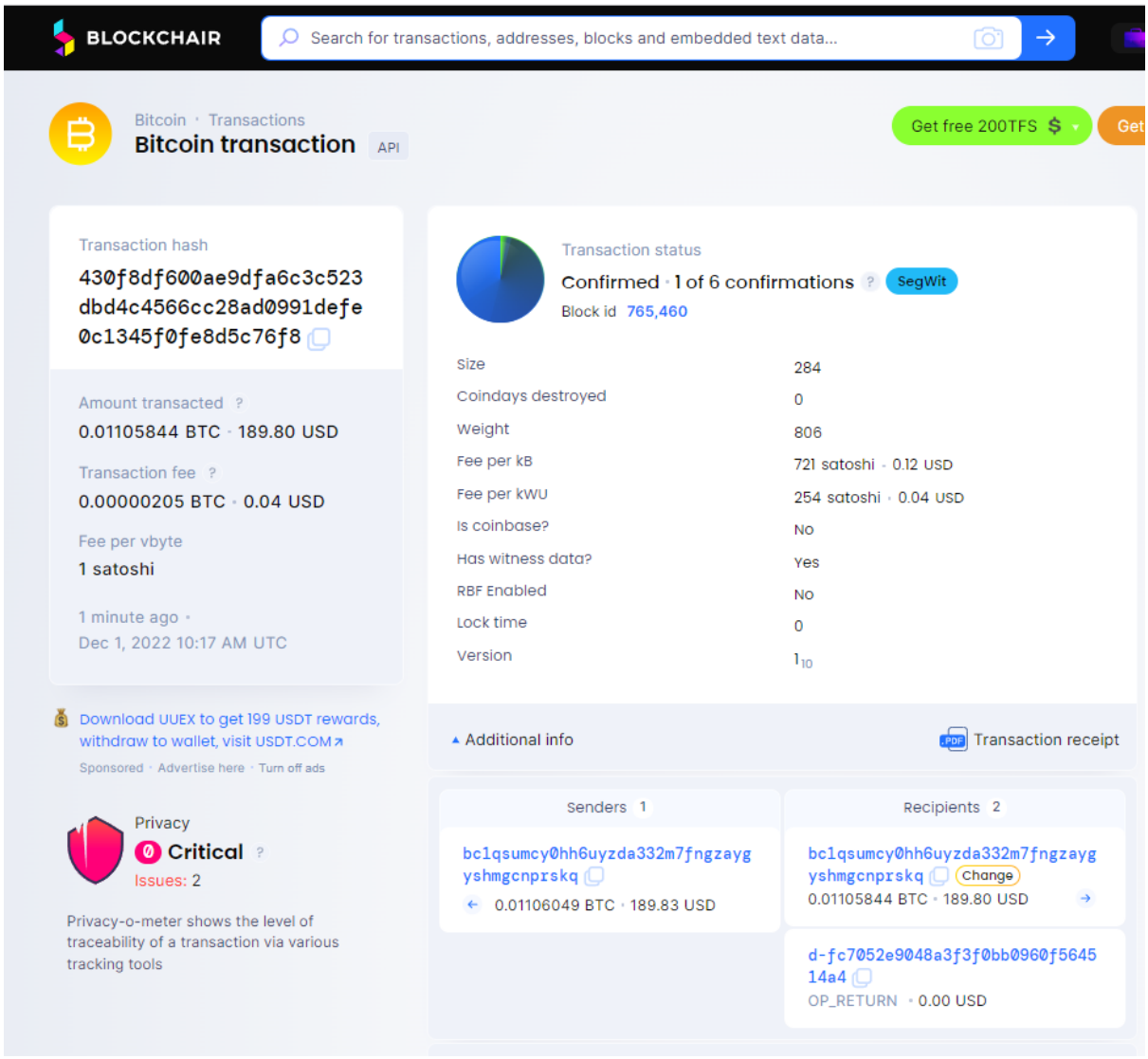
- Bitcoins or ecoins blockchains need to be
  1. Secure: the consensus chain cannot be overwhelmed; an attacker not be able to get 50% or more of the new block chain creation.
  2. Having a healthy mining system, or honest protocol-following nodes
  3. Incentive and desire to create more bitcoin.

- A fork in the chain is when a block is not accepted by other nodes and instead continue creating blocks attached to the last or previous valid or accepted block at the network.

- Can an attacker suppress some transactions? They can refuse to build upon blocks that contain transactions from a node or user they don't like. However the attacker can not prevent these transaction from being broadcast to the peer-to-peer network. Because the peer to peer network doesn't depend on the block chain, doesn't depend on consensus, and assuming that the attacker doesn't fully control the network, then the transactions are still going to find a way to reach the majority of nodes.

A) Print screen of a bitcoin transaction below:[i]

Hani Mebar, **Assignment 5**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
01/12/2022



Analysis:

- only 284 bits in size, the fee ‘tipped’ is per byte and they costs 1 satoshi per vbit, and equated to 721 satoshi per kiloByte, and 254 satoshi per kiloWattUnit.
- The exchange at the time yielded $0,12 cents + $0,04cents respectively.
- One thing I cannot determine is the sender and recipient. The sender seems to have made themselves a recipient but also created a new hash or wallet? I can’t be sure.
- In any case, the amount in Fiat currency was $189,83 minus $0,04 cents in transaction fees.

b) core is getting hot on Rig 1[ii]

Hani Mebar, **Assignment 5**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
01/12/2022

Rig 1

	Hashrate	Core Temp (°C)	Mem Temp (°C)	Fan (%)	Power (W)
RX 5700 XT MSI	98.13 MH	35	80	36	91
RX 5700 XT Gigabyte	99.10 MH	45	76	35	91
RX 5700 XT PowerColor	98.80 MH	42	64	31	93
RX 5700 XT ASUS	99.08 MH	33	78	35	83

[i] Bitcoin Transaction, 2022, URL https://blockchair.com/bitcoin/transaction/430f8df600ae9dfa6c3c523dbd4c4566cc28ad0991defe0c1345f0fe8d5c76f8, accessed 01 December 2022

[ii] Hirvela, Miko, 2022, Mining Dashboard, URL: https://mikohirvela.fi/cryptomonitoring, accessed 01 December 2022