# h5 Detective CoinBit

## Bitcoin and Cryptocurrency Technologies (Felten 2015)

* Centralization vs. Decentralization:
  + Systems are not purely centralized or decentralized
  + Relating to bitcoin’s decentralization there is five different questions:
    - Ledges maintainer of transactions
    - Authority of valid transactions
    - Bitcoins creator
    - The authority of system change
    - Exchange value acquirer of bitcoin
  + Software Wallet in use when bitcoins are changed into other currencies
  + Peer-to-peer connection as a part of bitcoin’s decentralization

## Distributed Consensus

* + Decentralizations keyword is consensus, more specifically distributed consensus which is used to build distributed e-cash system
  + Peer-to-peer connection in Bitcoin system distributes transaction to nodes in the peer-to-peer network as GoofyCoin system does
  + Hash pointers used to point out transactions
  + Block chain used to optimize system efficiency as ScroogeCoin does
  + Several issues and risk in this system. For example. system crash or it could be malicious
  + What bitcoin does differently in other systems is using incentives
* Consensus without Identity: the Block Chain
  + Bitcoin nodes doesn’t have identities. And one of the reasons is malicious identities managed by adversaries.
  + Bitcoin does not offer strong anonymity out of the box
  + Adversaries might try to steel bitcoins using forged signatures which is not possible, or adversary can simply not include some specific transactions into block using sender’s address information.
  + Double spending problem decreases after exponential confirmations
  + Double-spending attacks look in a system kind of identical from signature perspectives but consensus after all decide which transaction ends up in consensus.

## Incentives and Proof of Work

* + Incentive engineering in bitcoin
  + Two separated incentive mechanism: block reward and transaction fee.
  + Block reward is special transaction created by coin creation process. Kind of payment exchange in consensus.
  + Transaction is only valid if it gets into block chain
  + Transaction fee is kind of fee to block creator to get the fee after putting the transaction into a block chain
  + Proof-of-work: one way to do the POW is pick nodes in proportion on the computing power or alternatively picking nodes by an ownership of currency.
  + Bitcoin uses hash puzzles for proof-of-work concept
  + Miners computing power affects the number of winning blocks and mining as well

## Putting It All Together

* + Electricity cost in mining is eventually higher than front costs of the hardware, partially because of its incurrent over time.
  + Pseudonymous key pair can be created by any who at any moment and any number of them
  + Bitcoin transactions are messages to peer-to-peer network
  + The coin is a set of transactions to call anything in Bitcoin to an actual coin
  + Miners competing block creations to earn by that way
  + At the end of bitcoin transactions, to make transaction without fearing intrusion or pledge is safe and the possibility of money lost is very low.

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

* + 1. Online merchant decides to accept bitcoin payments
    2. A buyer has bitcoins to make a purchase
    3. The merchant and the buyer have bitcoin wallets which access to multiple addresses
       - Addresses are like bank accounts but work little bit differently. Bitcoin users can create as many addresses as possible
    4. The merchant creates a new Bitcoin address for the buyer to send a payment
       - In practise, the merchant creates cryptographic key pair, composing a private key and a unique public key. Anyone who has a valid private key can verify the payment
    5. The buyer submit payment to telling her client to transfer bitcoins to merchant
    6. The buyer holds private keys for all addresses owned
    7. The bitcoin client signs the transaction request with private key of the address transferred bitcoins from
       - Anyone on the network can use the public key to verify that the transaction request comes from legitimate owner of the transaction
         * The public key is used to receive bitcoins
         * The private key is used to sign transactions to those bitcoins
    8. Bitcoin miners bundle the transaction into new transaction blocks
    9. Hashes are cryptographic functions used transform a collection of data to fixed length a hash value
    10. Nonces are used to create hash values
    11. The mining computers calculates new hash values based on combination of previous hash value, new transaction block and a nonce.
    12. The block includes a “coinbase” transaction that pays certain number of bitcoins to the miner
    13. The miner is also awarded with fees, paid by transaction sending users.
        - The fee is incentive for the miner to include the transaction in their block (Crypto.com 2022)

## 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?

* Current state of cryptocurrency mining (Hirvelä 2022)
  + State of mining is currently unstable, and it may change fast. I would say that the state comes more unstable in a future. Because of new innovations relating to the scene. New tools and new innovations make the mining business careful mode, and the investors and miners need to put more and more focus to seek what’s happening there in the future market.
  + Cryptomining for regular net user might be tricky and need interests into the topic to fet to success level in mining. Especially, if user wants to collect and analyse data of mining. Instead of collecting data in one repository as Miko does for analyses purposes, there is possibility to use different applications and combine all data that way.
  + Mining requires efforts to build system and hardware, particularly, graphic cards and high CPUs are needed, which are known of high price on market. Top market leader graphic card prices are approximately 2000€ per card or even more.
  + Miko’s crypto Mining Monitor’s analytic counts revenue and profit as daily basis, and the value seems to be negative for the day 27.11.2022. Profit for the previous 24 hours is -1.37 euros.

## Sources:

Crypto.com, 2022, How Do Bitcoin Transactions Work?, [How Do Bitcoin Transactions Work? (crypto.com)](https://crypto.com/university/how-do-bitcoin-transactions-work#:~:text=The%20transaction%20is%20verified%20by,as%20valid%20by%20all%20participants.) Read: 27.11.2022

Felten, 2015, Coursera, How Bitcoin Achieves Decentralization, [Consensus without Identity: the Block Chain | Coursera](https://www.coursera.org/learn/cryptocurrency/lecture/71F3l/consensus-without-identity-the-block-chain) Read: 26.11.2022

Hirvelä, M. 2022, [Homepage (mikohirvela.fi)](https://mikohirvela.fi/index) Read: 27.11.2022