Topic 8 - Blockchain

- Explain the characteristics of the blocks in a blockchain (e.g.: immutability, linear growth)
- Explain how the crypto tools used in blockchain work (hash function, signature, merkle tree, hash pointer) and how they are used in the blockchain
- Explain why Paxos consensus is not enough for a blockchain, e.g.: to protect against the double spending conundrum
- Bitcoin: explain the structure of the transaction and how they are verified by the miner
- Smart contracts: discuss the gas prices for different primitives, e.g.: for Solidity

Material: blockchain slides, Bitcoin paper, Solidity tutorial (lecture 13)

The Blockchain

The Blockchain is a digitized, decentralized public ledger of cryptocurrency transactions.

Block Characteristics

A block

- ** Blocks are the individual "links" of the chain of transactions.
- ** A block designates a single transaction
- ** A block is typically composed of the following elements:
    - ** Data
    - ** A hash pointer
    - ** A timestamp
- ** Blocks are added to the chain, the chronological lists of transactions.
- ** This allows participants to keep track of the transactions, without a central recorded database.

How Crypto tools used in blockchain:

Crypto tools ensure the integrity of the blockchain

How they Work

Hash functions

- A hash functionHtakes binary input of arbitrary length, and creates fixed-length output of it.
    - ** $H:X=\{0,1\}*\to\{0,1\}L$
    - typically where $L \in \{128,160,256,512\}$
- **For security purposes, it is important that a small change in the input results in a large change in the output.
  Collisions exist, but they are hard to find with this property.

Merkle Trees

- **Merkle trees, or Hash trees, which are a data structure for summarizing information about a collection of data, with the intent of checking the content.
- ** Is a combination of hash functions with the binary tree structure.
- ** Uses a Hash function H (SHA1, MD5)
    - ** Leaves are H applied to the initial symbols.
    - ** Internal nodes are H applied to children of a node.

How they are used

Asymmetric Cryptography allows users of the blockchain to both sign and verify blocks.

- ** Keygen, an algorithm which returns two keys;
    - a public key, used to identify the user
    - A private key, which is used to apply a signature to a transaction, to express consent
- ** Sign, An algorithm which computes the signature of som input, based on the secret key, and some data (typically a hash)
- ** Verify, Decrypts the signature using the public key, and compare the result with a hash of the received data.

Paxos consensus

- **A blockchain network is completely asynchronous and decentralized.
- **For currency, this requires the solving of the problem of double-spending, i.e. being able to spend the same money more than once.
- Paxos is named after the Parliament on the fictitious Greek island of Paxos.
- Paxos is a family of algorithms (by Leslie Lamport) for distributed consensus in an asynchronous system
- ** In Paxos termination / liveness is not guaranteed, but happens in “reasonable environments”
-
    - ** Different roles exist:
    - Proposer: Offers proposals, with multiple proposers at once, they instead compete to reach approval first.
    - Acceptors: Accepts or rejects proposals
    - Learners: Simply learns the agreed upon proposals
- Proposals must have majority to be accepted.
- ** Paxos Consensus works by sending a prepare request to some acceptors (other participants of the blockchain)
    - ** The acceptors accept the proposal
    - ** The proposer sends a commit request
    - ** The acceptors accept the commit.
- ** Paxos only requires a majority to accept, meaning half the participants of the blockchain can never answer, and Paxos will still work.

Bitcoin: The structure of the transaction and how they are verified by the miner

Transactions

- ** A transaction contains the following data:
    - **A list of input transactions

    - **A list of tuples of the recipient public key, and the amount to send.
    - **Personal signature, signed with private key
- In order to verify a transaction, one must:
    1. Verify the signature using the public key of the sender
    2. Verify the signatures of each of the input transactions
    3. Ensure that the money has not been spent between the input transactions and the new transaction.
- As transactions are signed using the private key, only the owner of the identity can transfer the money from that point.
- A single user can have any number of identities.

Miners

A miner does the following:

1. Verify all the transactions by looking that input transactions are covered and properly signed
2. Compute the Merkle root hash for the transactions
3. Solve the puzzle on the previous block, for immutability
4. Broadcast the new header
5. Go on collecting new transactions for next blockMiners receive compensation for computing the next block.

Smart Contracts: gas prices for different primities, Solidity

- Smart contracts are computer protocols that facilitate, verify or enforce the negotiation or performance of a contract, or that make a contractual clause unneccessary.
- The rules are penalties are defined around an agreement, same as with traditional contracts, but automatically enforces those contracts.
- Smart contracts are code that are added to the blockchain.

Ethereum

- Ethereum is a smart contract based blockchain. Contracts live in the distributed network, and has its own balance of Ether, the currency/ fuel, memory and code.
- Every time a transaction is sent to a contract, the code for the contract is executed
    - The contract can perform transactions, store data and interact with other contracts.
- To run contracts, a transaction with Ether is made to the contract, optionally with additional input.
- The contract runs until it completes or runs out of Ether.
- Ether is awarded to the winning miner.
- Each miner runs the smart contract, and produces the same output.

Solidity

- An object oriented language for implementing smart contracts.
- Used in Ethereum.