Chapter 1

Introduction

1.1 Blockchain definition

Blockchain is a list of records, called *blocks*, that are securely linked together using cryptograhpy. Each block contains a cryptograhpic hash of the previous block, a *timestamp* , and transaction data, generally represented as a *Merkle tree*. The timestamp proves that the transaction data existed when the block was published to get into its hash.

This structure allows for the datastructure to be immutable, and provides a linear forward history.

1.2 Blockchain vs Distributed Ledger Technologies (DLT)

Blockchain is a type of DLT i.e. not all DLTs are blockchain.

A DLT is a decentralized database that is managed byvarious participants. There is no central authority that acts as monitor. Similar to a blockchain.

The main difference between Blockchain and DLT is that a Blockchain shares its records via blocks , cryptograhpically protected blocks, i. e. a specific application of a DLT.

Chapter 2

Introduction to Bitcoin

2.1 Identity

Identity is required for

- Sending or Receiving money
- General accounting

In a similiar way as to a Home address and a mailbox key. It's important to keep it secure.

- Public key: is for receiving
- Private key: is for unlocking
- The private key is generated at Random once
- The public key is generated **from** the private key.

There a total of 2^{160} addresses possible. Each entity in Bitcoin is issued an address. The address is generated from a hash of the users' public key.

2.2 Bitcoin Transactions

2.2.1 Distributed Database model

- Everyone stores a copy of the database
- Lightweight node: Only transaction headers are downloaded to validate transactions.

2.3 Proof-of-work consensus

2.3.1 Bitcoin Security

Example double spend attack.

We protect ourselves with timestamps.

Blockchain Forking: The longest chain is accepted as valid.

2.4 Cryptography in Bitcoin

2.4.1 cryptograhpic hashing functions

A function with these properties

- Preimage resistance
- Second preimage resistance
- Collision resistance

Theorem 1 ***Preimage resistnace:*** *Calcualate the preimage of an output is almost imposible*

Theorem 2 ***Second preimage resistance:*** $\forall x$ *it is computationally difficult to find some value* x' *such that* $H(x) == H(x')$

Theorem 3 ***Collision resistance:*** *It is computationally difficult to find* $x \wedge y$ *such that* $H(x) == H(y)$

Bitcoin uses the SHA-256^2 method hash function, which consists of applying the SHA-256 to the output of a SHA-256: $SHA\text{-}256(SHA\text{-}256(x))$

2.4.2 The Bitcoin block header

A Bitcoin block consists of two parts **The header** and **The data**. Similar to an IP packet.

The Header is composed of:

- Previous block hash
- The Merkle root
- Nonce (Random number used only once)