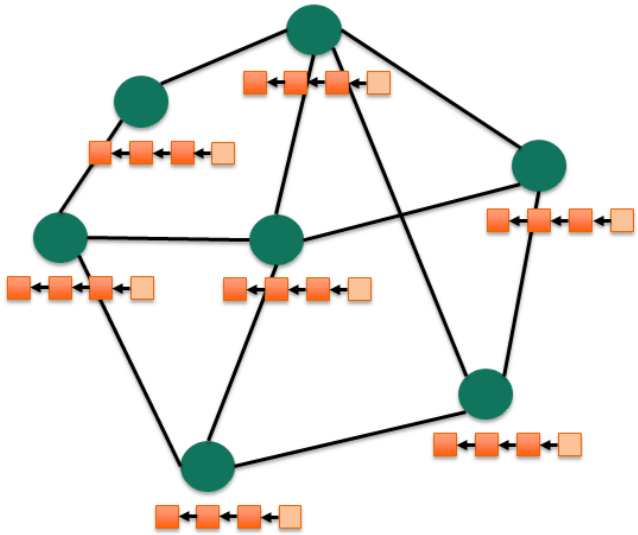
Data Analytics for the Assessment of Blockchain Technology (WiSe2021)

Thomas Rose, Kathrin Hausmann, Andrei Ionita, Timo Meiendresch, Selin Sezer

RWTH Computer Science 5, Fraunhofer FIT, B-IT

Week 5 - 27.11.2020
Blockchain Technology (1)



Fraunhofer FIT

Agenda

1. Introduction
   - Decentralization
   - Ledger/Distributed Ledger
   - What is Blockchain?
   - History
2. Cryptographic Primitives
   - Public Key Cryptography
   - Digital Signatures
   - Hashing
   - Merkle Tree
3. Blockchain Anatomy
   - Transaction & Block
   - Chain of Blocks
   - Consensus
   - Nodes & Network
4. Overview

INTRODUCTION

Who ensures the correct execution of "value transactions"?

Ledger

- A ledger is ...
  - back in the 1500s, a large volume or service book that is regularly located in one place and openly accessible.
  - turned into the principal book of accounts for a business entity.
- In modern days, ledger account for recording credits and debits separately for every business.

  → Requires two books to confirm a transaction took place.

  → ”Double Entry Ledger Accounting”
- Digital ledgers and databases can be edited, copied and transferred

- .

Distributed Ledger

- How about keeping copies of the ledger distributed on a network to overcome the weaknesses of having one ledger?
  - No authoritative copy
  - More robust system
  - But how do they work together?
  - Alignment?

Distributed Ledger

- How about keeping copies of the ledger distributed on a network to overcome the weaknesses of having one ledger?
  - No authoritative copy
  - More robust
  - But how do t
  - Alignment?

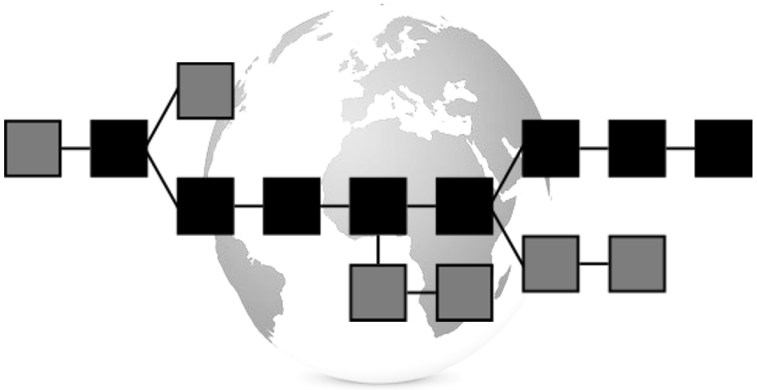
Why decentralization?

- Shift of power and authority in a community away from one central entity and making community members self-sovereign
  - e.g. BitTorrent, Bitcoin

- Potential benefits for networked systems include:
  - Less likeliness to fail
  - Harder to attack
  - Harder to exploit system's users

- Taking the value away from oligarchs back in the hands of the user

What is a Blockchain?



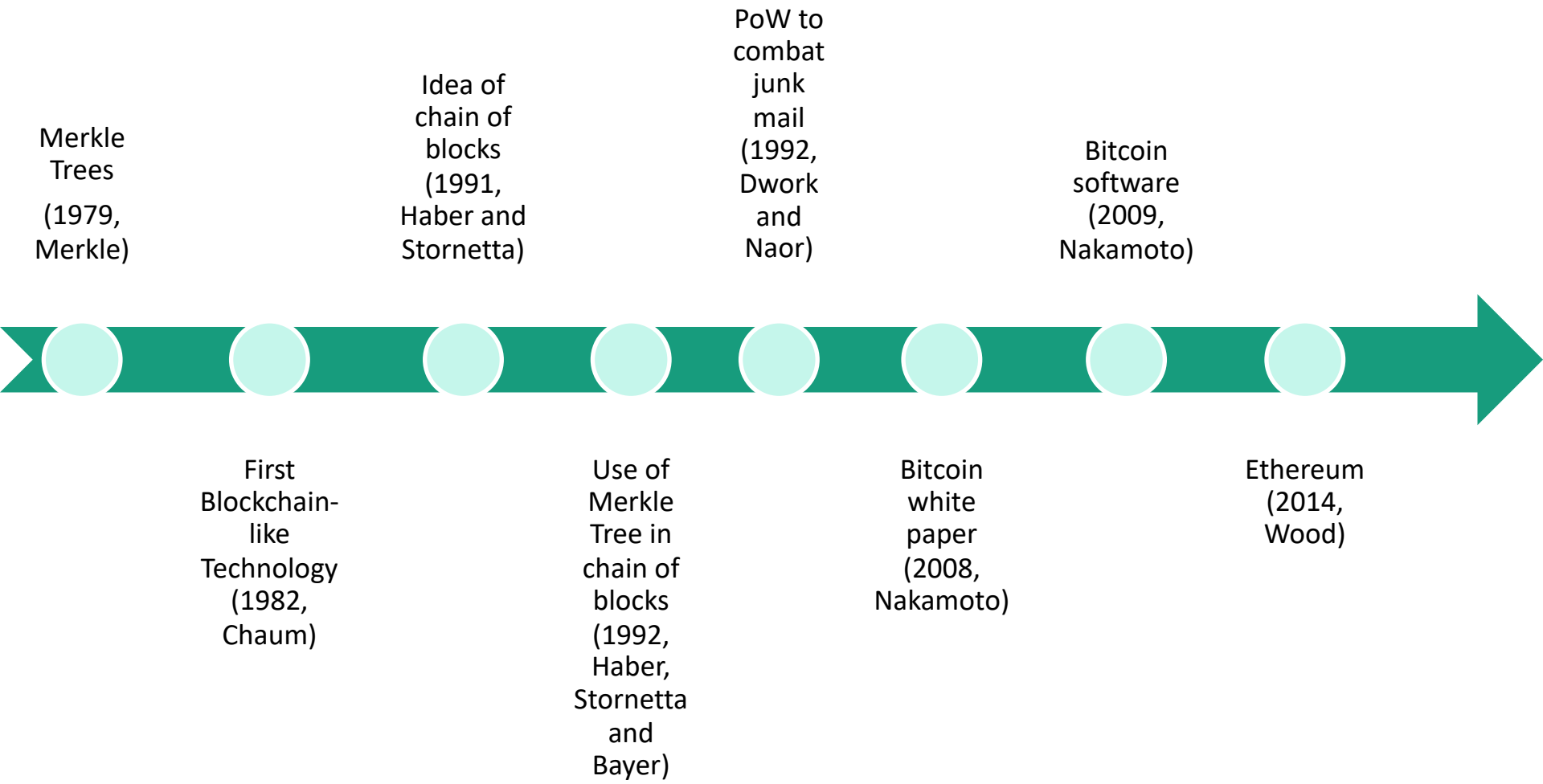
Definition

A **Blockchain** is a **distributed, decentralized ledger** that stores transactions in a manner that is **visible**, **chronological** and **unchangeable** for everyone in the network.

Attributes

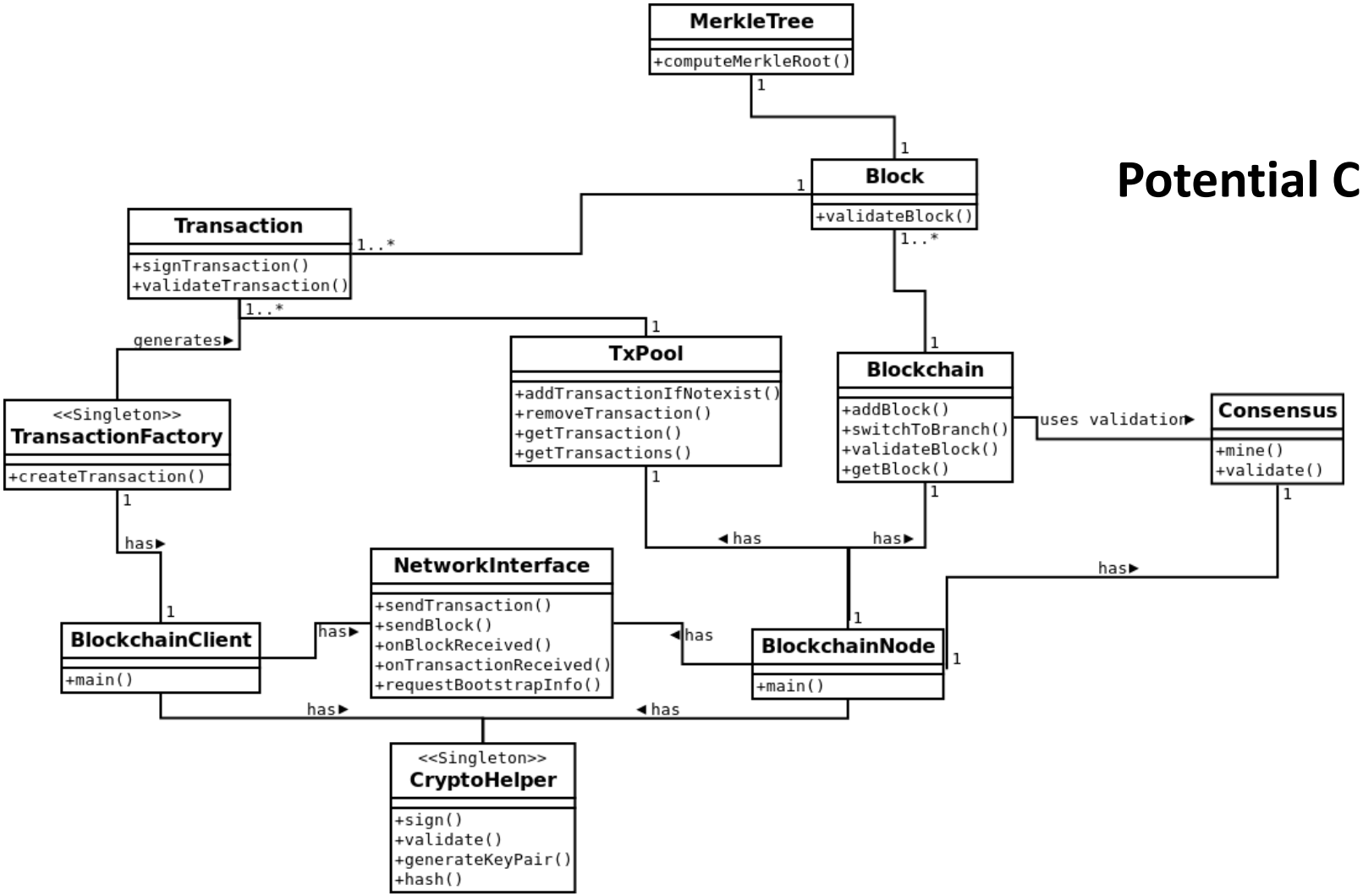
- Irreversible transactions that are confirmed in near real time
- Systems on a peer-to-peer basis carry out transactions independently and securely
- Transactions are verified by the network instead of a central authority
- All intangible documents and assets can be expressed via code and stored in the blockchain
- All transactions are known to the entire network (pseudonymity)

History



Fraunhofer FIT

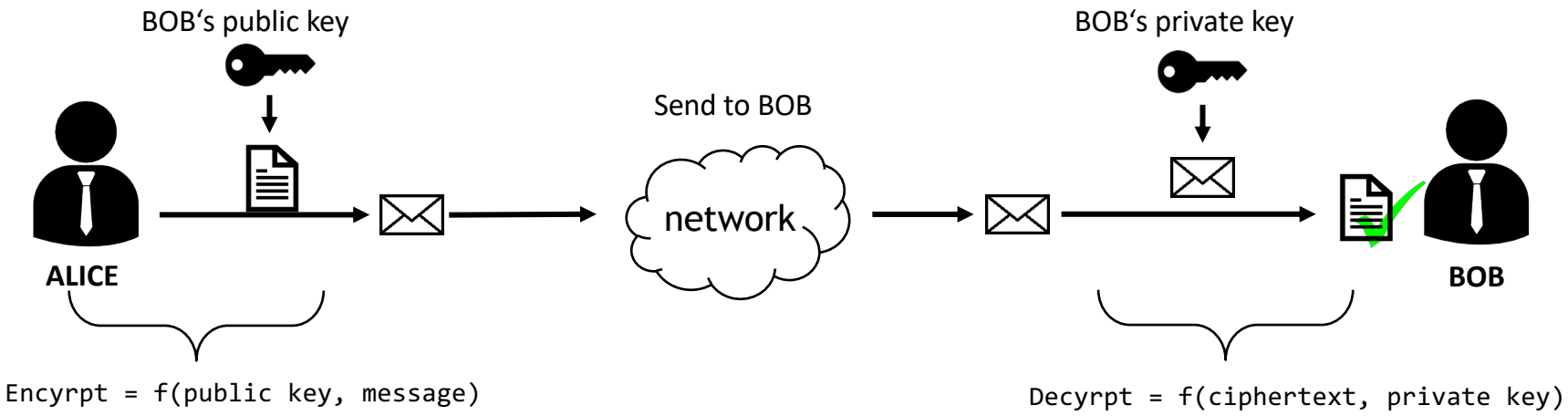
Blockchain Components



Potential Classes

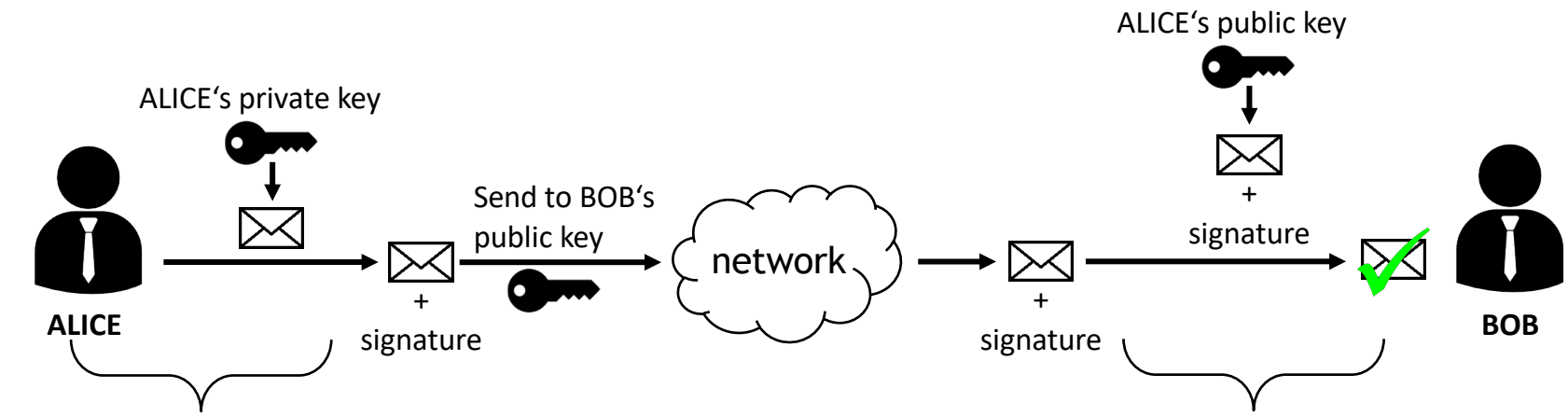
CRYPTOGRAPHIC PRIMITIVES

Public Key Cryptography



- Sender only needs to know the public key of the receiving person
- It is possible to communicate in private with someone without shared keys
- It is possible to generate public keys from private keys but it is very difficult to ”**reverse**” the algorithm to accomplish otherwise

Digital Signatures & Identities



Hashing

- Hash functions transform digital information of arbitrary content and size into fixed formats
- Output computation is efficient (For *n*-bit string -> O(*n*))
- „Sligth“ changes of the input string result in significantly different output strings
- Original information, i.e. transaction, not reproducible

SHA1 Hash of „abc“

A9993e364706816aba3e25717850c26c9cd0d89d

SHA1 Hash of „abC“

57babce0612ae7c07c380ddd1fb9d6b4c0dc1033

SHA1 Hash of „Lorem ipsum dolor sit amet“

38f00f8738e241daea6f37f6f55ae8414d7b0219

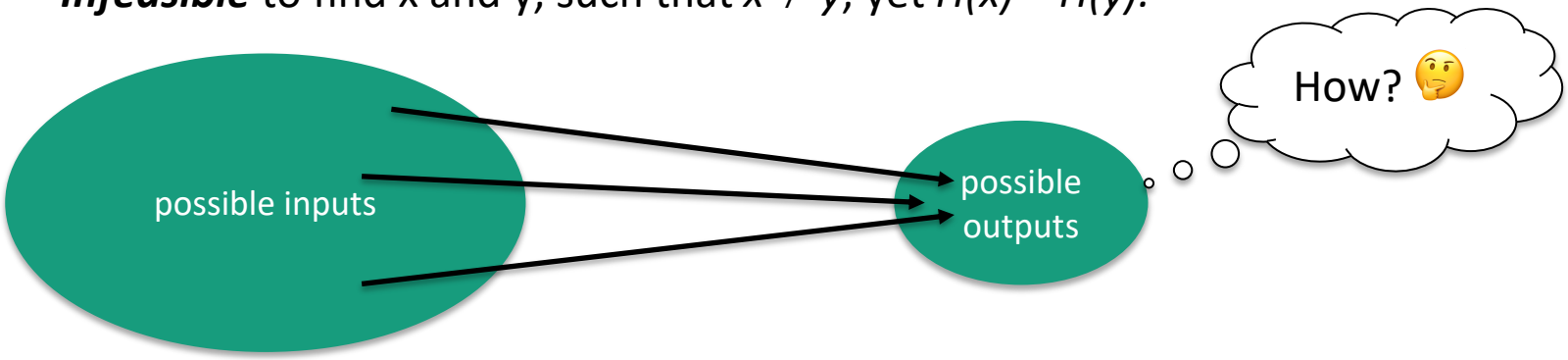
SHA256 Hash of „Thomas Rose“

4a18fa813ffc60dc893d513863c40dc4acd146e2f9c6b1983946b2435459d92a

Hashing

- Collision-resistance

  Infeasible to find x and y, such that $x \neq y$, yet $H(x) = H(y)$.



- Puzzle-friendliness

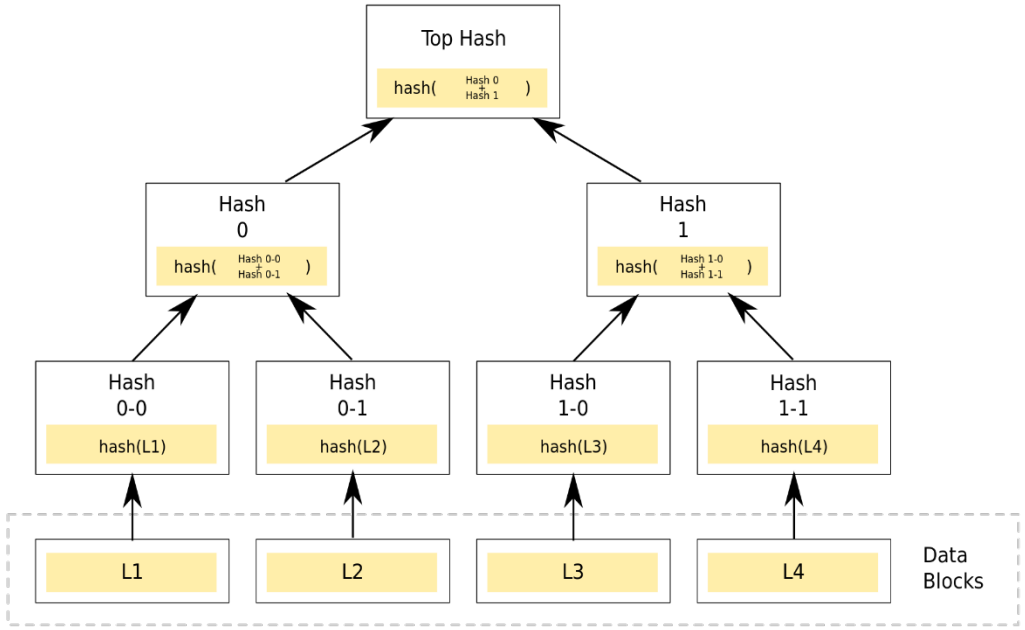
  If k is chosen in a suitably randomized way, it is ***infeasible*** to find x such that

  $H(k \,||\, x) = y$.

Merkle Tree

- Merkle trees encode the representation of *blocks* of data in a hierarchical fashion from the bottom to the top

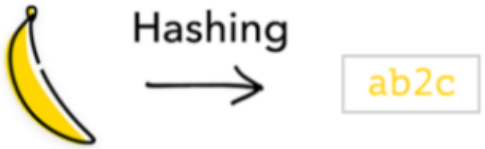
„One“ hash value represents the content of the entire block, i.e. transaction record, *uniquely* if hashing is collision-free.



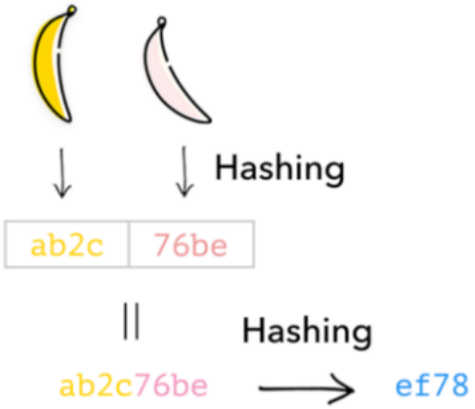
Merkle Tree

Exercise

- Let’s say a piece of information is represented by a banana.
- How can a banana be encoded?



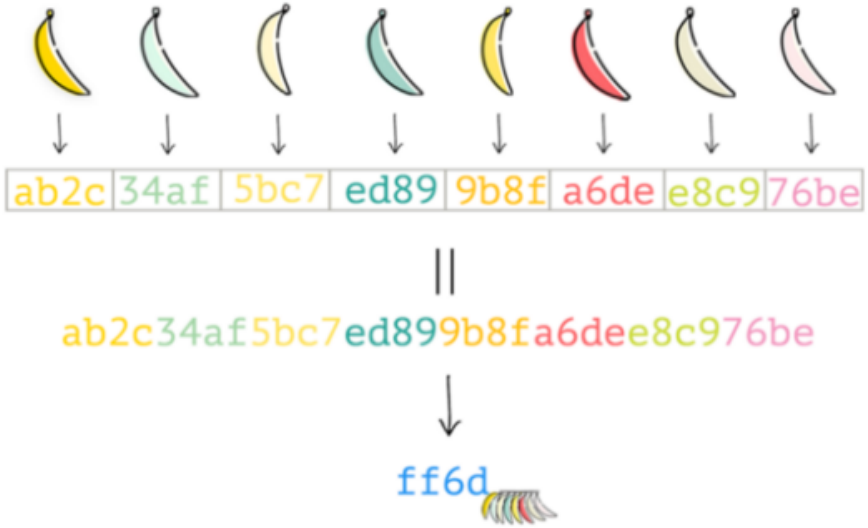
- How can 2 bananas be encoded?

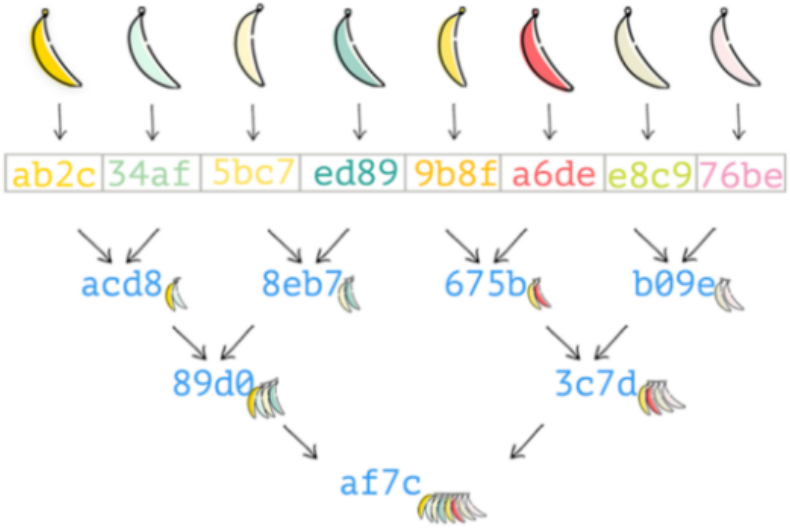


Merkle Tree

Exercise

- How can 8 bananas be encoded?

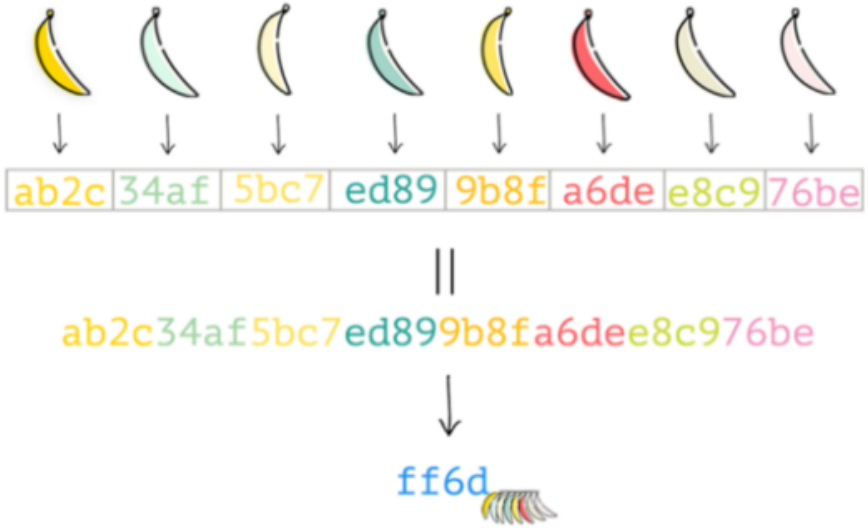


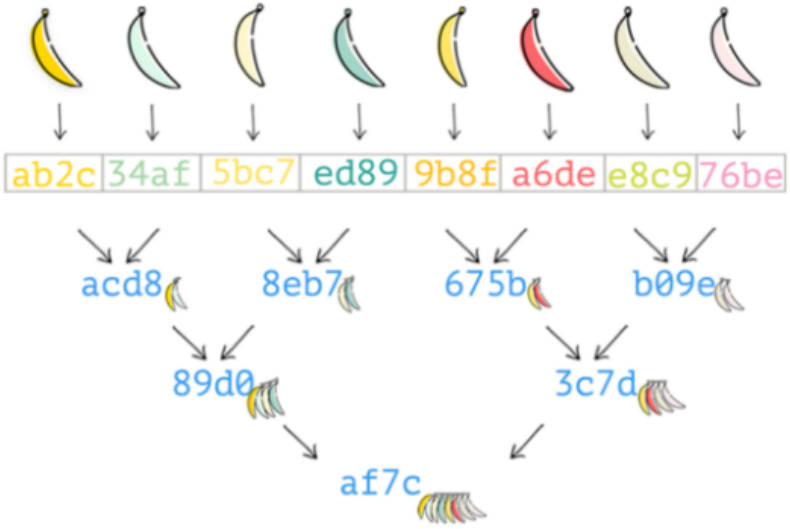


Merkle Tree

Exercise

- What kind of info do we need to verify that the red banana was used for calculating the root?

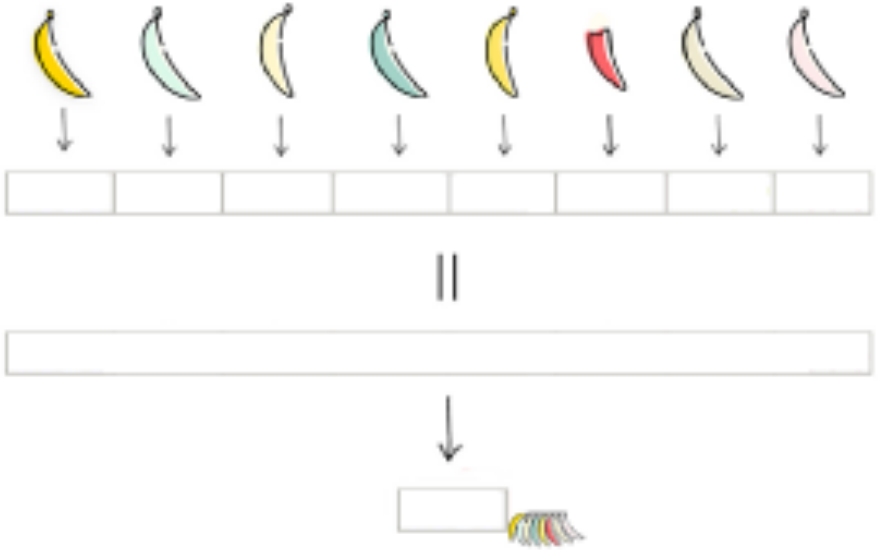


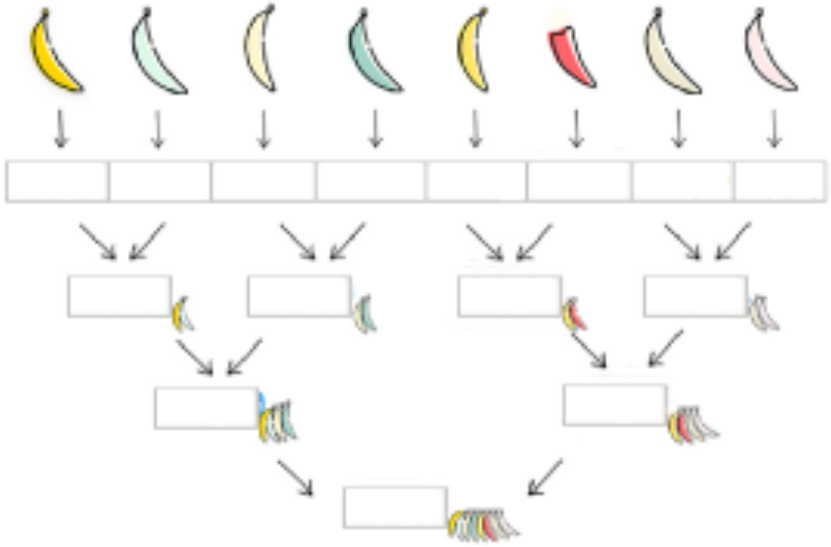


Merkle Tree

Exercise

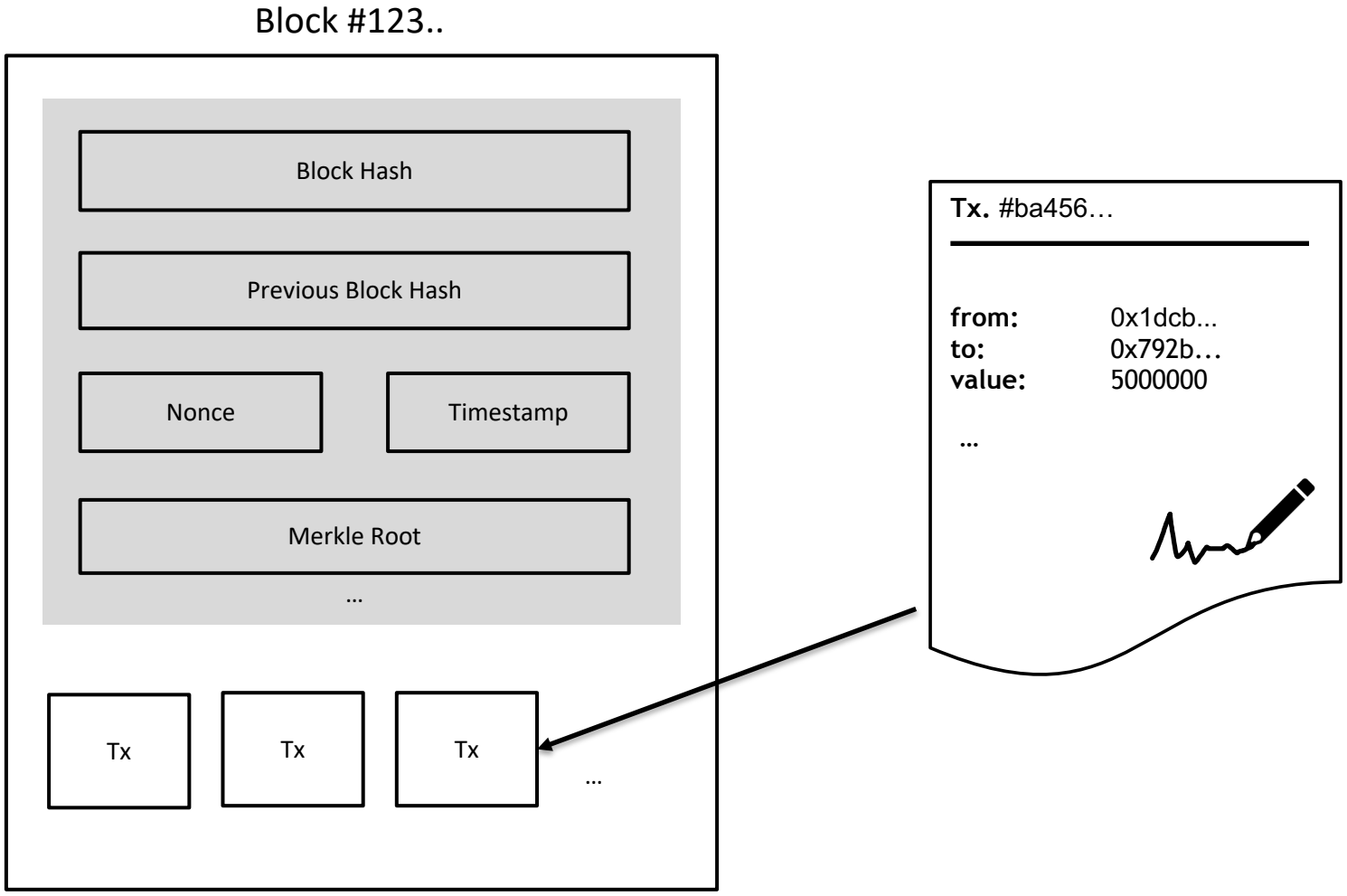
- What happens if one of the bananas has been bitten?



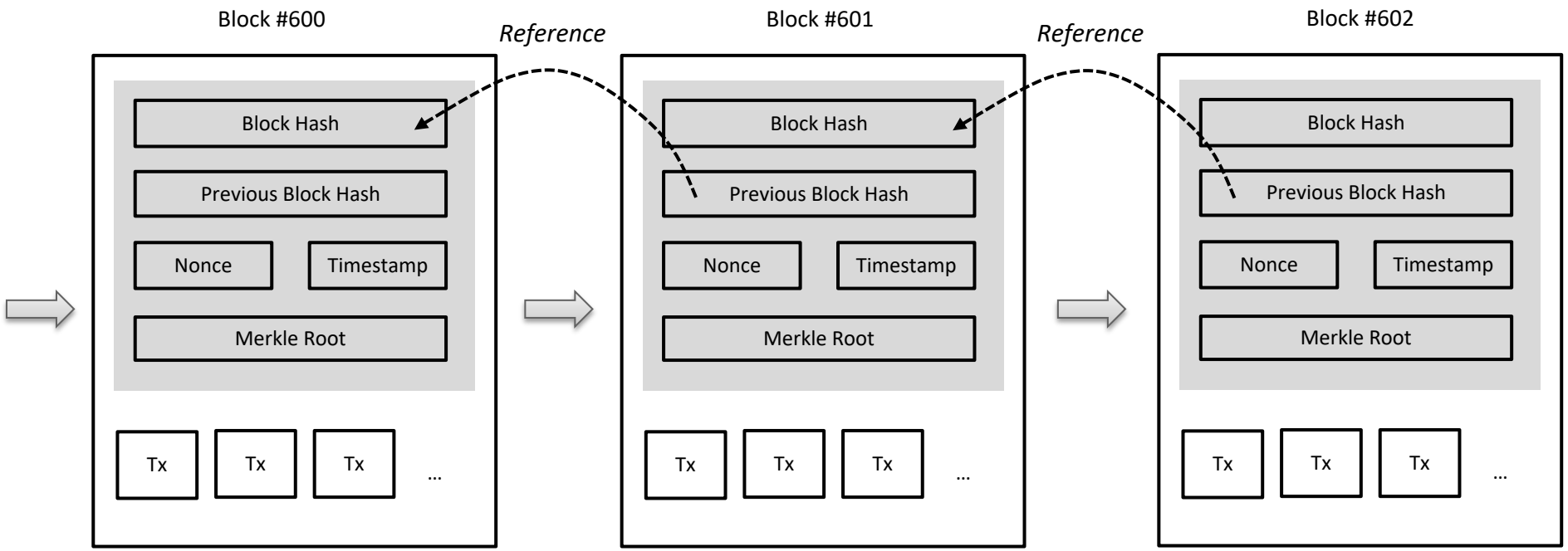


BLOCKCHAIN ANATOMY

Transaction & Block



Chain of Blocks



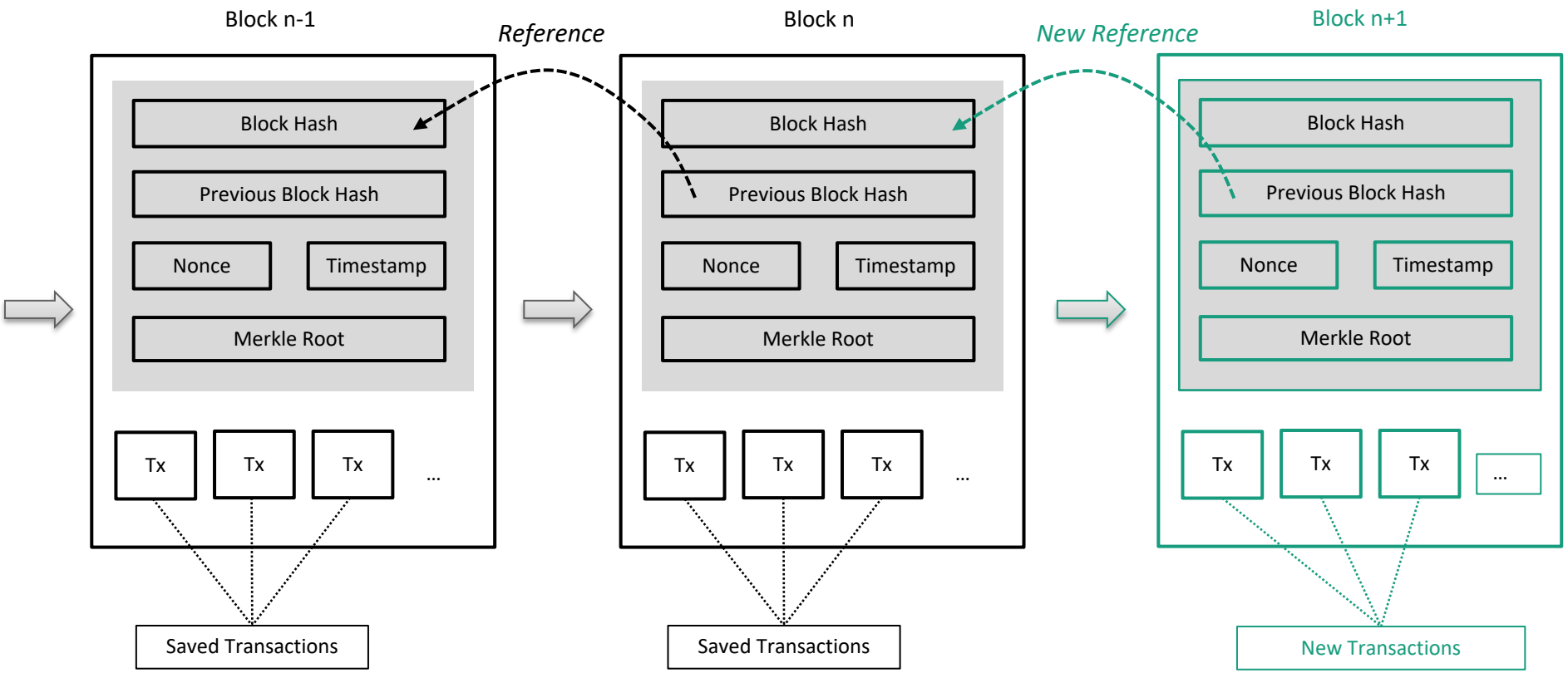
Pop-Quiz

- Which of the following can be detected?

- ☑ Inserting a new block in the middle of the blockchain
- ☑ Tampering with the content of an existing block
- ☑ Removing a block from the middle of the blockchain
- ☑ Changing the order of the blocks

Consensus Finding

Food for Thought



Consensus Finding

- Centralised transaction management comes with *one* central authority
- Blockchain technology uses the concept of *consensus finding* to verify propositions in a network of peers
- Typically cryptographic challenges are used for verifying the correctness of statements
  - The original Proof of Work for Bitcoin is based on a computational challenge required for email sending

Consensus Finding

Proof of Work & Mining

- As a proof of work, a value is searched for (**nonce**) with which a hash with the desired properties can be achieved
- A block is considered valid if the hash value of the entire block is below another threshold number (**difficulty**)
- Combination of block data and the **nonce**
- Ultimately, many possibilities are tried out with brute force

Latest Blocks

Height	Relayed By	Size(B)	Reward	Time	Block Hash
657,348	Poolin	1,114,442	6.40854787 BTC	6 minutes ago	000000000000000000214a6755b4758808b5d82b63ea81f42e0189eb733306a
657,347	ViaBTC	1,325,848	6.96946056 BTC	7 minutes ago	00000000000000000ef65ede0bb61defadae73fdde6f871fbcc1d68fcde457
657,346	Huobi.pool	1,336,908	6.71473084 BTC	22 minutes ago	000000000000000000036b8ee3dcfd3794cd2a07d01fe6ca247b0551bc2cb6d8
657,345	F2Pool	1,225,612	6.53897858 BTC	29 minutes ago	000000000000000000005286afe8fa70864296bebd7fcdbeb726b0ba180626e27
657,344	Binance Pool	1,344,894	6.93998063 BTC	32 minutes ago	00000000000000000000efb0e6dffb07b54f42f95bb3e449854d9ef1a29174640
657,343	Huobi.pool	1,227,623	6.68656505 BTC	45 minutes ago	000000000000000000000ac8dc20894133d4b7f0340f406621ca38f3da4b1565d3
657,342	F2Pool	1,269,816	7.06195944 BTC	48 minutes ago	000000000000000000000929c486b621048471aa952cfeeecab78e3a2a386eb6fd
657,341	Poolin	1,263,057	6.59567850 BTC	57 minutes ago	000000000000000000008fe195532521406ce6b846dd2dfad70abcf4de1413408
657,340	Binance Pool	1,350,328	6.72276579 BTC	59 minutes ago	000000000000000000000908833c0efdad7c0a2fa187e5d8b3be19249bb7cd9753
657,339	BTC.com	1,422,719	7.02203131 BTC	1 hour 01 minutes ago	000000000000000000000da692be52188e959cbff42c4d2c31f4566ddd0772607c

**Picture taken from https://btc.com/ (17 November 2020)*

Consensus Finding

Mining

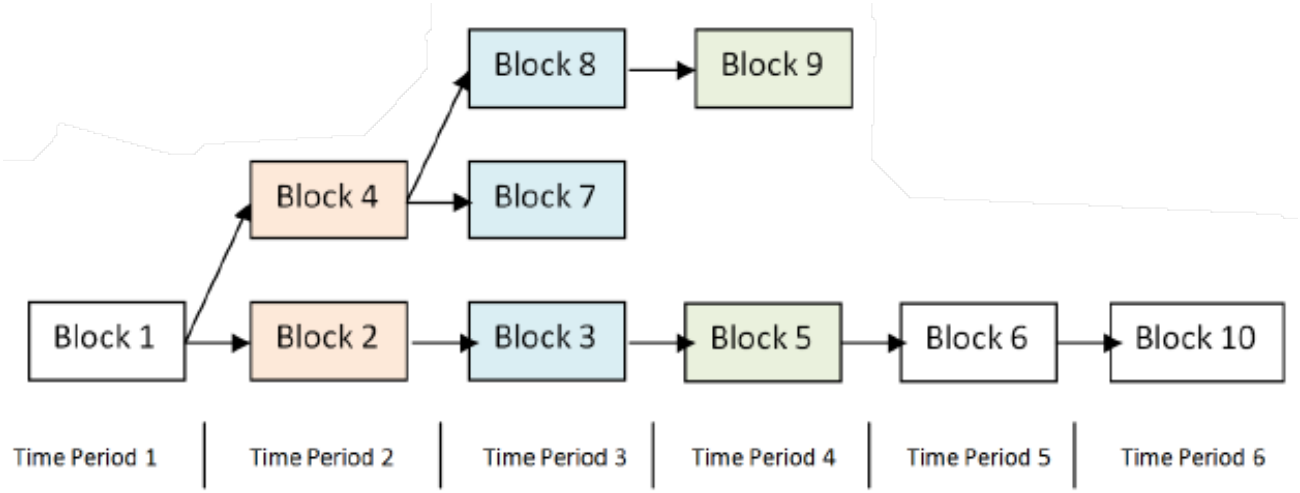
- Difficulty level can change to ensure that blocks are created at regular intervals (approx. 10 mins in Bitcoin)
- In principle, every user in the Bitcoin network can participate in "mining", but a high use of resources is necessary
- Today it is practically no longer possible to calculate this with a "normal" computer
  - Association to form **mining pools**

- **Incentive:**
  - The participant who finds a suitable nonce / proof receives a reward
  - (As of 11 May 2020: 6.25 BTC + transaction fees)

Consensus Finding

Branching & Transaction Validation

- Although the "accepted" blockchain can be seen as a list, it is best to represent the blockchain as a tree
- The longest way through the tree is the "accepted" blockchain
- By adding the transactions in a block, the network signals that the contents of the transactions are plausible
- Each new block added on the blockchain after that is considered a confirmation of the previous blocks (and transactions)



Consensus Finding

Different Implementations

Proof of Work

- Validation by solving a mathematical problem, e.g. finding the right random number to satisfy a specific condition
- Requires computing power, energy, time
- E.g. Bitcoin, Ethereum

Proof of Stake

- Validation by those nodes that hold larger amounts of money – „trust the bosses“
  - The more value a node owns, the higher is the chance to be selected
- Faster, more trust based

Consensus Finding

Different Implementations

Lottery Protocol

- Randomly selected nodes perform the validation
- Requires a trusted lottery mechanism – hardware?
- E.g. Sawtooth Lake: Proof of elapsed Time: Intel® Software Guard Extensions (SGX)

Explicit Validation Nodes

- Selected nodes have the right to validate
  z.B. BigchainDB, erisDB
- Permissioned access to the Blockchain

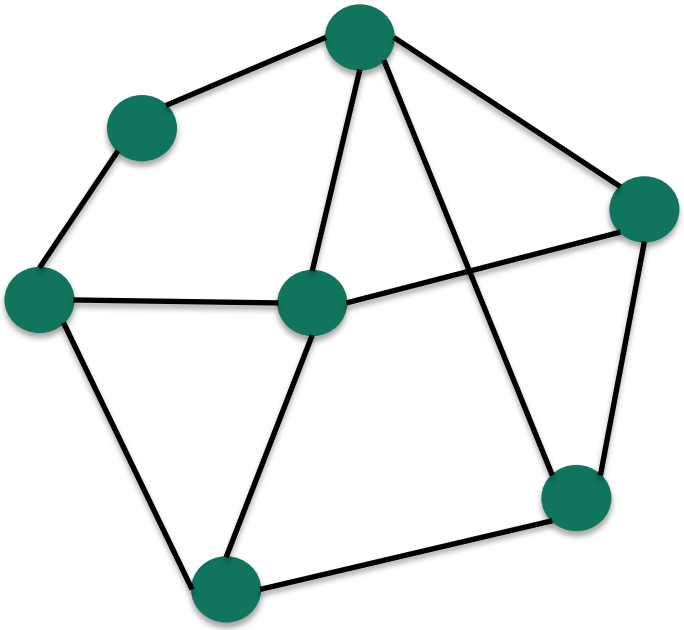
A combination of all methods is also possible!

Nodes & Network

- Nodes ←→ Computers that make up a blockchain network
- P2P Network
  - where all nodes are equal → no hierarchy, no centralized, special, master nodes
  - random nodes are peered with random other nodes
  - new nodes can come at any time
  - publishing transactions through a simple *flooding* algorithm
- Well behaving nodes ...
  - validate and propagate transactions
  - also add new transactions to their transaction pool
- But it is also possible for a node to forward ...
  - double spends
  - transactions that aren't standard or valid

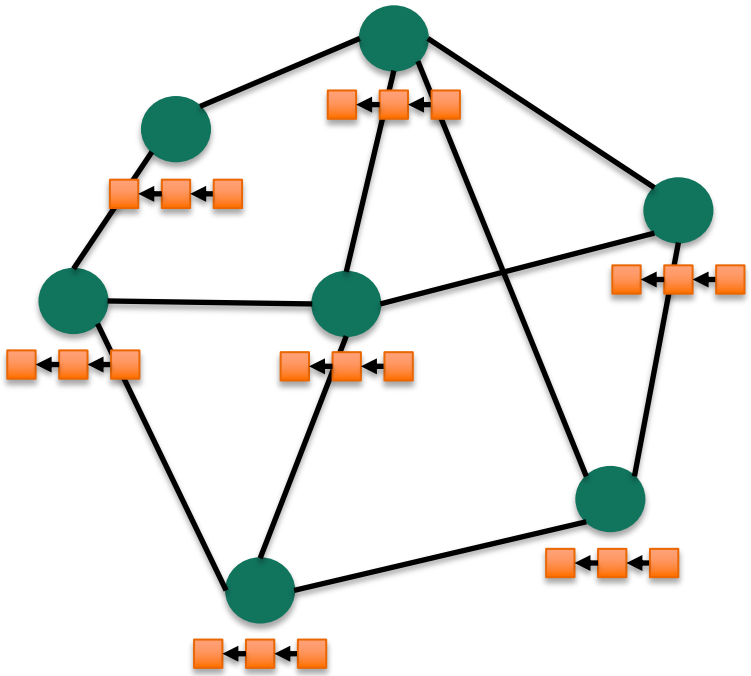
OVERVIEW

Structure of the Blockchain network



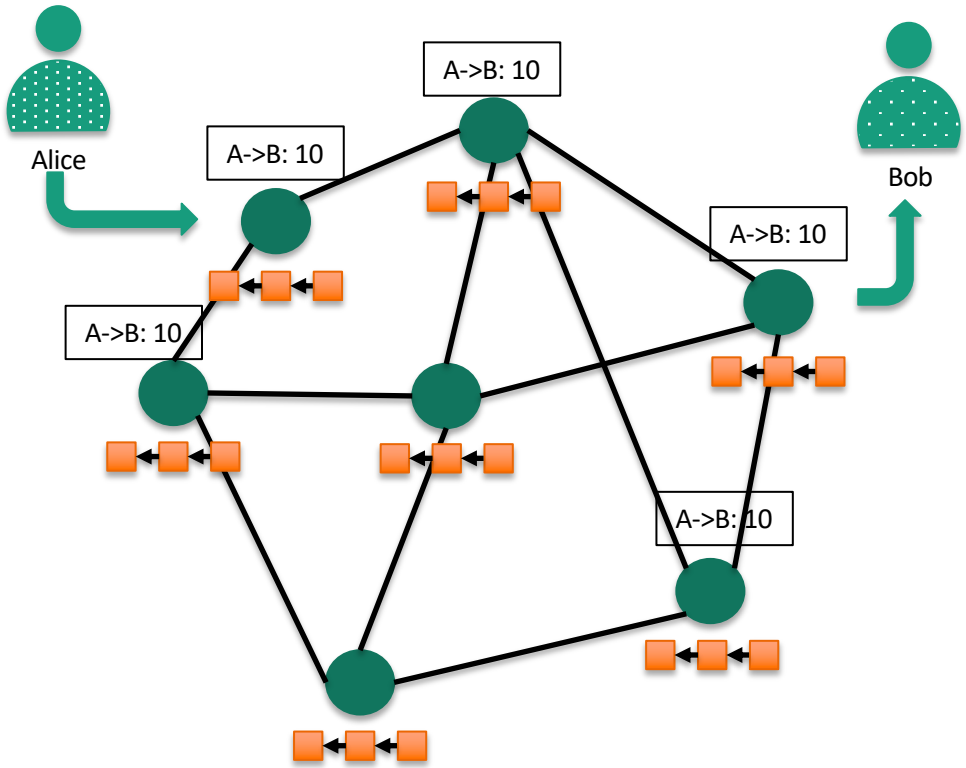
- Peer-to-peer Network
- Computers are nodes in network
- Blockchain network replaces intermediary platforms

Storage and management of transactions in a distributed ledger



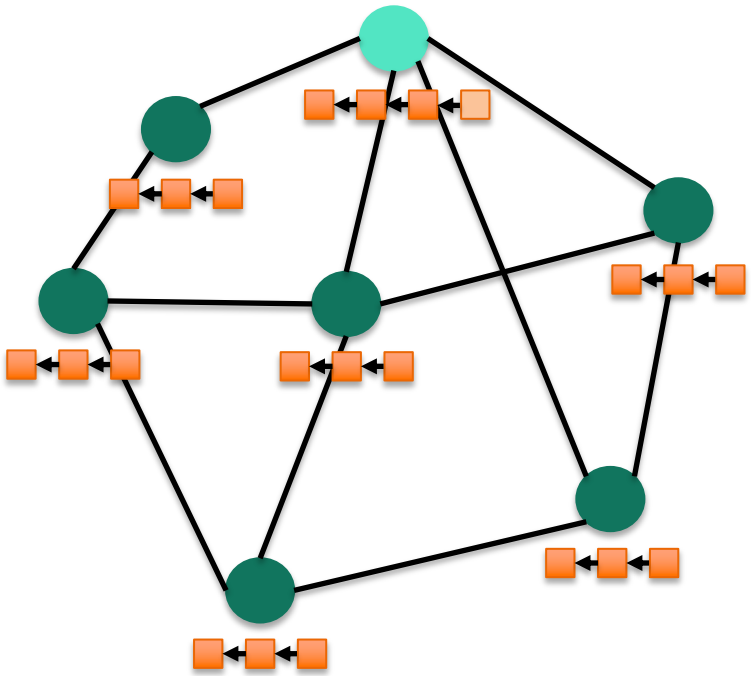
- Transactions are saved in a block
- Blocks are chained together
- All network nodes store the ledger
- Distributed ledger replaces the databases

Flow of transactions



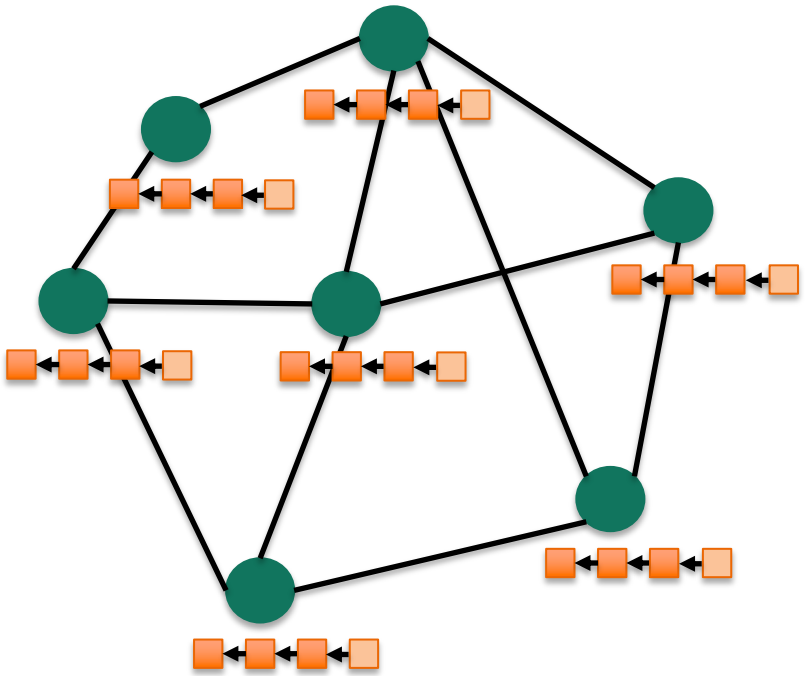
- Alice publishes a transaction on her computer
- Nodes that are directly connected verify the transaction
- Nodes distribute the transaction to other connected nodes
- Transaction spreads across the network

Consensus mechanism



- Which network node adds a new block to the ledger?
- Consensus mechanism: proof of work
- The new block is attached to the distributed ledger

Immutability of data, decentralization and trust



- Immutability of data
  - It is not possible to manipulate saved transactions
- Decentralization
  - Blockchain enables intermediaries to be replaced
- Trust
  - Distributed ledger and the consensus mechanism lead to security

References

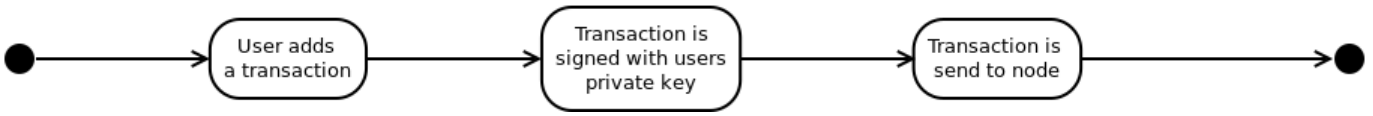
1. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press, 2016.
2. ConsenSys Academy, "Blockchain: Foundations and use cases (mooc)." [Online]. Available: https://www.coursera.org/learn/blockchain-foundations-and-use-cases
3. Y. Chen, "Ever wonder how merkle trees work?" Jun 2016. [Online]. Available: https://media.consensys.net/ever-wonder-how-merkle-trees-work-c2f8b7100ed3

ADDITIONAL MATERIAL

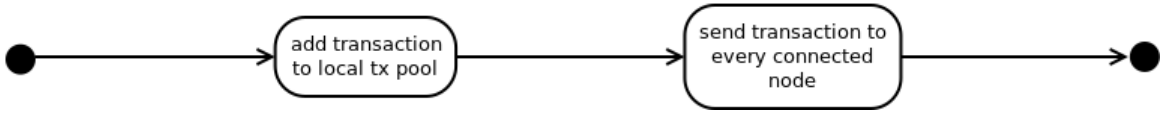
Blockchain from a technical perspective

Important Blockchain Processes

Client User creates a transaction



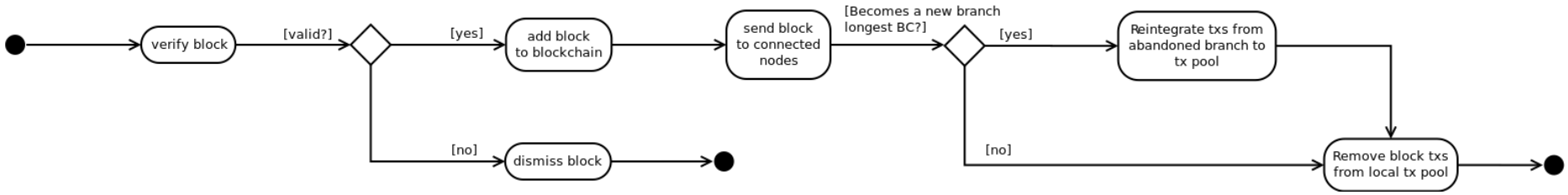
Node receives a new transaction



Blockchain from a technical perspective

Important Blockchain Processes

Node receives a new block

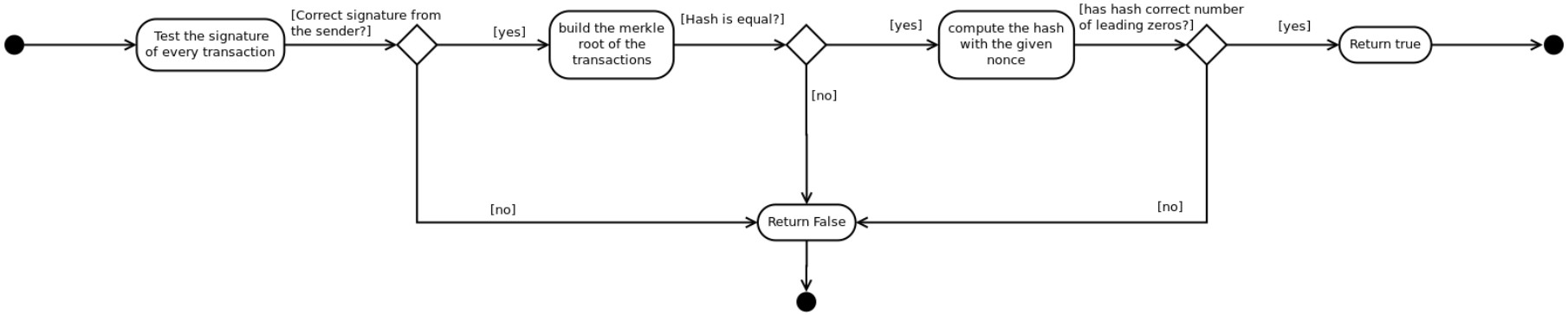


Fraunhofer FIT

Blockchain from a technical perspective

Important Blockchain Processes

Node verifies a block

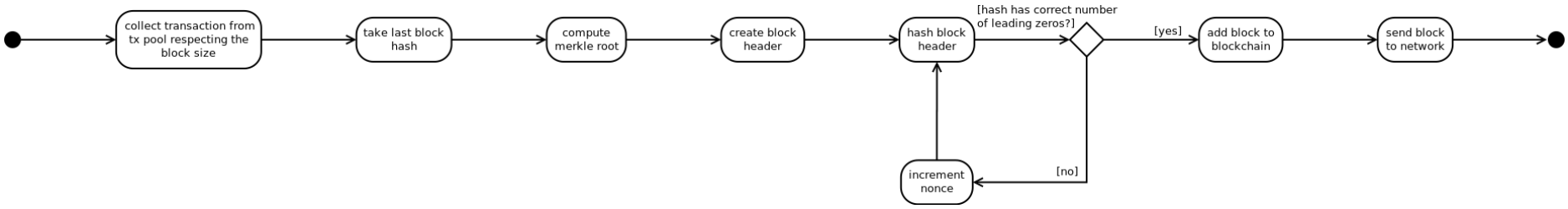


Fraunhofer FIT

Blockchain from a technical perspective

Important Blockchain Processes

Node mines a new block



Fraunhofer FIT