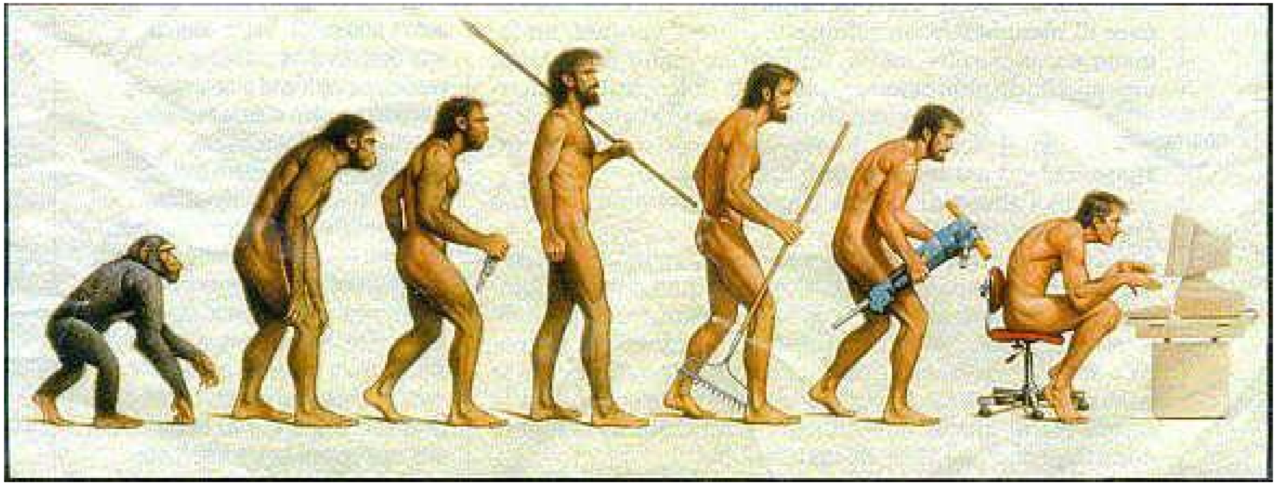
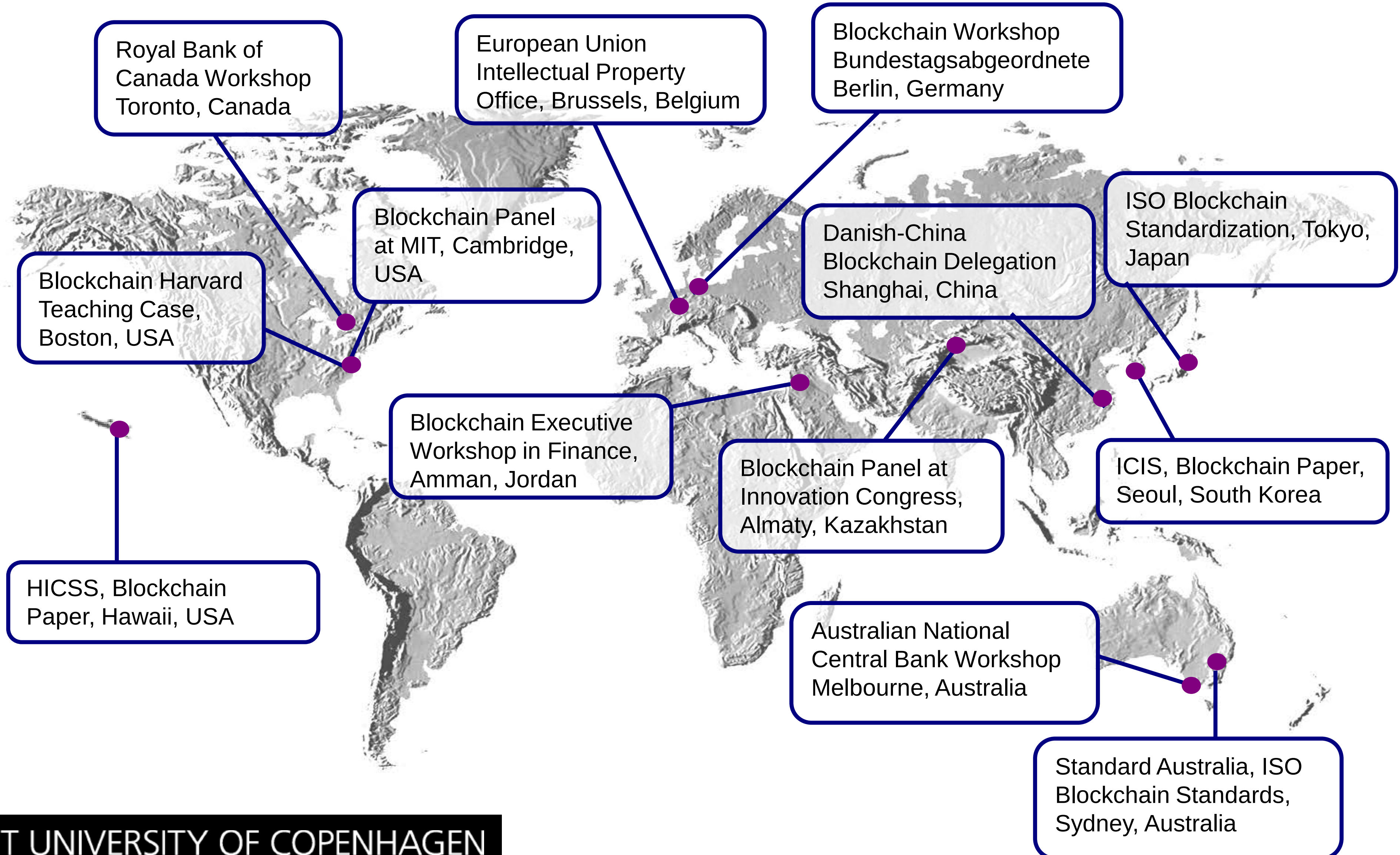
Blockchain Technology Foundations



Prof. Dr. Roman Beck | Professor
IT University of Copenhagen | Rued Langgaards Vej 7 |
DK-2300 Copenhagen S | Denmark
beck@itu.dk | www.itu.dk |
www.timegroup.info | www.blockchainschool.eu | phone +45 7218 5323 | skype roman-beck | twitter @roman_beck

Lead Researcher | Head of Research Group Technology, Innovation Management & Entrepreneurship (TIME) | Head of European Blockchain Center | AIS Council Representative for Europe, Middle East, Africa | Head of Dansk Standard ISO TC 307 Blockchain & Distributed Ledger Technology Group | Senior Editor, The DATA BASE for Advances in Information Systems (DataBase) | Associate Editor, Business and Information Systems Engineering (BISE) | Editorial Board, Journal of Business Economics

EUROPEAN BLOCKCHAIN CENTER SELECTED ACTIVITIES



Blockchain Components
What Makes a Blockchain?

- **Data structures:** The storage of **transactions** on the blockchain using a combination of **cryptographic hashing**, **cryptographic data structures**, **linear data structures & inter-chained blocks**

- **Consensus:** Allows the **nodes** of the blockchain network agree on the validity of data before it is added to the data storage layer by using **variants of consensus mechanisms** such as **PoW**, **PoS** or **PoA**

- **Protocols:** Through the use of the **p2p protocol** called **gossiping**, the blockchain network consisting of **nodes** (certified depending on environment) can synchronize transactional data in a secure and distributed manner.

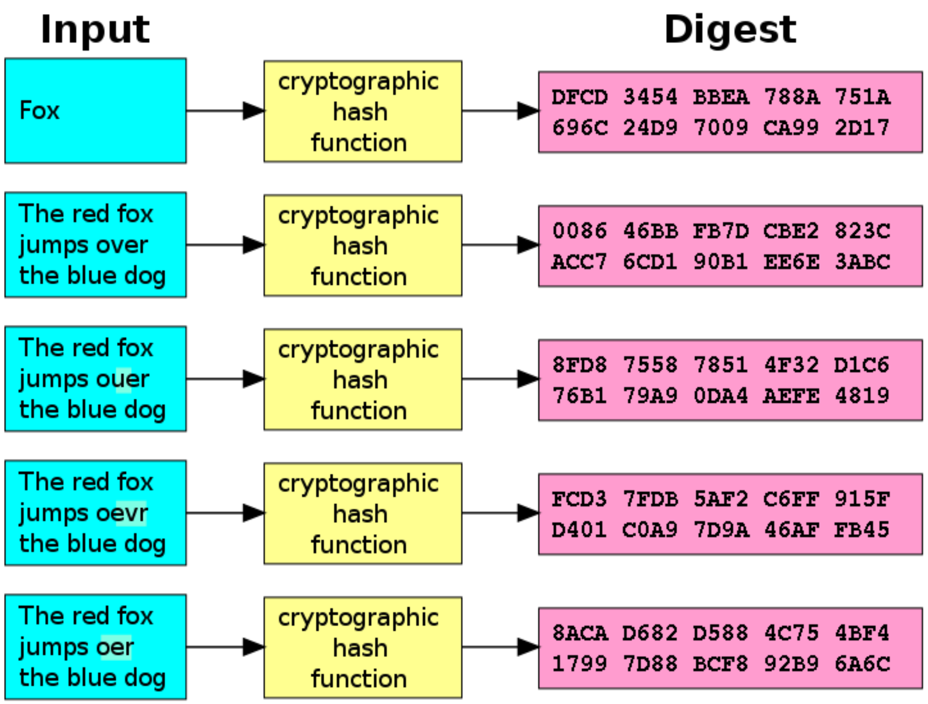
The technology behind blockchain is made up of preexisting technologies which date as far back as 1979.

Merkle, R. C. (1979). INFORMATION SYSTEMS LABORATORY.

Blockchain Data Structures - Cryptographic Hashing

- Hash functions are small computer programs that transform any kind of data into an output of fixed lengths, regardless of the size of the input data.

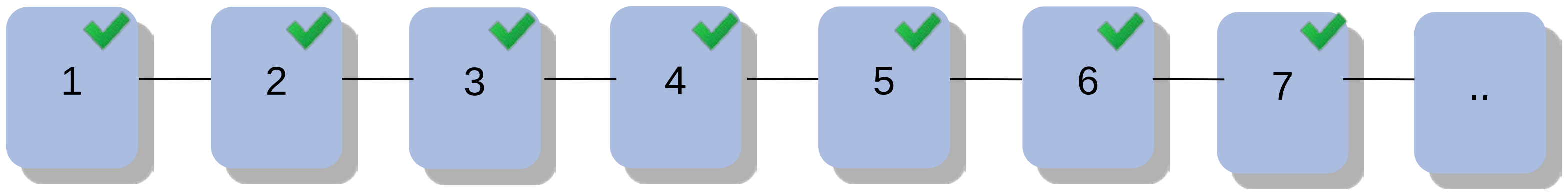
- An important group of hash functions is called cryptographic hash functions, which create digital fingerprints for any kind of data.



Drescher, D. (2017). Hashing Data. In Blockchain Basics (pp. 71-79). Apress.

Storage on the Blockchain - Linear Block Storage

Linear means *“Progressing from one stage to another in a single series of steps; sequential.”*

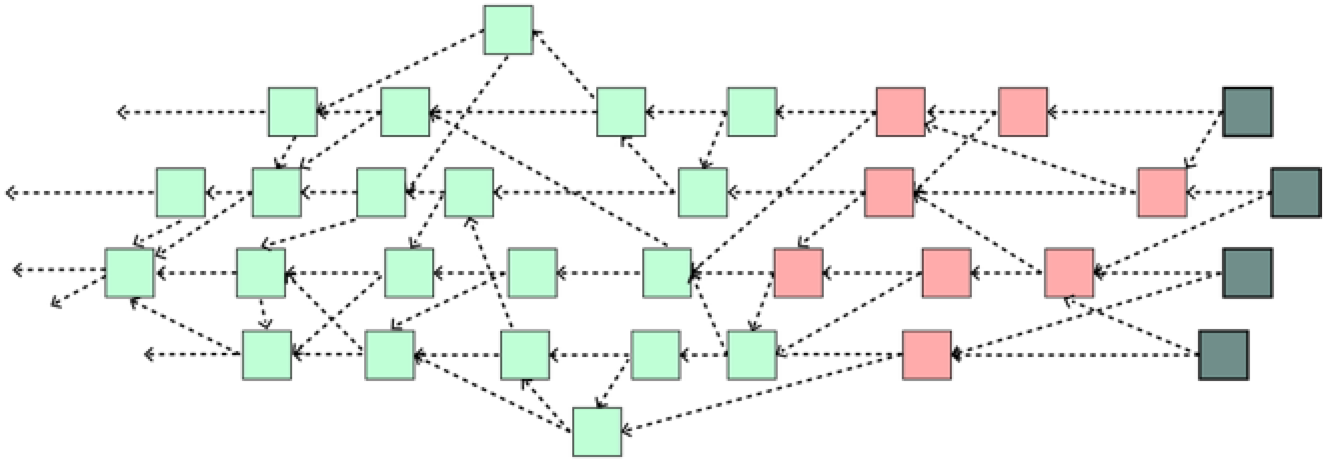


Most blockchain implementations use linear block storage such that they link each block to the next which represents a linked list.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Storage on the Blockchain - Non-Linear Block Storage

Other **Distributed Ledger Technologies** (DLT) use non-linear data structures such as **Directed Acyclic Graphs** (DAG).

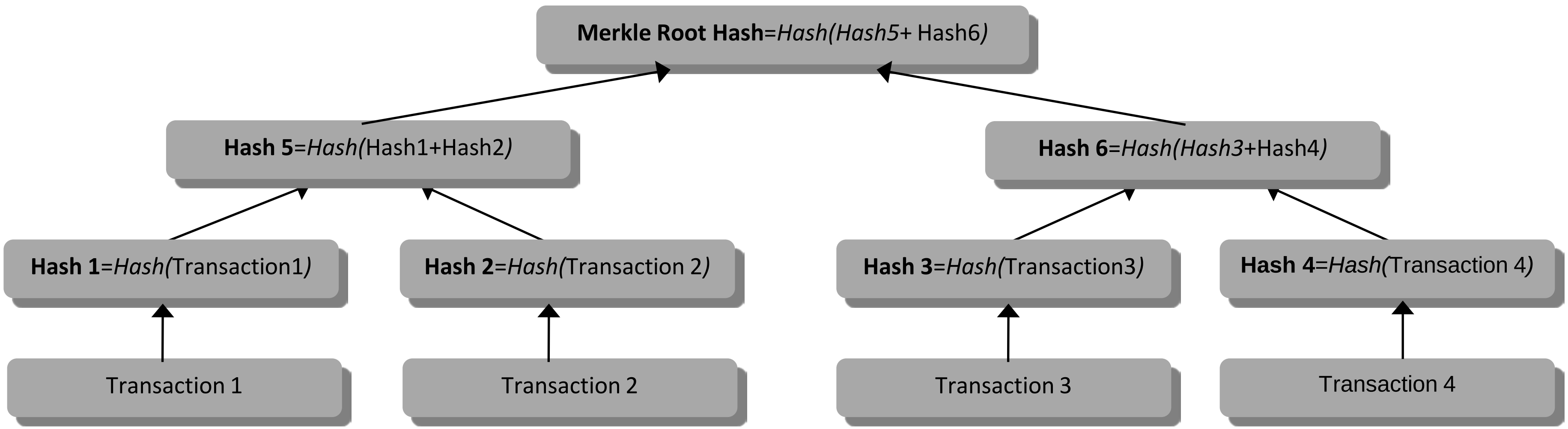


Based on a directed acyclic graph - IOTA

DAG Blockchain implementations include IOTA, Hashgraph, Dagcoin & Byteball.

Storage on the Blockchain - Cryptographic Data Structure

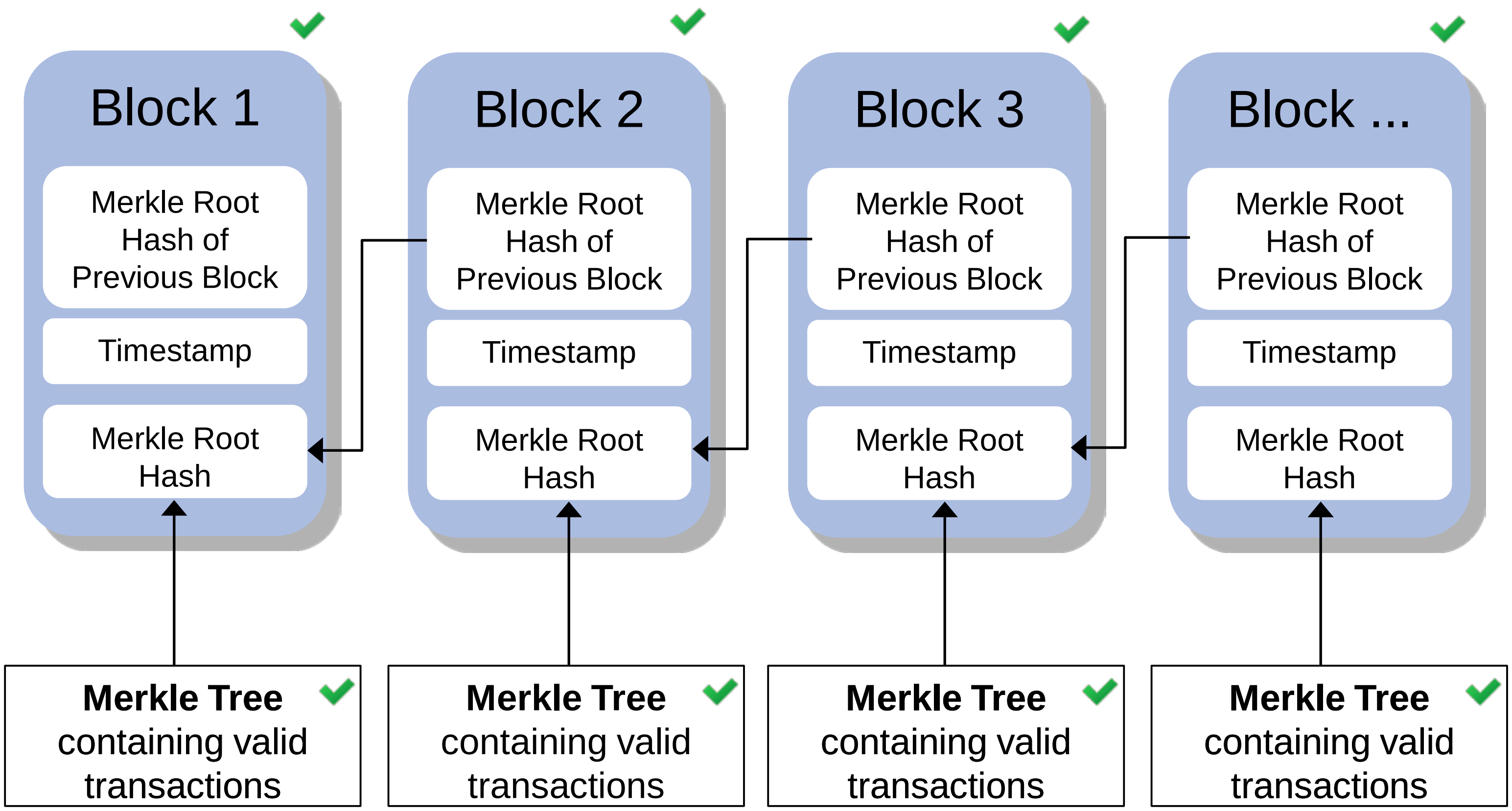
Each block in a blockchain has exactly one cryptographic data structure which contains transactions



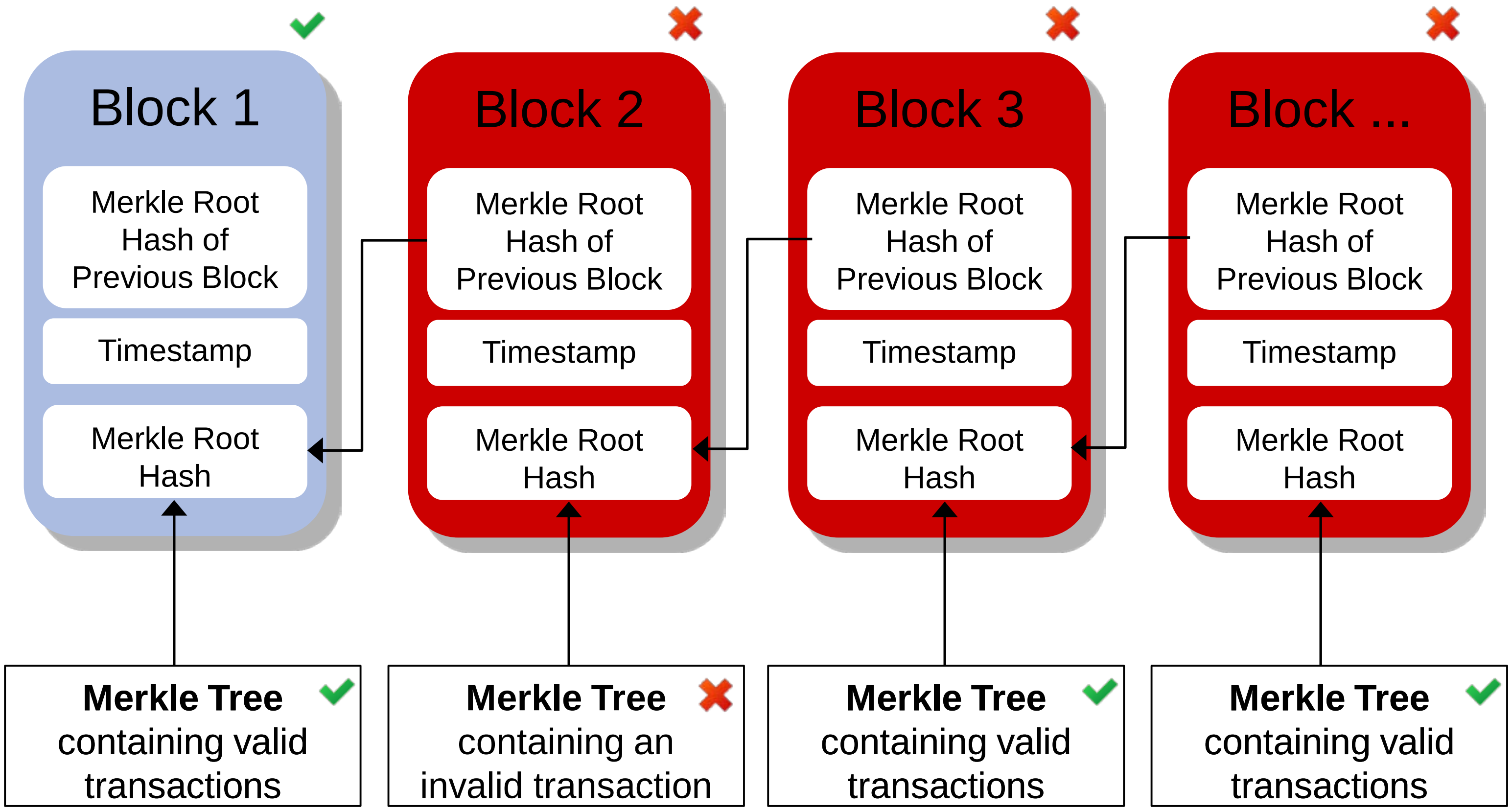
Merkle trees, also referred to as "hash trees" were patented in 1979 by Ralph Merkle.

Merkle, R. C. (1982). U.S. Patent No. 4,309,569. Washington, DC: U.S. Patent and Trademark Office

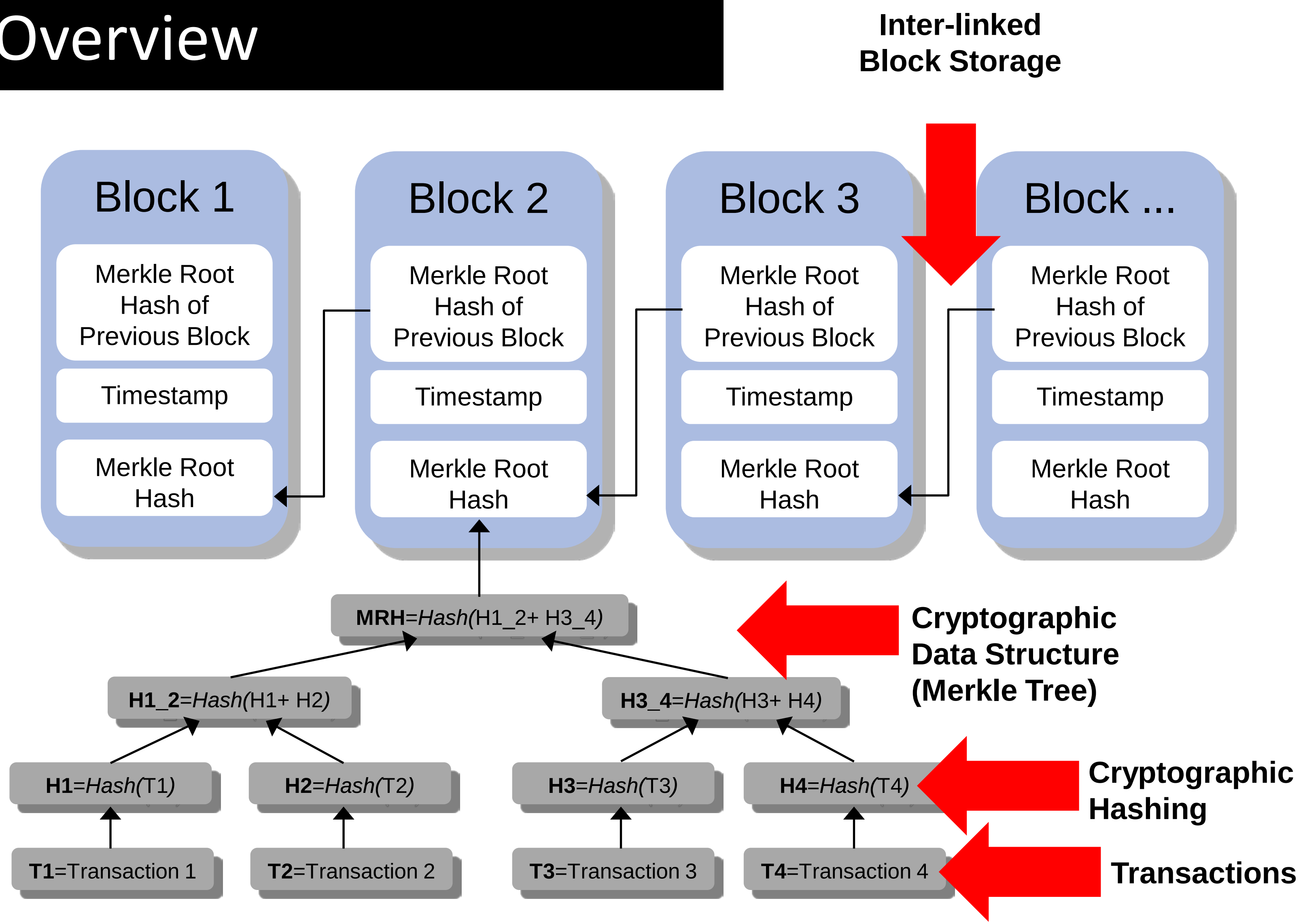
Blockchain Data Structures - Inter-Chained Blocks



Blockchain Data Structures - Inter-Chained Blocks



Blockchain Data Structures - Overview



Consensus - Nodes

Each node on a blockchain contains a full replication of all transactions stored in blocks. Two different types of nodes exist:

- **Non-validator nodes** have the ability to read blocks and propose new transactions but not partake in the consensus.

- **Validator nodes** have same privileges as non-validator nodes plus the responsibility of appending and validating blocks on the blockchain.

Danzi, P., Kalør, A. E., Stefanović, Č., & Popovski, P. (2017). Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices. arXiv preprint arXiv:1711.00540.

Consensus
- Consensus Across Nodes

- Consensus mechanisms are used ensure that the validator nodes agree on the **validity of the data** stored on the blockchain, without the need of a central authority.

- The two largest (cryptocurrency) blockchains (as of January 2018) have a combined total of just under 40 000 validator nodes.

  - Ethereum has 28273 validator nodes
  - Bitcoin has 11701 validator nodes

https://www.ethernodes.org/network/1
https://bitnodes.earn.com/dashboard/

Consensus - Variants

- **Proof of Work (PoW)**: In the 1992 journal paper by Dwork and Naor presented PoW as a method to counter spam emails. Bitcoin was the first to combine PoW with the **economic incentives** of cryptocurrencies to reward honest validator nodes.

- **Proof of Stake (PoS)**: PoS also uses economic incentives of cryptocurrencies to reward honest validator nodes but **without the computational overhead**.

- **Proof of Authority (PoA)**: PoA is a **favorable consensus mechanism for permissioned environments**. Economic incentives are no longer needed to run this consensus, thus more trust must be put into the nodes in this environment.

Dwork, C., & Naor, M. (1992). Pricing via processing or combatting junk mail. In Annual International Cryptology Conference (pp. 139-147). Springer, Berlin, Heidelberg.
Hopkins, A. L., Lala, J. H., & Smith, T. B. (1987). The evolution of fault tolerant computing at the Charles Stark Draper Laboratory, 1955–85. In The Evolution of fault-tolerant computing (pp. 121-140). Springer, Vienna.

Consensus - Proof of Work (PoW)

- PoW validator nodes are commonly referred to as **miners** that compete to solve **computational expensive hashing problems** which are easy to verify.

- The first miner to solve a given hashing problem is allowed to add a new block to the blockchain, this miner is then rewarded with some cryptocurrency.

- PoW in the Bitcoin algorithm involves finding a number (**Nonce**) so that the function *Hash*(Merkle Root Hash of previous block + **Nonce**) returns a value that starts with at least **K** integers.

- K is referred to as the **difficulty**, and as of January 2018 the Bitcoin PoW has the difficultly of 18.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
https://blockchain.info/charts/hash-rate

Consensus - Proof of Stake (PoS)

- Validator nodes in **PoS do not mine**, which means less electricity consumption.

- The node that is selected to add a block to the blockchain is selected in relation to their **stake** (usually cryptocurrency). The selected node that adds a block is rewarded in a cryptocurrency.

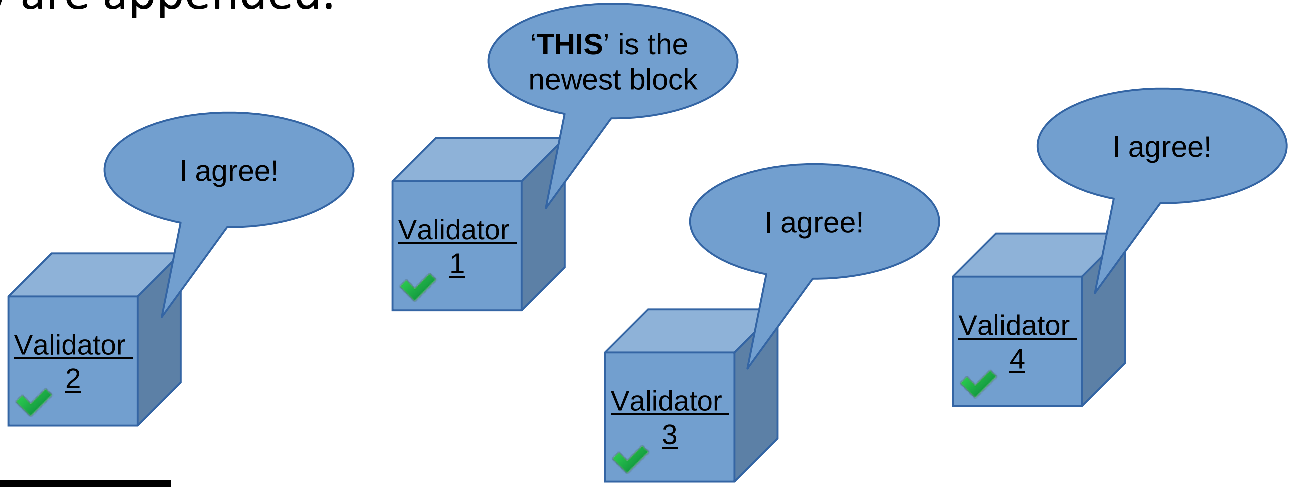
- Monopolies can easily exist and control the network, which is why **heuristics** such as randomization are generally used.

- A democratic version of PoS exists (**DPoS**) where validator nodes are referred to as witnesses, who are voted by a group of nodes called delegates.

Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies without proof of work. In International Conference on Financial Cryptography and Data Security (pp. 142-157). Springer, Berlin, Heidelberg.

Consensus - Proof of Authority (PoA)

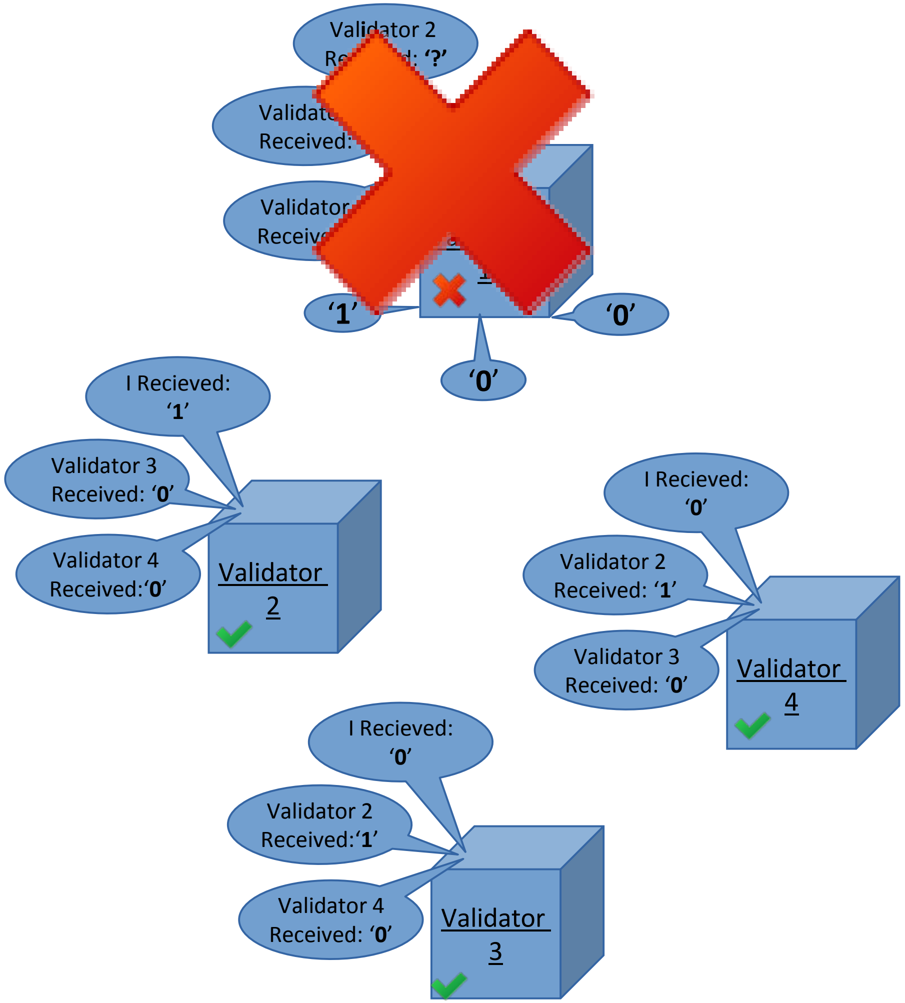
- The **real world identity** of the validator nodes decides who can add and validate a block on the blockchain.
- All validator nodes must be selected by some central authority to ensure that they are trusted, this is also referred to as a **permissioned environment**.
- Validator nodes generally vote to achieve consensus on the validity of blocks before they are appended.



Consensus - Proof of Authority (PoA)

Consensus mechanism that vote can be broken by malicious nodes.

To prevent this, Byzantine voting mechanisms such as **Practical Byzantine Fault tolerance (PBFT)** introduce multiple rounds where each node repeats what was said by each node.



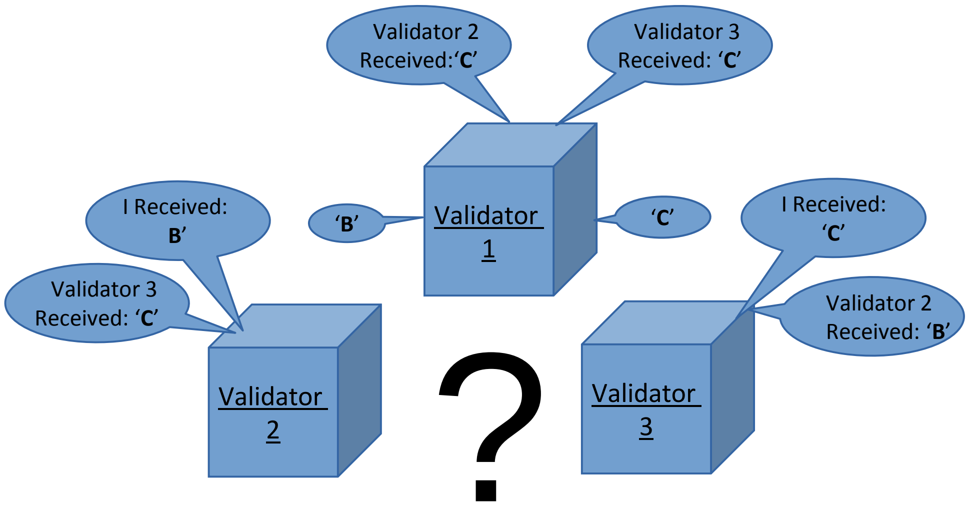
Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In OSDI (Vol. 99, pp. 173-186).

Consensus - Proof of Authority (PoA)

The 1982 paper titled the byzantine generals problem proves that for every malicious node (***m***) you need at least ***2m+1*** non malicious nodes.

If one malicious node exists ***(m=1)***

You need 3 ***(2x1+1)*** non malicious nodes.



Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), 382-401.

Consensus – Comparison

	PoW	PoS	PoA
Environment	Permissionless	Permissioned & Permissionless	Permissioned
Economic Cost	High	Low	Low
Performance	Slow	Fast	Fast
Validator Scalability	Good	Good	Bad

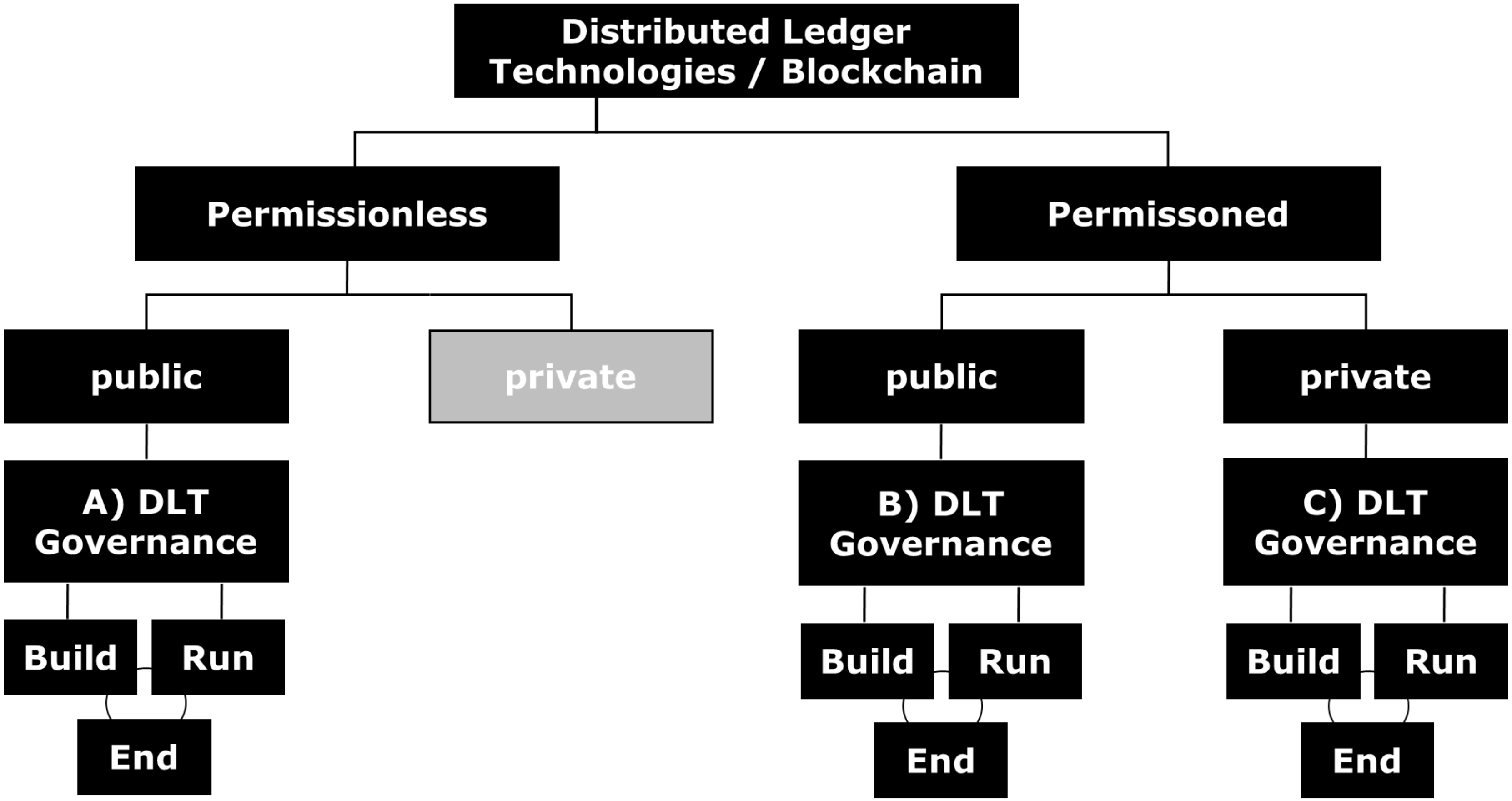
A large body of work demonstrates that the scalability issues of PoA can be addressed with new higher performance consensus mechanisms.

Crain, T., Gramoli, V., Larrea, M., & Raynal, M. (2017). (Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchains. arXiv preprint arXiv:1702.03068.

Baird, L. (2016). Hashgraph consensus: fair, fast, byzantine fault tolerance. Swirlds Tech Report.

Liu, J., Li, W., Karame, G. O., & Asokan, N. (2016). Scalable Byzantine Consensus via Hardware-assisted Secret Sharing. arXiv preprint arXiv:1612.04997.

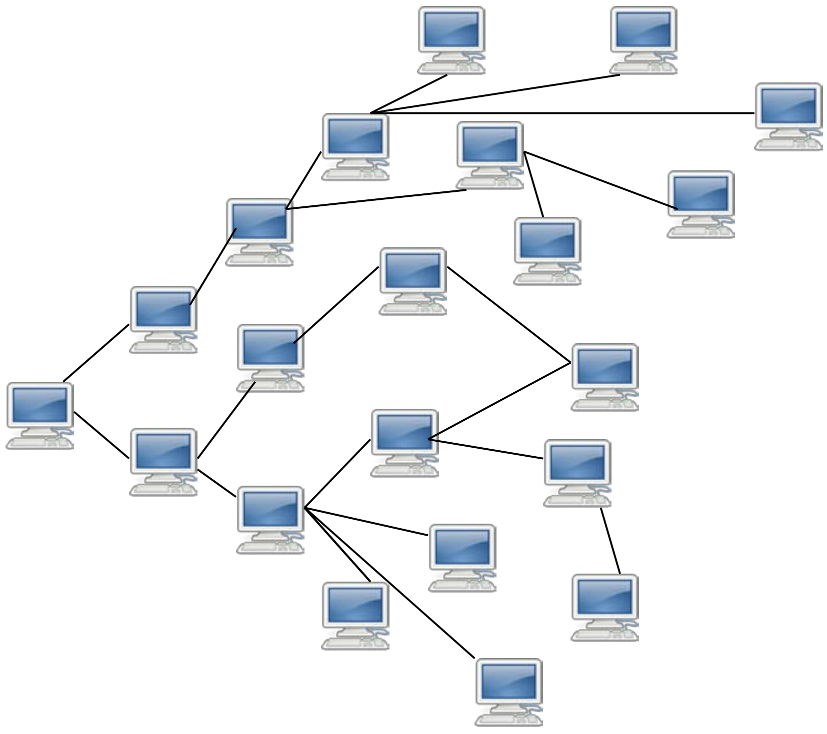
Consensus – Type of Blockchain and Access Rights



Consensus - Variants

Protocols
- Gossip Protocol

"Information spreads throughout the human grapevine at an amazing speed, often reaching almost everyone in a community, without any central coordinator."



Jelasity, Márk (2011-01-01). *Serugendo, Giovanna Di Marzo; Gleizes, Marie-Pierre; Karageorgos, Anthony, eds. Gossip. Natural Computing Series. Springer Berlin Heidelberg. pp. 139–162.*

Contact information

EUROPEAN BLOCKCHAIN CENTER

For further information please contact me!

Prof. Dr. Roman Beck
Lead Researcher
Head of Research TIME Group
Head of European Blockchain Center

IT University of Copenhagen
Rued Langgaards Vej 7
DK-2300 Copenhagen S, Denmark
beck@itu.dk|www.romanbeck.com
phone +45 7218 5323 | twitter @roman_beck