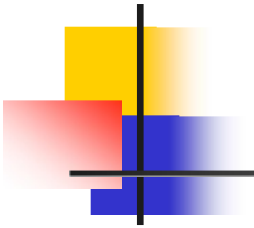


CSE 543

Information Assurance and Security

Blockchain and IA Applications

Professor Stephen S. Yau

Fall 2022

Important Features of Blockchain

- Decentralization
- Immutability
- High Fault Tolerance
- High Availability
- Transparency
- Auditability

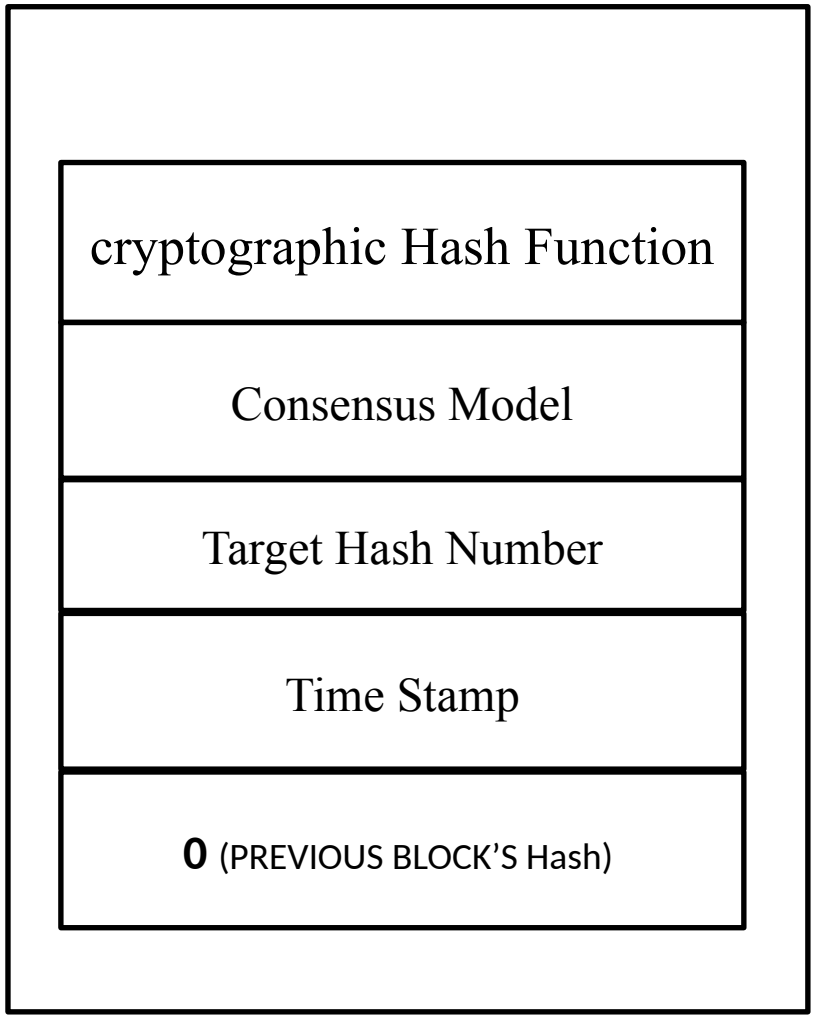
Major Applications of Blockchain

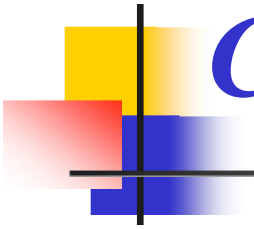
- Software development
- Supply chain
- Electronic voting
- Cloud, edge and/or IoT computing
- Finances
- Healthcare
- Smart city and/or smart world
- …

What Is a Blockchain?

- A sequence of blocks, in which *each block consists of a header and body*, and the *blocks are linked by storing the previous block's hash in the current block header*
- The first block in blockchain is called ***genesis block***

Genesis Block

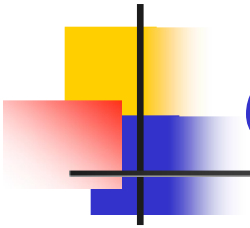




Cryptography

Cryptography:

- Study of mathematical techniques related to certain aspects of information security, such as confidentiality, data integrity, entity authentication, and data origin authentication.
- The basic component of cryptography is a ***cryptosystem***



Cryptosystem

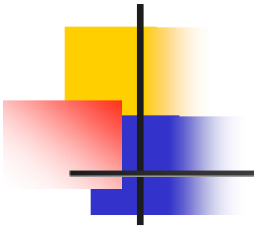
*A **cryptosystem*** is a 5-tuple (*E, D, M, K, C*), where *M* is the set of plaintexts,

K is the set of keys,

C is the set of ciphertexts,

E: $M \times K \rightarrow C$ is the set of encipher functions,

D: $C \times K \rightarrow M$ is the set of deciphering functions.

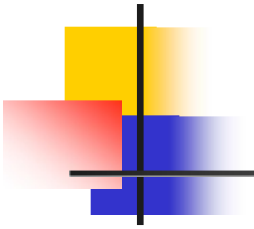


Types of Cryptosystems

Symmetric cryptosystems are ***classical cryptosystems***:

$M = D(K, E(K, M))$

K, is used as both encryption and decryption



Types of Cryptosystems (cont.)

Asymmetric cryptosystems:

$M = D(K_d, E(K_e, M))$

K_d is the decryption key and K_e is the encryption key

$K_d \neq K_e$

Cryptography in Blockchain

- A ***one-way hash function***, also known as ***a message digest***, is a mathematical function that takes a variable-length input string and converts it into a fixed-length binary sequence that is computationally difficult to invert - that is, generate the original string from the hash.

Cryptography in Blockchain (cont.)

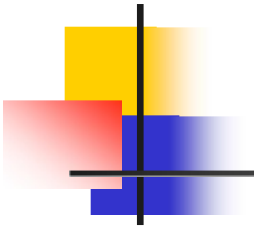
- ***Hashing*** is a process using a ***one-way cryptographic function*** to generate a digest of fixed size from a string of input text, such as SHA256 and Scrypt.
- **Digital Signatures** for source verification

Cryptography in Blockchain

- In blockchain, private keys are used to digitally sign the records in block body, and public keys are used to verify signatures

Consensus in Blockchain

- A means for majority of the nodes to reach an agreement before adding validated blocks to the blockchain.
  - Two consensus models used in blockchain: Proof of Work, and Proof of Stake.



Blockchain Network

- **Blockchain Network is a peer-to-peer network**
  - Each node (peer) has the following functions:
    - ***Store a part of the blockchain***
    - ***Store the entire copy of blockchain***
    - ***Generate and validate blocks being added to the blockchain***

Blockchain Network

- For nodes to actively participate in a blockchain network, they must be ***always connected*** to the network
- The nodes that generate new blocks are called ***miners***

Target Hash In Genesis Block

- ***Difficulty level*** (from 0 to 2^256) set in genesis block
- When a new block is added to a blockchain, the hash number Hn of the new block is computed with the input as block header of the new block:

```
if Hn < Target Hash:
        add new block to blockchain
else:
        reject new block
```

Consensus in Blockchain

- **Proof of Work:**
  - A block generated by a miner is accepted, when it shows proof of spending a pre-determined amount of computational resources in generating the block.
  - For example, in bitcoin, the nodes are required to solve the cryptographic problem of finding a hash of the block which is less than the target hash of the blockchain.

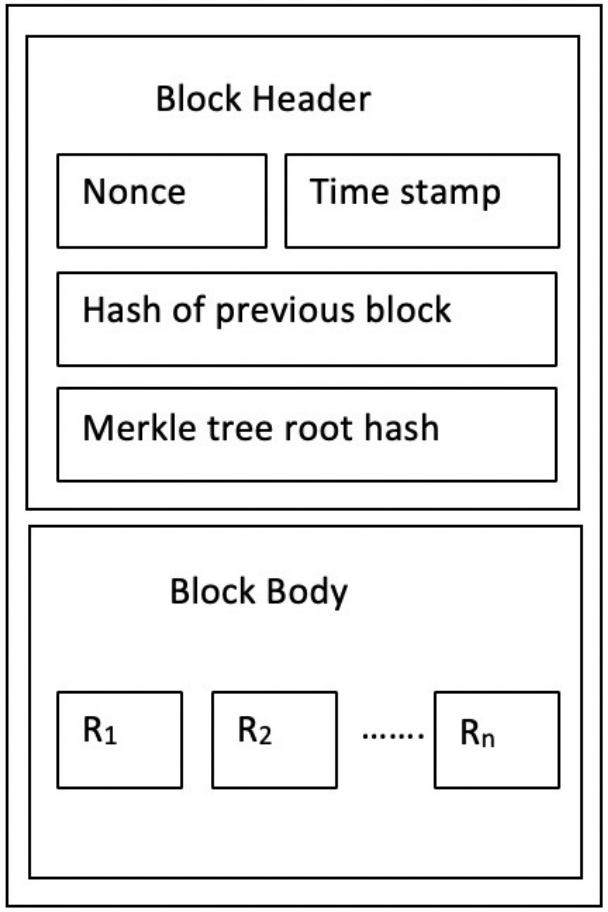
Consensus in Blockchain (Cont.)

- **Proof of Stake**
  - The ***miner*** which creates a block is chosen randomly based on what is at stake by the miner
  - For example, the wealth of the miner could be at stake

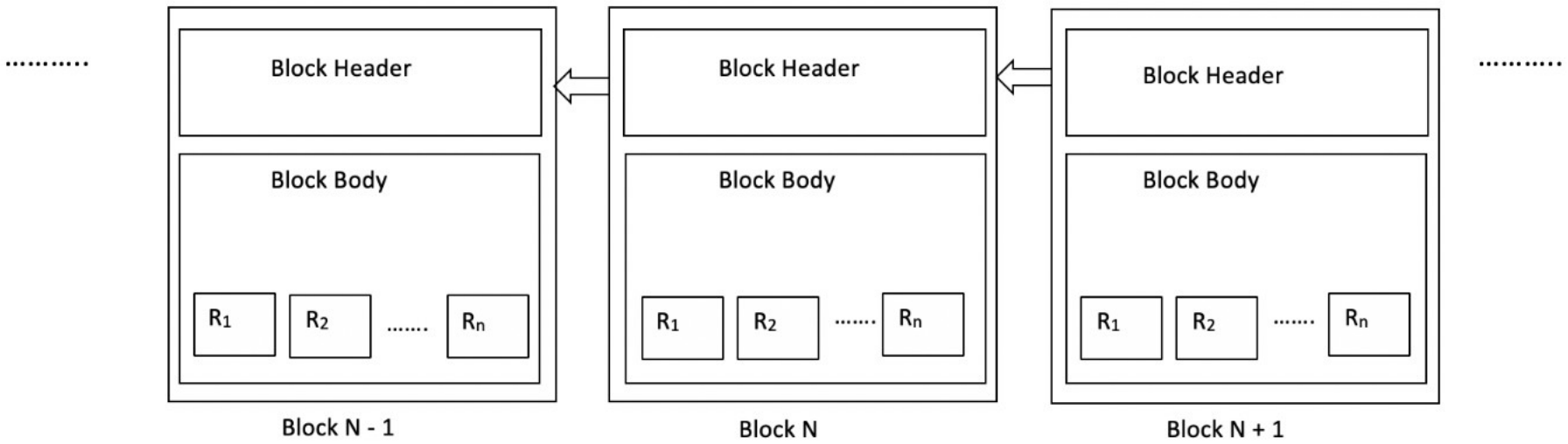
Timestamp

- **Timestamp**
  - The current time (in seconds) in universal time since January 1, 1970 when the block is created.

Block structure



Blockchain Structure



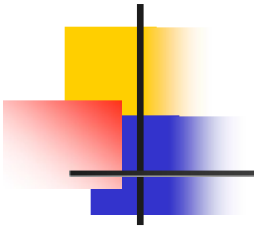
Block Structure in Blockchain

- **Header**
  - Previous block's hash
  - Merkle tree root hash
  - Timestamp
  - Nonce

- **Body**
  - Records. For examples,
    - Validated healthcare records
    - Financial records (e.g. Bitcoin Transactions)

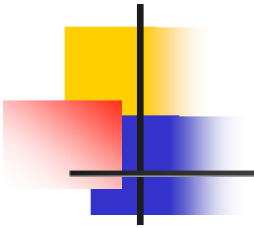
Header

- **Previous block's hash**
  - Calculated as Hash (Merkle root hash | Previous block hash | Timestamp | Nonce)
- **Merkle tree root hash**
  - Created by repeatedly hashing pairs of records in block body until there is only one hash left, which is called Merkle root tree hash
  - Each leaf node stores transaction record from block body
- **Nonce (Number Only used Once)**
  - A random number that meets the requirements of a target hash.



Smart Contracts

- An interactive computer program that ***defines transaction protocol, including*** the ***high level terms*** of a contract of an agreement
- ***Automatically executed*** in blockchain



Smart Contracts Creation

Two Phases:

1. Initialization

   Initialize agreement with ***actionable clauses and properties***

2. Execution methods

   Implement methods to handle actionable clauses

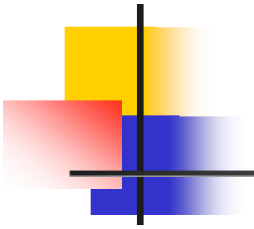
A Smart Contracts Example

1. Client and Tasker agree on blockchain platform
2. Client creates and deploys smart contract on blockchain platform with agreement clause(s)
3. Tasker performs task and provides the result to smart contract
4. Smart contract automatically verifies the result against agreement clauses
5. Smart contract automatically triggers execution action in the agreement on blockchain platform.

Reference: https://rubygarage.org/blog/ethereum-smart-contract-tutorial

Types of Blockchains

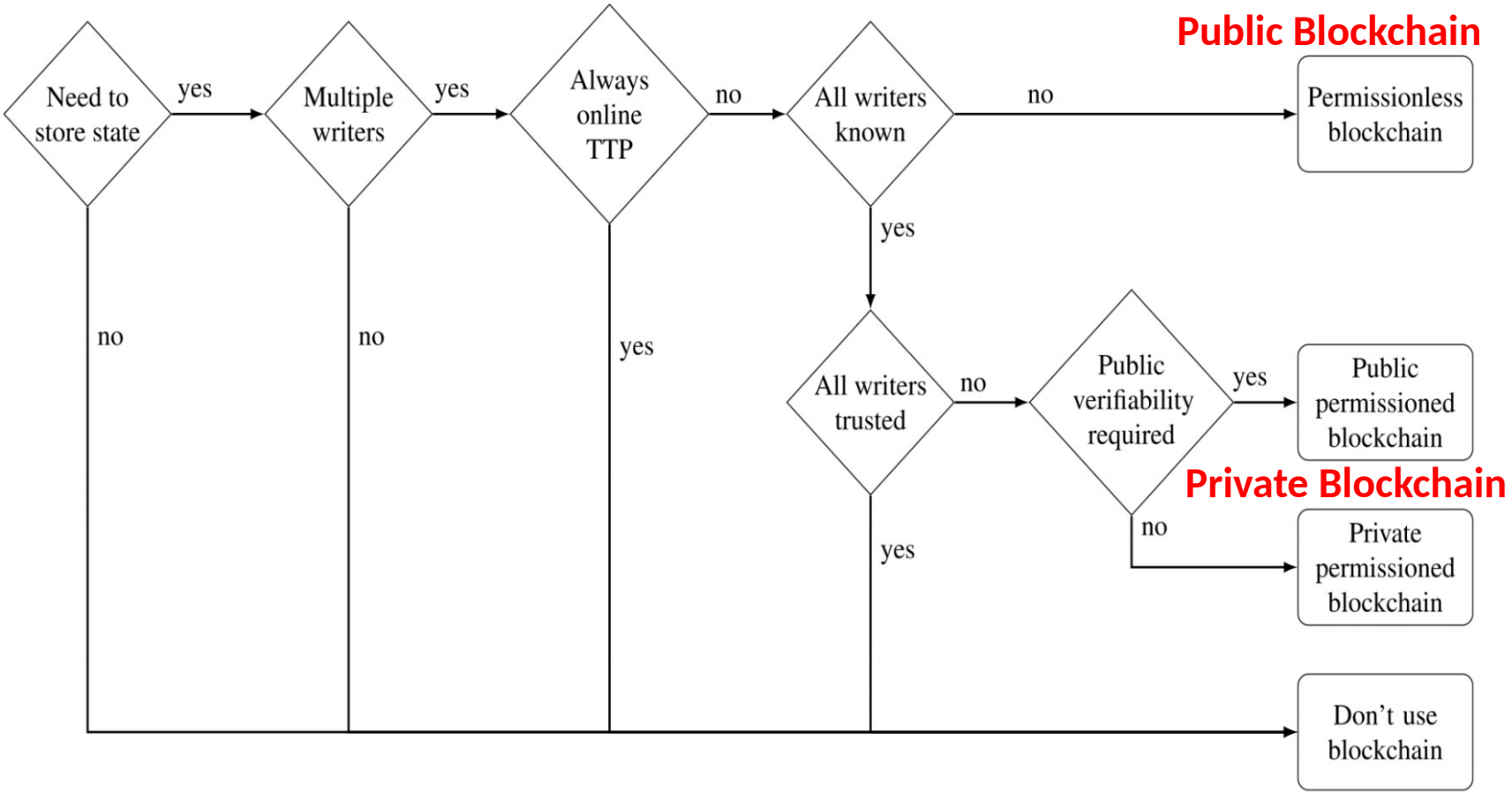
- **Public (Permissionless)**
  - Participation/access not restricted to any nodes
  - Anyone with an Internet connection can be part of this blockchain
  - Example - Bitcoin
- **Public (Permissioned)**
  - Anyone can join after passing a suitable identity verification process.
  - Mixture of public permissionless and private blockchains and support many options for customization.
  - Example - Ethereum



Types of Blockchains

- **Private (Permissioned)**
  - Under administrative control of an entity/organization, or a closed group
  - Does not require expensive mining process
  - Example – Corda
- **Consortium**
  - Combination of several blockchains
  - Example - Hyperledger

Is blockchain suitable for your application?



Reference: Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y. and Han, J., 2018. When intrusion detection meets blockchain technology: a review. Ieee Access, 6, pp.10179-10188.

Popular Blockchain Platforms

- Hyperledger (https://www.hyperledger.org/)
- Ethereum (https://www.ethereum.org/)

Challenges

- **Scalability**
  - All the active nodes must have entire copy of blockchain which is a huge storage requirement
- **High computational resource requirements**
  - Proof of Work consensus algorithms require significant amount of computation power to calculate hash of block
- **51% attack**
  - If a group of miners can control more than half of blockchain network's computational resources, this will undermine the major features of blockchain

References for Blockchain and IA Applications

1. Zheng, Zibin, et al. "An overview of blockchain technology: architecture, consensus, and future trends." *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017.
2. M. E. Whitman and H. J. Mattord , Principles of Information Security, 7th edition, Thomson Course Technology, June 27, 2021. ISBN-10: 035750643X, ISBN-13 : 978-0357506431
3. Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y. and Han, J., 2018. When intrusion detection meets blockchain technology: a review. 10.1109/ACCESS.2018.2799854 https://ieeexplore.ieee.org/document/8274922.

References for Blockchain and IA Applications

4. M. Conti et. al, “A Survey on Security and Privacy Issues of Bitcoin”, ArXiv: DOI:10.1109/COMST.2018.2842460
5. P. Zhang et al, “FHIRChain: Applying Blockchain to Securely and Scalable Share Clinical Data”, in J. Comp. & Struct. Biotechnology, 2018.
6. H. Zhu and Y. Zhang, "Collaborative Testing of Web Services," in IEEE Transactions on Services Computing, vol. 5, no. 1, pp. 116-130, Jan.-March 2012, doi: 10.1109/TSC.2010.54.

References for Blockchain and IA Applications

7. B. Anderson and S. S. Yau, "A Blockchain-based Scalable Approach to Protecting Electronic Voting from Central Authority Attacks," Proceedings of 6th IEEE Cyber Science and Technology Congress, (virtual). October 2021, 8 pages.
8. Stephen S. Yau and Jinal S. Patel School of Computing, Informatics, and Decision Systems Engineering Arizona State University "A Blockchain-based Testing Approach for Collaborative Software Development"
9. Stephen S. Yau and Jinal S. Patel School of Computing, Informatics, and Decision Systems Engineering Arizona State University "Application of Blockchain for Trusted Coordination in Collaborative Software Development"