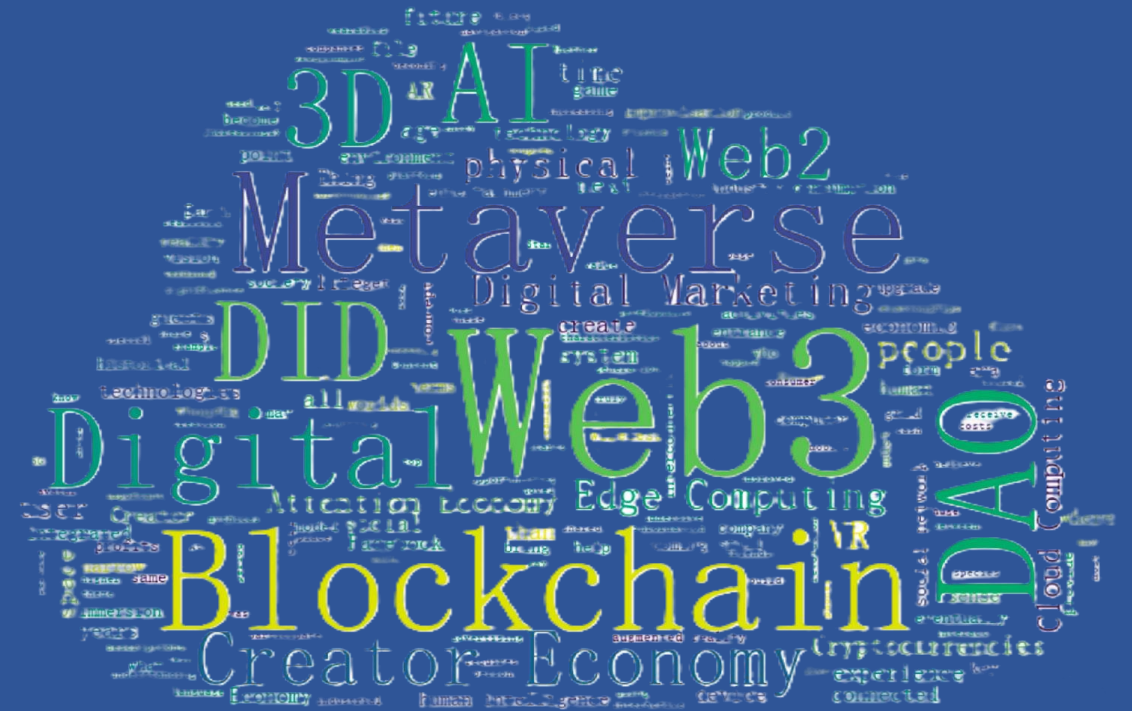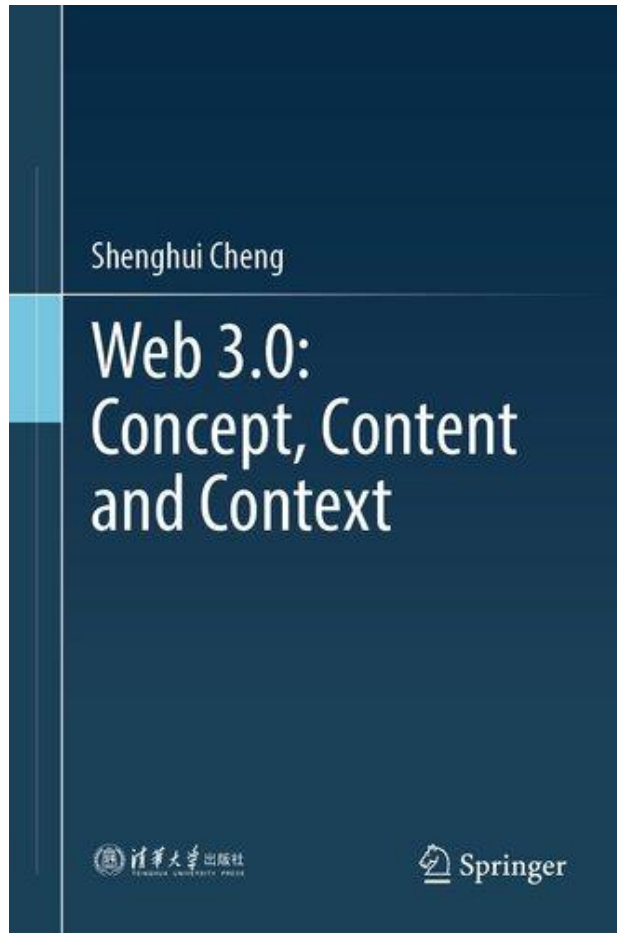# Intro to Web 3.0

IF3110 – Web-based Application Development

Reference

Shenghui Cheng - Web 3.0: Concept, Content and Context - Springer Nature Singapore (2024)

Outline

- What is Web 3.0
- The 3 Characteristics of Web 3.0
- History of Web 3.0
- Blockchain
- Smart Contracts
- DAO
- Token
- Multi-application of Web 3.0

What is Web 3.0?

Web 3.0 represents the third iteration of Web technology, and its concept is still expanding, resulting in the absence of a standardized and universally accepted definition.

People have generally reached a basic understanding of Web 3.0:

- Web 1.0 resolved the issue of user content browsing in the past.
- Web 2.0 addressed the problem of user-generated content in the present.
- Web 3.0 considered the future solution to user information security and content ownership, often referred to as "a user-owned Internet".
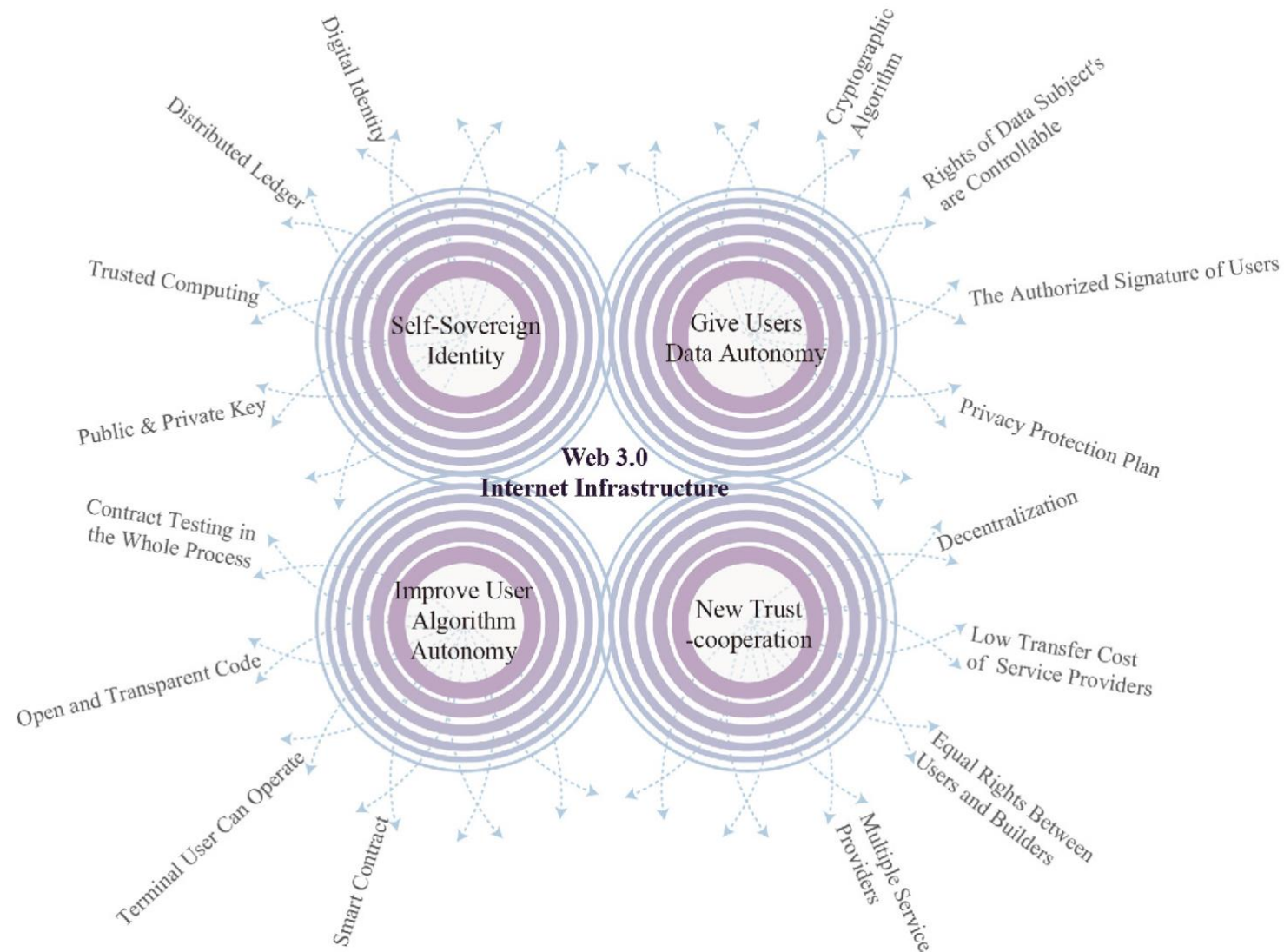
Web 3.0 is centered around the user and places a strong emphasis on user autonomy

Self-Sovereign Identity (SSI)

In Web 3.0, users are not required to create accounts on internet platforms; instead, they authenticate each other's digital identity using the signature and verification mechanism of public and private keys.

Web 3.0 can leverage distributed ledger technology to establish a distributed public key infrastructure (DPKI) and a robust distributed digital identity management system.

Data Autonomy

- Web 3.0 grants users the autonomy to manage their data, disrupting the inherent data control monopoly held by centralized entities.

- User data is safeguarded through cryptographic algorithms and stored on a distributed ledger.

- Users retain the authority to determine with whom they share their data and how it is utilized.

- Only the personal data authorized by the user's signature can be legally accessed.

User Independence when Dealing with Algorithms

- A smart contract, deployed on a distributed ledger, is a program that can be invoked, offering functionality, flexibility, and key benefits such as transparency, trustworthiness, automatic execution, and obligatory compliance.
- The code of the smart contract becomes public and transparent upon deployment to the distributed ledger.
- Users can verify and inspect the code at any time, which helps detect possible algorithm abuse, bias, and associated risks.

Novel Relationship of Trust and Collaboration

- During the Web 1.0 and Web 2.0 era, users faced challenges in placing trust in internet platforms.

- Web 3.0 operates in a decentralized manner, devoid of a single controlling platform, and offers multiple service providers.

- Platforms are interconnected through distributed protocols, enabling users to switch between service providers at a fraction of the cost.

- Web 3.0 represents the convergence of two fundamental aspects of human civilization: freedom and trust.

Novel Relationship of Trust and Collaboration

- During the Web 1.0 and Web 2.0 era, users faced challenges in placing trust in internet platforms.

- Web 3.0 operates in a decentralized manner, devoid of a single controlling platform, and offers multiple service providers.

- Platforms are interconnected through distributed protocols, enabling users to switch between service providers at a fraction of the cost.

- Web 3.0 represents the convergence of two fundamental aspects of human civilization: freedom and trust.

Web 3.0 is a New Economic System
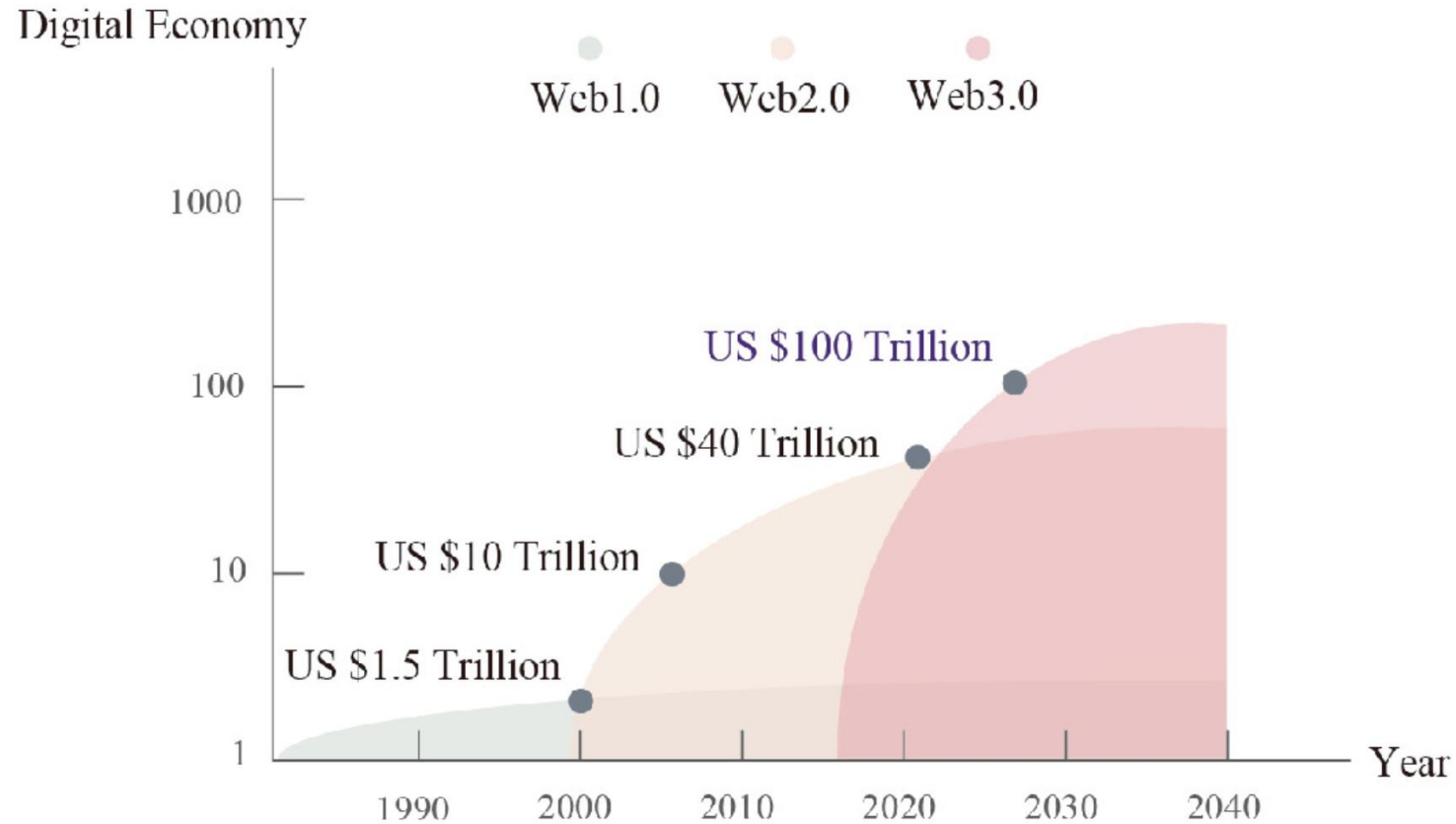
Fig. 1.5 Comparison of the size of the digital economy for Web 1.0, Web 2.0 and Web 3.0 (*Source* Folius venture)

Characteristics of Web 3.0
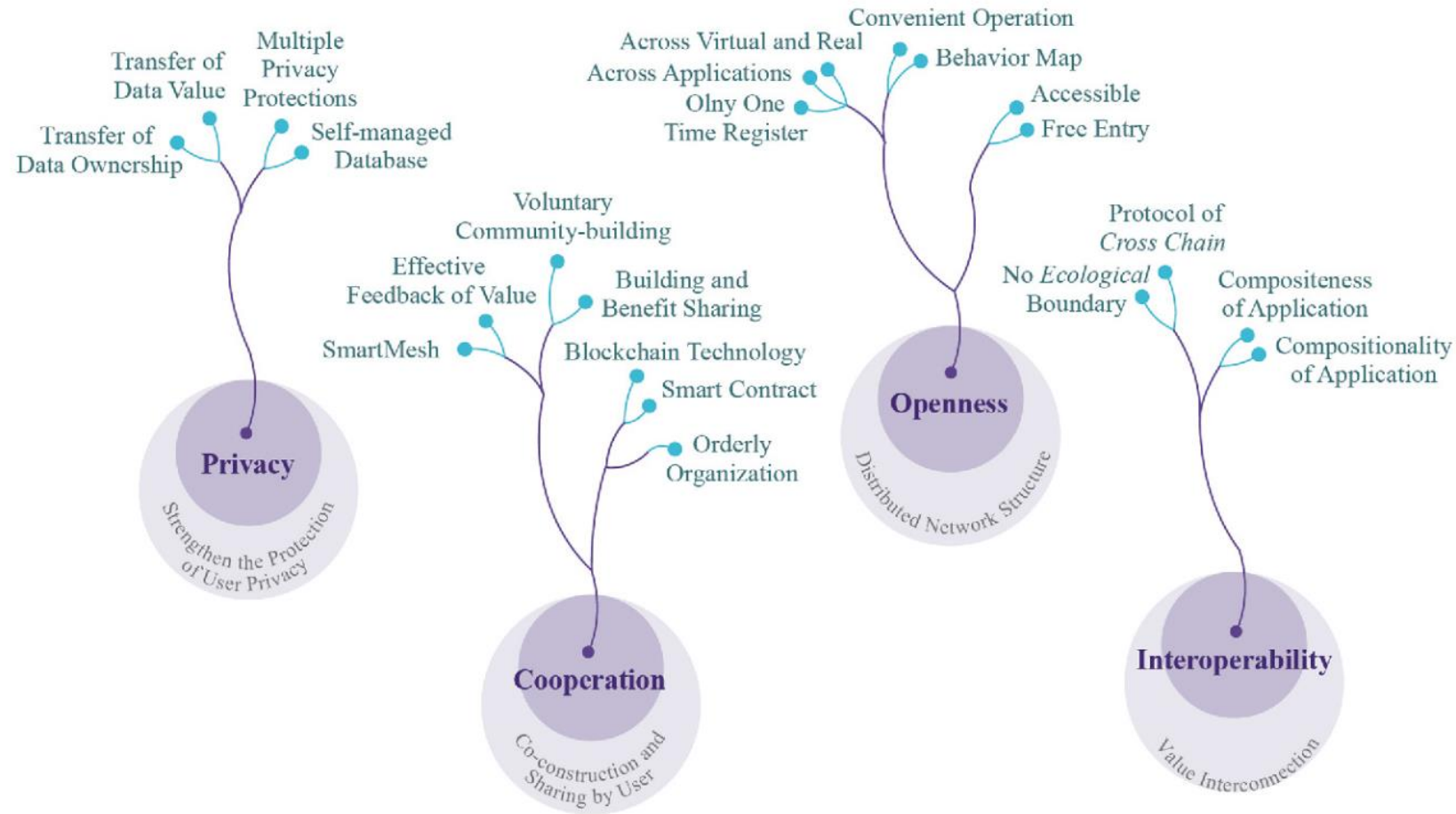
Openness—Distributed Network Architecture

- Users enjoy unrestricted access and encounter minimal barriers when entering a particular "field" of Internet applications.

- User behavior is no longer confined by third-party entities, leading to the dissolution of traditional boundaries and barriers between different Internet application ecosystems.

- The "cross- chain" protocol facilitates interconnectivity among diverse infrastructure-based applications within the Web 3.0 ecosystem.

Privacy—Enhanced User Privacy Protection

- Users are increasingly inclined to safeguard their personal data privacy comprehensively, aiming to achieve data ownership and value transfer.

- User data in the Web 3.0 era is no longer under the ownership of platforms; instead, ownership is transferred to decentralized individuals.

Co-creativity—Users Build and Share Content Together

- By leveraging the token incentive mechanism, effectively rewarding content creators in the emerging content economy.
- The incentive mechanism of Web 3.0 motivates users within the same community to actively contribute, participate in collective governance, and share the resulting benefits.
- The development of the Web 3.0 ecosystem, including applications, tools, and protocols, relies heavily on collaboration, and the organizational structure that enables users to collaborate effectively is known as a DAO (Decentralized Autonomous Organization)

History of Web 3.0

	Web 1.0	Web 2.0	Web 3.0
Time	1991-2004	From 2004 to Now	From 2014 to Future
Technology	HTML\ASP\PHP	HTML5\JS\RSS	Blockchain\OWL
Attribute	Hyper Text	Social Networks	Semanticweb
Medium	Static Text	Interactive Content	Fictitious Economy
Infrastructure	Personal Computer	Cloud & Mobile Devices	Blockchain
Model	Read-only	Interactive	Intelligent Execution

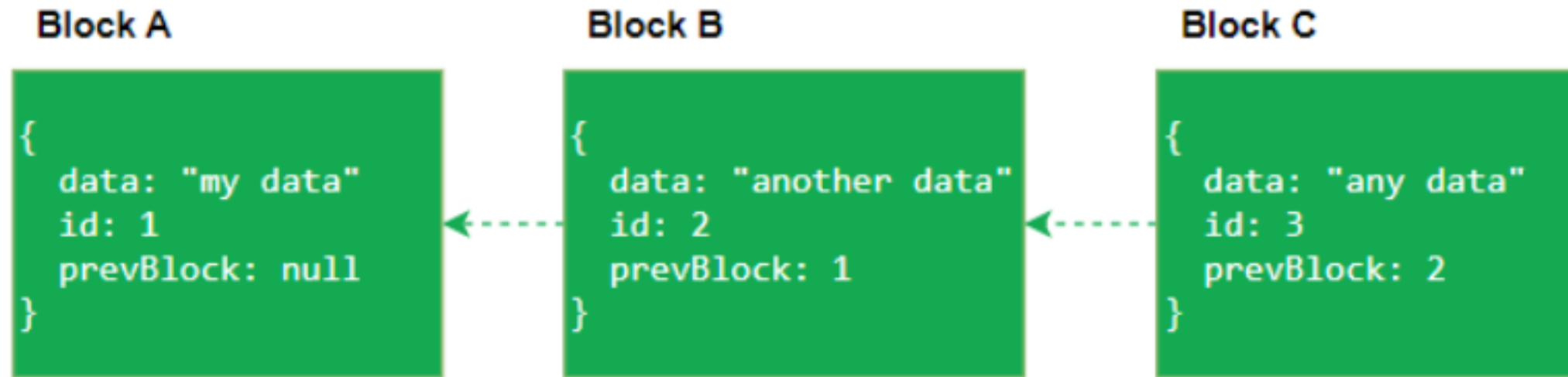# Infrastructure of Web 3.0

- Blockchain: Underlying Architecture
- Smart Contracts: Summary and Guarantee
- DAO: Organizational Form
- Token: Equity Vehicle

Blockchain

- A blockchain consists of interconnected blocks, each containing specific information and arranged chronologically.

- The blocks maintain accuracy by including the hash value of the previous block .

- The entire chain is stored on all nodes, and the servers within the system provide storage space and computational support for the blockchain system as a whole.

- Every network node within the blockchain stores the same data, and any modification to a file (such as a transaction) by any node requires confirmation and consensus from over half of the nodes.

- Once information changes, all participants on the chain become aware of it, making tampering with blockchain data extremely difficult.
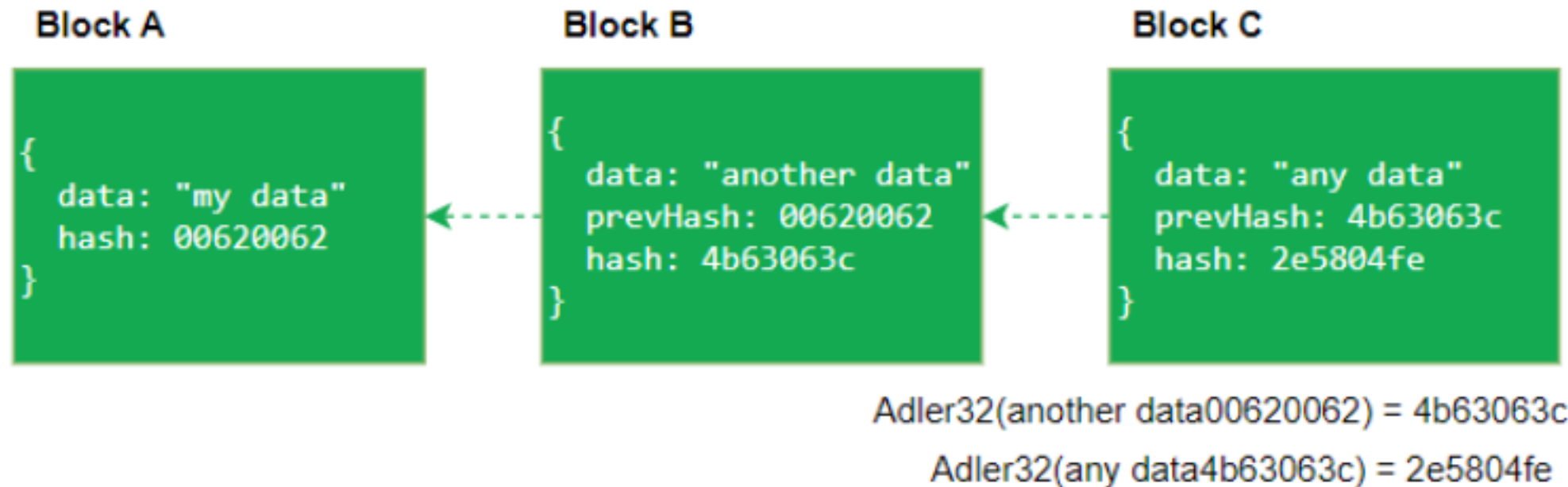
Blockchain

Blockchain refers to a series of data blocks that are linked together.

Block A

```
{
  data: "my data"
  id: 1
  prevBlock: null
}
```

Block B

```
{
  data: "another data"
  id: 2
  prevBlock: 1
}
```

Block C

```
{
  data: "any data"
  id: 3
  prevBlock: 2
}
```

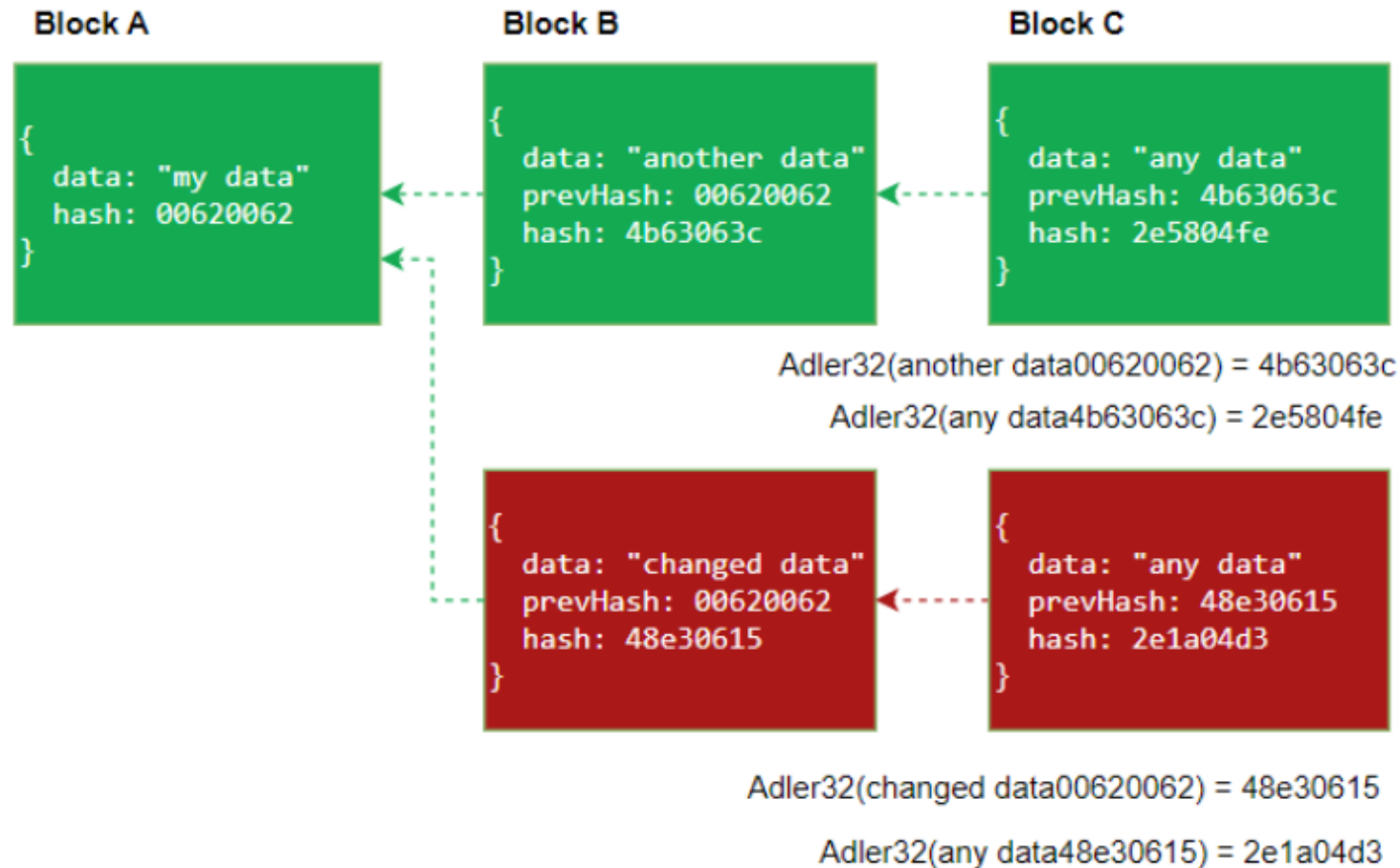https://saigontechnology.com/blog/introduce-to-blockchain-technology/

Blockchain

To enhance the security and integrity of the blockchain, each block is encrypted using a hash function and linked to the previous block through the resulting hashed token

Block A

```
{
  data: "my data"
  hash: 00620062
}
```

Block B

```
{
  data: "another data"
  prevHash: 00620062
  hash: 4b63063c
}
```

Block C

```
{
  data: "any data"
  prevHash: 4b63063c
  hash: 2e5804fe
}
```

Adler32(another data00620062) = 4b63063c

Adler32(any data4b63063c) = 2e5804fe

https://saigontechnology.com/blog/introduce-to-blockchain-technology/

Blockchain

Block A

```
{
  data: "my data"
  hash: 00620062
}
```

Block B

```
{
  data: "another data"
  prevHash: 00620062
  hash: 4b63063c
}
```

Block C

```
{
  data: "any data"
  prevHash: 4b63063c
  hash: 2e5804fe
}
```

Adler32(another data00620062) = 4b63063c

Adler32(any data4b63063c) = 2e5804fe

```
{
  data: "changed data"
  prevHash: 00620062
  hash: 48e30615
}
```

```
{
  data: "any data"
  prevHash: 48e30615
  hash: 2e1a04d3
}
```

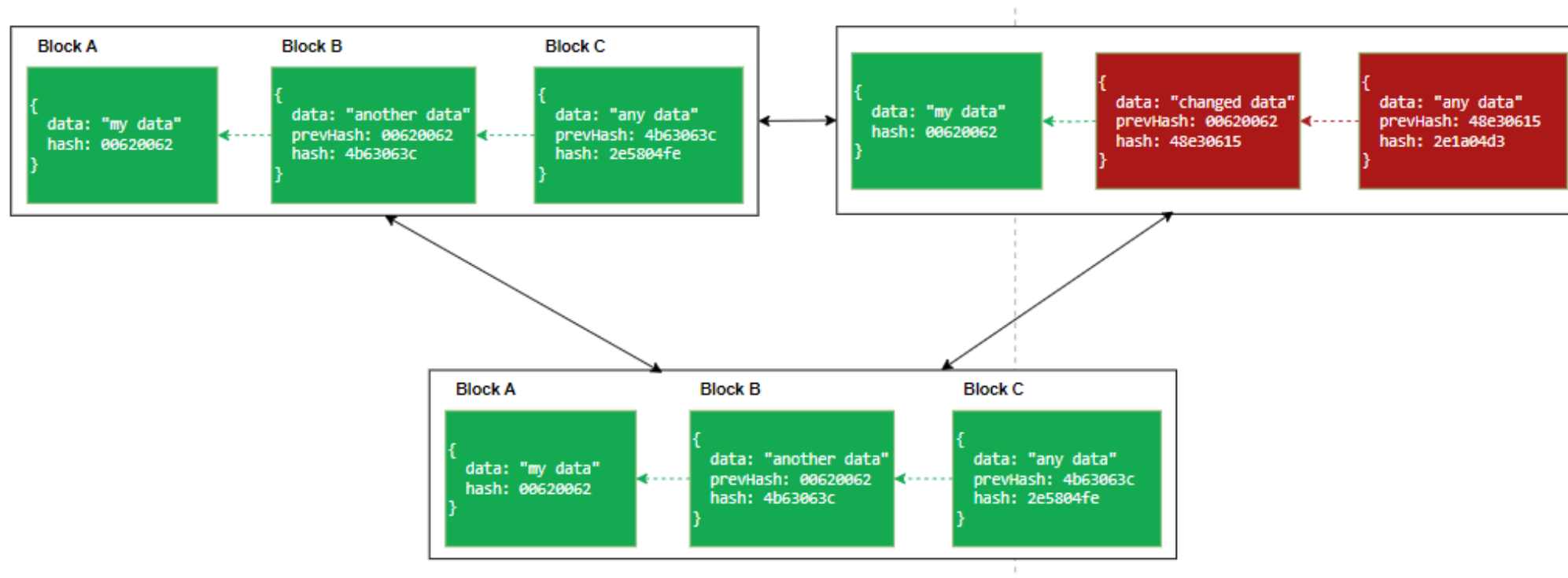Adler32(changed data00620062) = 48e30615

Adler32(any data48e30615) = 2e1a04d3

In the event that an attempt is made to alter the information contained within a block, the hash signature will change and the chain will be broken

https://saigontechnology.com/blog/introduce-to-blockchain-technology/
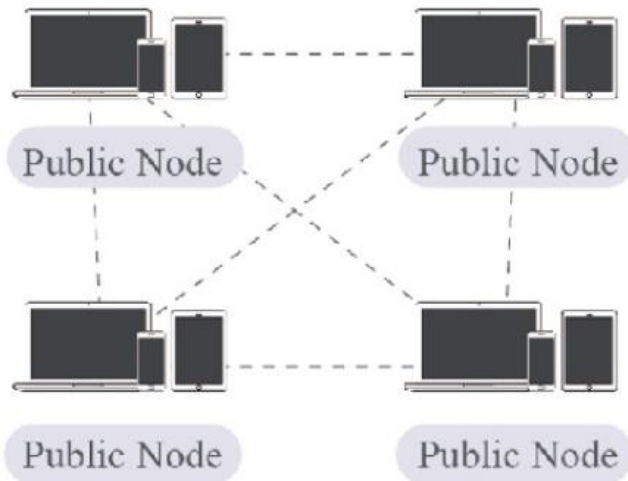
Blockchain

Create multiple copies of the blockchain and store them on different nodes owned by various stakeholders, with each node maintaining its own version of the data
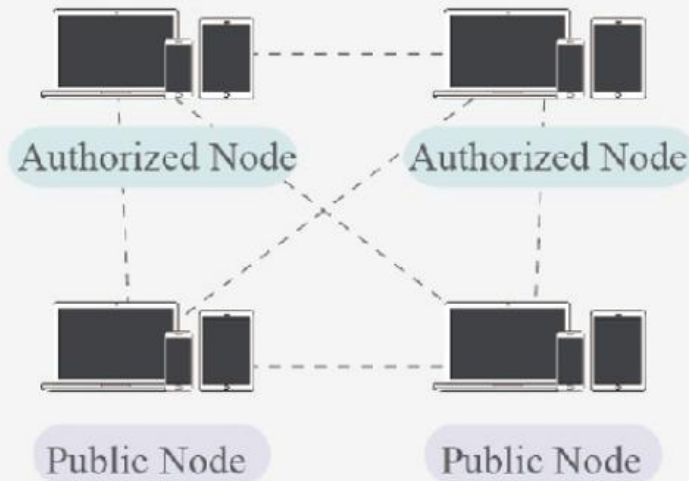

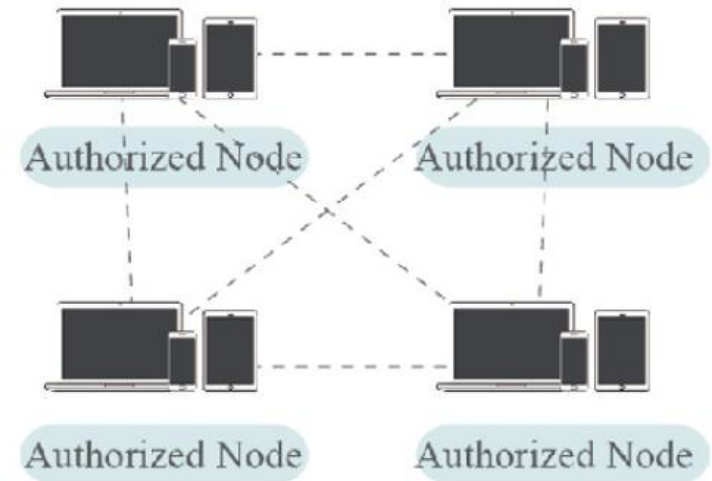https://saigontechnology.com/blog/introduce-to-blockchain-technology/

Blockchain Categories

Public Blockchains

Public Node   Public Node

Public Node   Public Node

Consortium Blockchain

Authorized Node   Authorized Node

Public Node   Public Node

Private Blockchain

Authorized Node   Authorized Node

Authorized Node   Authorized Node
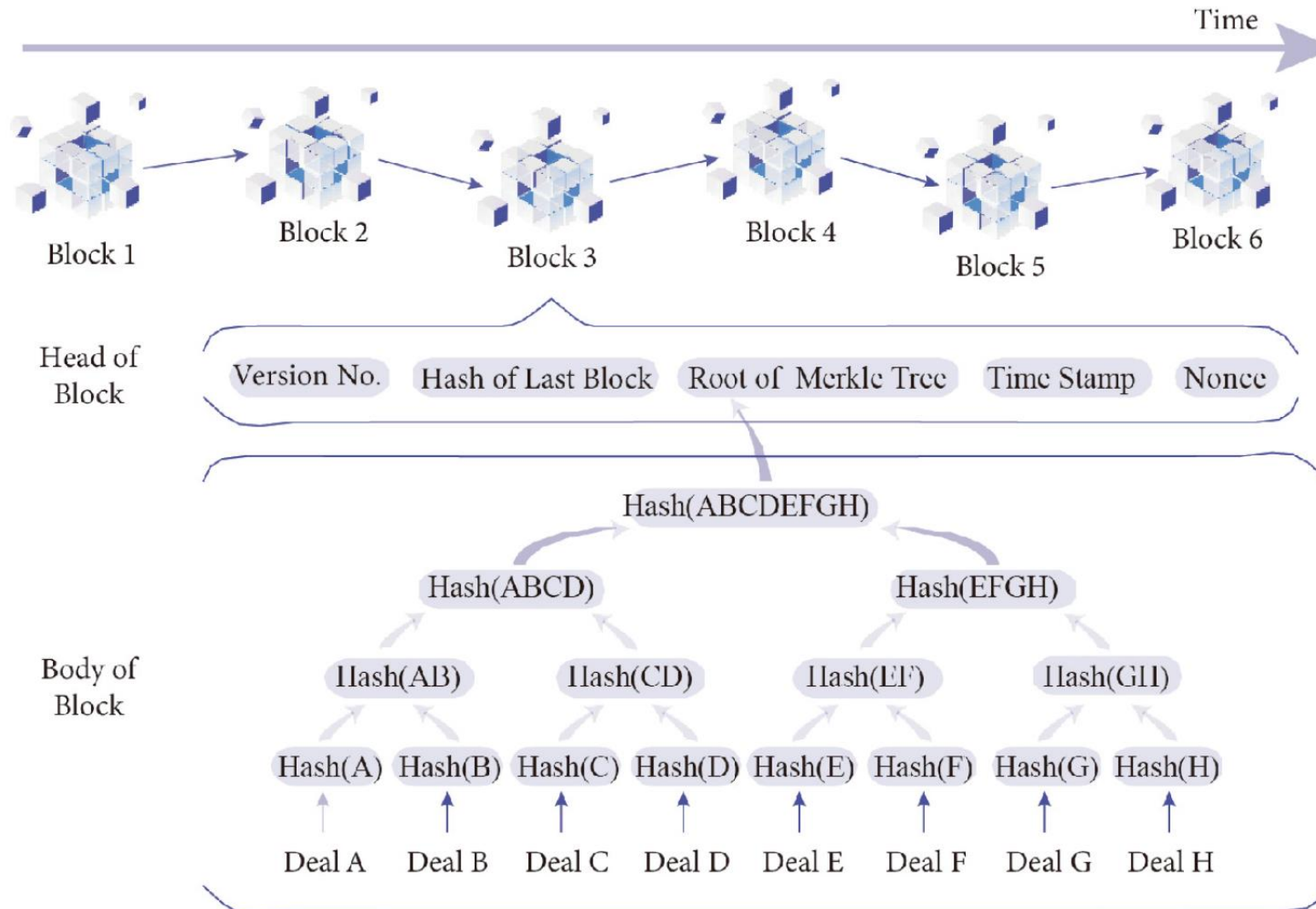
Example: Bitcoin data structure

The concept of blockchain was initially formulated by Satoshi Nakamoto in 2008. Notably, Bitcoin (BTC) stands as the exemplar of a blockchain product, with Ethereum (ETH) serving as another noteworthy representative within the realm of blockchain technology.

Bitcoin and Ethereum

	Bitcoin	Ethereum
Basic type	Transaction Based on Ledger	Account Based Ledger
Structure of Data	Hash Pointers + Merkel Tree	Hash Pointers + MPT Tree
Rules for Determination of Bookkeeping Rights	Proof of Work(PoW)	Proof of Stack(PoS) + Proof of Work(PoW)
Script Language	Simple Scripting Language	Solidity(Turing-complete)
Total Tokens	Fixed	Unfixed
Out Time of Block	10 min	15 s

Smart Contract: Contract Codification & Execution

- computer program capable of consistent execution across network nodes that maintain no mutual trust and,

- operate devoid of central oversight

- Typically Runs On top of Blockchain, ex: Ethereum/Binance/Solana

|	Bitcoin	Ethereum's Smart Contract
Using	Basic script	Solidity (Turing Complete)
Function	for verifying block and transaction legitimacy	as programming medium for diverse functionality

- Empower decentralization , ensuring transparent, uniform execution across all nodes

Smart Contract: challenges

- Blockchain time constraint, cannot exceed conventional applications
- It's hard to change smart contracts post-deployment.
- Invocation of smart contract on Ethereum requires processing fee to be paid "gas fee"

- Traditional vs DAO
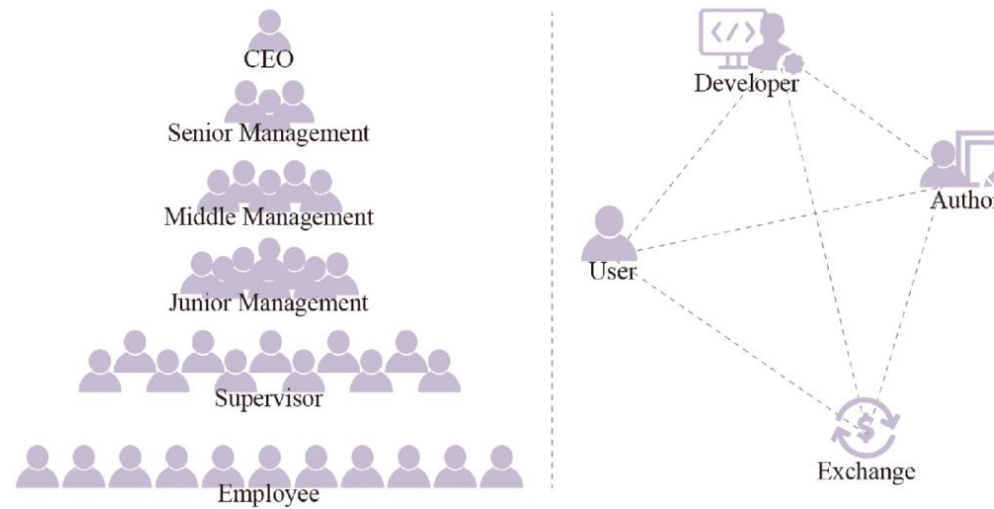
- Characteristics
    - Single legal entity
    - Necessity for labor contracts
    - Salary-based incentives

DAOs (Decentralized Autonomous Organizations)

- Built on Smart Contract, is a form of organization that runs on blockchain

- Facilitates Decision making process using Voting protocol, typically proportional to the ownership of coins (eg. 1 coin 1 vote/1T1V).

- Characteristics
  - Absence of centralized legal entity
  - Algorithms driving contract ops
 - Tokens Serving as incentives

	DAO	Traditional Organizations
Management Model	Distributed	Graded Management
Money Flow	Transparent	Almost Opaque
Mode of Operation	Open	Private

Token as Equity Vehicle

- Tokens: Fundamental Unit carrying interests within blockchain and "atomic" unit of Web 3.0
- Blockchain = immutable decentralized public ledger
- However, maintaining ledger is costly, thus token rewards are provided as incentive for bookkeeping tasks
- Represents
  - Ownership
  - Symbolize various assets

Token as Equity Vehicle

- Classification and application of asset-based tokens
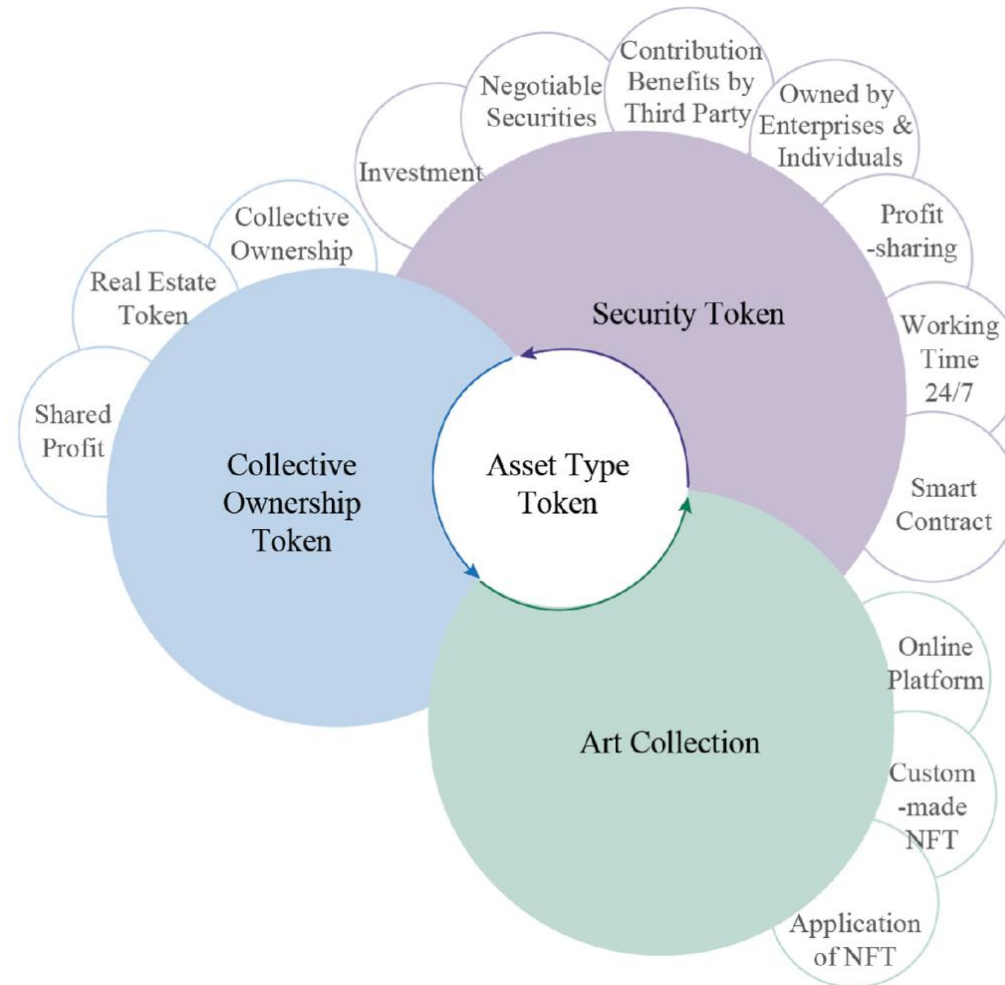
Companies and Application maps