803400815101 Blockchain and Smart Contracts

Artificial Intelligence Technologies Program (Graduate)

Graduate School of Natural and Applied Sciences

2023 - 2024 Spring Semester

ANKARA UNIVERSITY

The First University of The Republic of Turkey

Introduction to Blockchain and Basics

Assist. Prof. Dr. Murat KARAKUS

mrtkarakus@ankara.edu.tr

Department of Software Engineering

Faculty of Engineering

Ankara University

Outline

- Topics to cover:
  - Blockchain System
  - Blockchain Concepts
  - Blockchain Types
  - Mining Concepts and Its Use in Blockchain
  - Intro to Encryption and Cryptography in Blockchain
  - Distributed Ledger Technology Concepts and Types

Some Forewords…

- Evolution of Banking Since the 15th Century
  - Medici Family's Role in Modern Banking
- Impact of the 2008 Global Financial Crisis
  - Changing Consumer Perceptions
- Erosion of Trust in the Banking and Finance Sector
  - Loss of Trust in Banks and Regulators
  - Criticisms of Central Banks
- The Challenge of Rebuilding Trust

Some Forewords…

- 2008 Financial Crisis and Lehman Brothers
  - September Bankruptcy

- Emergence of Bitcoin
  - Pseudonymous Author: "Satoshi Nakamoto"
  - Publication: "Bitcoin: A Peer-to-Peer Electronic Cash System"
  - Ongoing Mystery Surrounding Satoshi's Identity

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

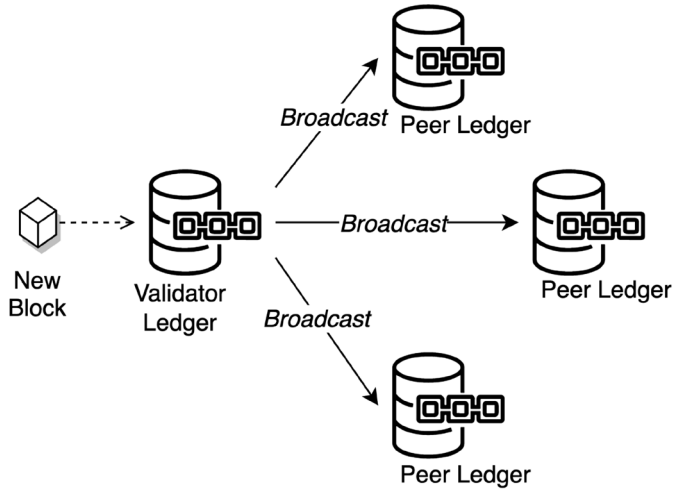
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties

Some Forewords…

- Introduction of Bitcoin
  - Decentralized Digital Currency
  - Protection Against Manipulation
- Data Recording and Distribution
  - Strong Encryption (Cryptography)
  - Distributed to All Users, Not a Central Authority
- Nakamoto's Influence
  - Notable Technological Concept
  - Rapid Development
  - Universal Acceptance
- Impact of Blockchain Technology
  - Transformation in Data Replication Concepts



Some Forewords…

- Blockchain and Data Copying
  - Permits Data Copying
  - Restricts Copies within Distributed Ledger
- Digital Inflation Mitigation
  - Elimination of Digital Inflation Problem
- Enablement of Cryptocurrencies
  - Foundation for Crypto Money Applications

Some Forewords…

- Bitcoin as a Disruptive Force
  - Anarchist Challenge to Traditional Finance
- Banking Crisis Accelerating Bitcoin's Rise
  - Transforming into a Rescuer
- Key Conceptual Components
  - Not Exclusive to Satoshi Nakamoto
  - Preceding Articles from the 90s

Some Forewords…

- [1]1991: Haber and Stornetta
  - Crypto Signatures and Timestamps

    [1]How to Time-Stamp a Digital Document", Stuart Haber, and W. Scott Stornetta, In Advances in Cryptology - Crypto '90, pp. 437-455. Lecture Notes in Computer Science v. 537, Springer-Verlag, Berlin 1991.
- [2]1996: Ross Anderson
  - Decentralized Data Storage
  - Immutable Saved Updates

    [2]The Eternity Service, Ross J. Anderson. Pragocrypt 1996.
- [3]1998: Schneier and Kelsey
  - Encryption for Sensitive Log Files
  - Protection on Untrusted Machines

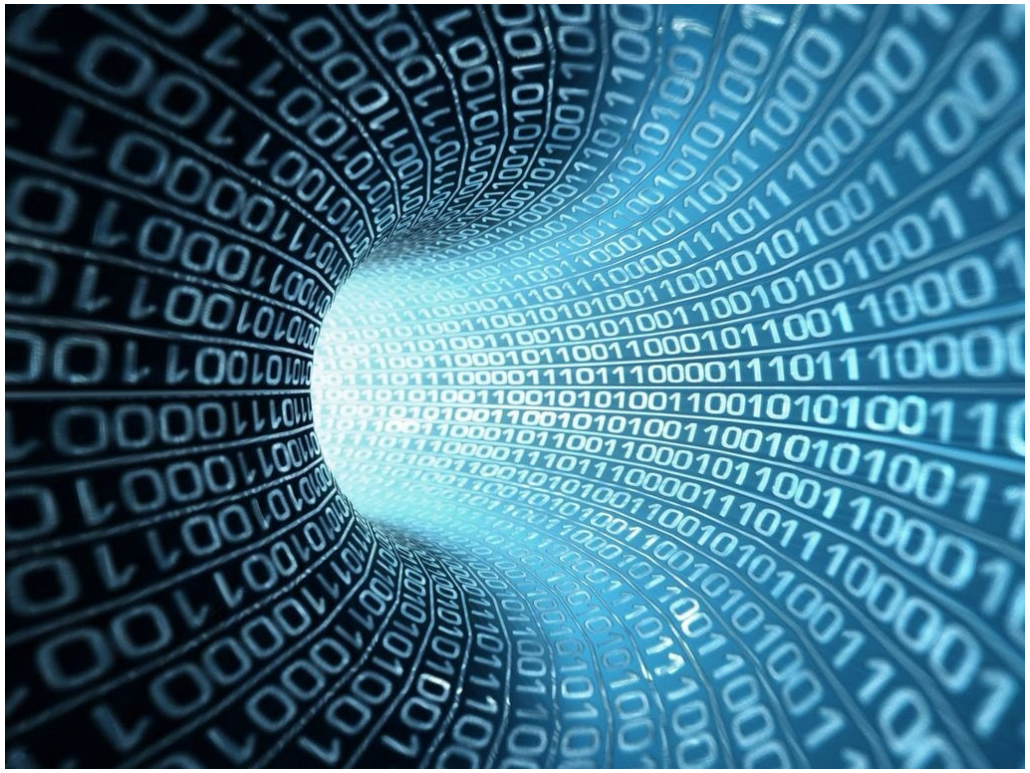
    [3]Cryptographic Support for Secure Logs on Untrusted Machines, Bruce Schneier, and John Kelsey, in The Seventh USENIX Security Symposium Proceedings, pp. 53-62. USENIX Press, January 1998.

Basic Concepts

- Understanding Blockchain Technology
  - Basic Concepts such as
    - Data
    - Databases
    - Network Technologies
    - Cryptography

Basic Concepts
What is Data?

- Turkish Equivalent of "Data"
  - Normalizing in Daily Language
- Definition: Raw Information
- Data Collection Methods
  - Measurement, Counting, Experiment, Observation, Research
- Quantitative Data
  - Numeric Values
- Qualitative Data
  - Non-Numeric Information



Basic Concepts
What is Data?

- Data's Meaningfulness
  - Aggregation, Sorting, Summarization
  - Manual or Computer Processing
- Transformation into Information
  - Enabling Explanation and Problem Solving
  - Supporting Decision-Making
- Diverse Data Sources
  - Unrecorded Data Examples
- Non-Human Data Generation
  - Cosmic Rays and Electrons

Basic Concepts
Databases

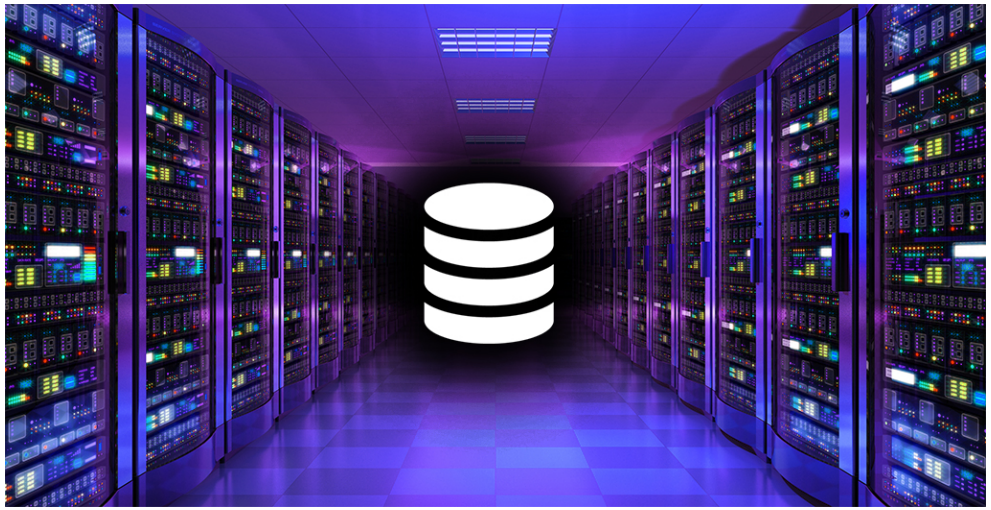
- Punched Cards for Data Storage
  - Careful Organization in Cabinets
- Evolution of Data Storage
  - Transition to Analog, Magnetic, and Digital Systems
  - Increased Demand for Data Storage Since the 1950s
- Impact on Librarianship and Archiving
  - Modernization and Adaptation to Computer Systems

Basic Concepts
Databases

- The "1960s computer systems used "database."
- The Saturn V rocket parts database is the first modern application in this sector.
- Until the 1970s, all databases were fundamentally notebook applications for text-only content.
- In 1973, Edgar Codd of IBM San Jose Research Laboratory defined "Relational Database," a groundbreaking concept.

Basic Concepts
Databases

- Limitations of Spreadsheets
  - Not Ideal for Data Storage and Analysis
- Petabyte-Sized Databases
  - Capacity for Trillions of Rows
- Emergence of NoSQL Databases
  - Since the 2000s
- Fixed Structured Single Schemas
  - Quick Search in Big Data Collections
- Google's Use of NoSQL Database
  - Fast Concept Retrieval in Billions of Web Pages



Basic Concepts
Databases

- Cloud storage and database services are available.
- Amazon offers RDS, DynamoDB, and Redshift.
- Hardware becomes apps and applications become services.
- Cloud solutions offer cost-effective infrastructures.
- Yet, technological growth continues.

Basic Concepts
Infinity and Beyond

- Vast Number of Stars in City-Free Sky
- Limited Exploration of Universe's Stars
- Proliferation of Internet-Connected Devices
  - Outnumbering Humans
- Rapid Growth of Trillion-Dollar IoT Economy
- **Can all this system's data be distributedly stored?**

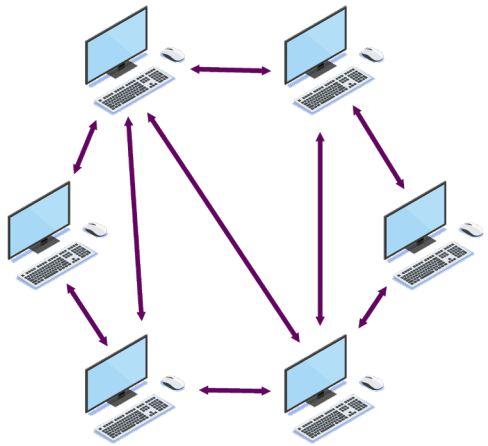
Basic Concepts
Infinity and Beyond

- Actually, the answer to this question was given many years ago.

- eDonkey and BitTorrent
  - Independent Projects in the Early 2000s

- Peer-To-Peer (P2P) Data Sharing
  - Developed for Sharing Data with Others
  - Communication with Unknown Machines

- Internet-Based Storage Solution



Basic Concepts
Infinity and Beyond

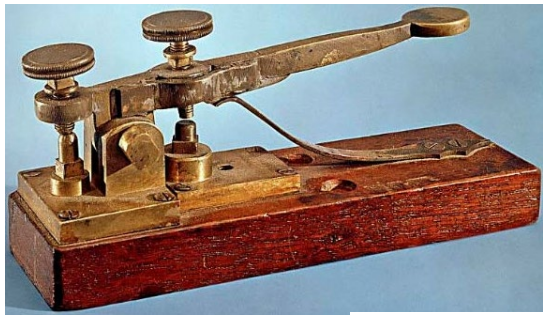
- Data Distribution Across Millions of Devices
- Machines Holding All or Part of Data
- Efficient Retrieval from Multiple Devices
- Data Exchange with Other Users

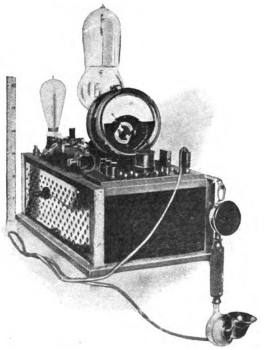
Basic Concepts
Infinity and Beyond

- Direct Benefits for Users
- Storage Alternative to Cloud
  - Content Not Protected
  - Lack of Storage Options
- Evolution into Distributed Ledger Systems
- Foundation for Discussing Blockchain Technology

Basic Concepts
A Brief History of Network Technologies

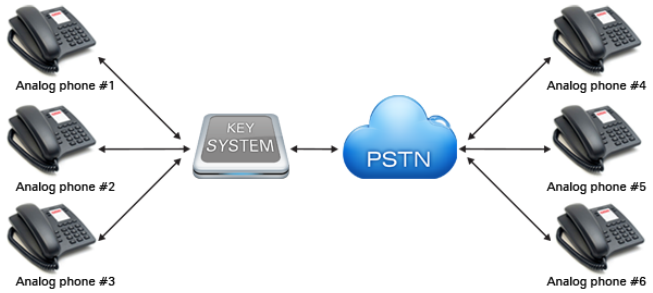
- Electricity's Impact on Communication Tech
- 1830: Joseph Henry's Remote Bell-Ringing Mechanism
- 1835: Samuel Morse's Magnetic Telegraph and Morse Code
- Late 1800s: Introduction of the Radiophone
- Alexander Graham Bell and Charles Sumner Tainter's Contribution





Basic Concepts
A Brief History of Network Technologies

- Germany invented Telex, a text-transfer system, in 1930.
- MODEM was invented in 1949.
- Bell Telecom commercialized MODEM technology in 1958.
- Telephone networks went digital in 1958.
- IBM established SABRE, a US airline network connecting 2000 terminals in 65 locations, in 1964.



Basic Concepts
A Brief History of Network Technologies

- ARPAnet: Pioneering Network (1969)
  - Connecting Multiple Computers
- Invention of Ethernet (1973)
  - By Xerox Engineers Metcalfe and Boggs
- Debut of Novell NetWare (1982)
  - First Network Operating System
- Creation of Mobile GSM Standards (1987)
- Publication of HTML by Tim Berners-Lee (1990)
  - Enabling the World Wide Web (WWW) Platform

Basic Concepts
A Brief History of Network Technologies

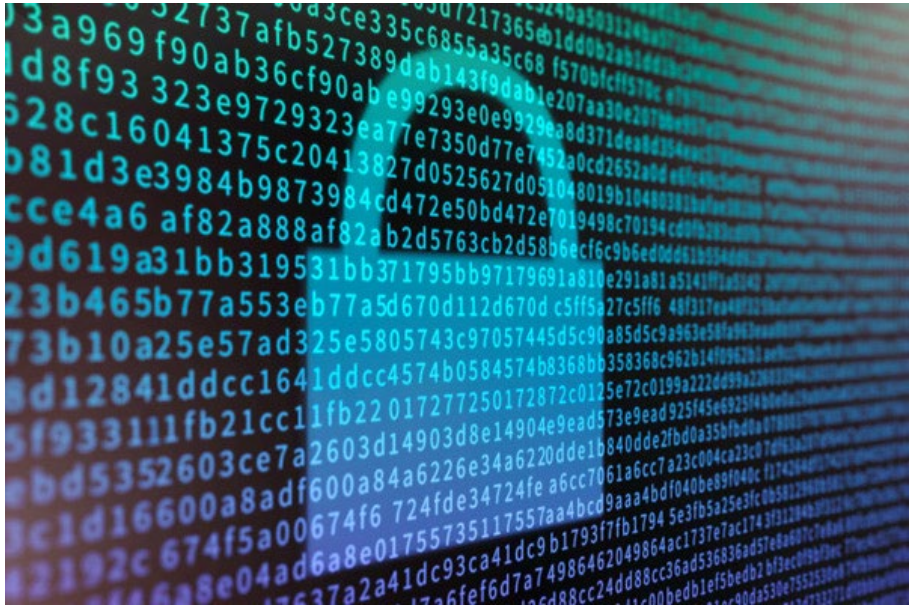
- The NSF made the Internet public in 1991.
- 36 million people were online by 1996.
- WiFi standards were developed in the 2000s.
- Mobile Web access became common after 2009.
- High-speed communication networks let blockchain technology expand quickly today.

Basic Concepts
Cryptology

- Significance of Cryptology in Blockchain Technology
- Historical emphasis on data protection
- Origins of Cryptology in the Ancient Greek "Kryptos"
- Study of Secrecy in Cryptology
- Cryptography as a subfield of Cryptology
- Derived from the Greek "graphien" (meaning writing)
- Encryption of data, including Texts

Basic Concepts
Cryptology

- Encryption Process
  - Converts Data into Seemingly Random Form
  - Utilizes a Rule Structure
- Key-Based Decryption
  - Key Needed to Revert to Original Form
- Data Meaningless without Key
  - Incomprehensible to Unauthorized Parties
- Data Security and Accessibility
  - Restricted to Key Owner

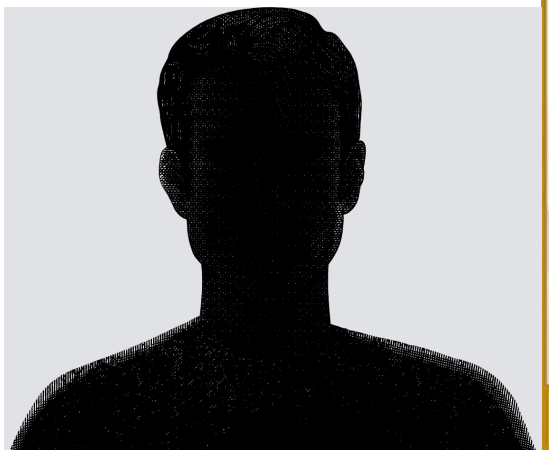


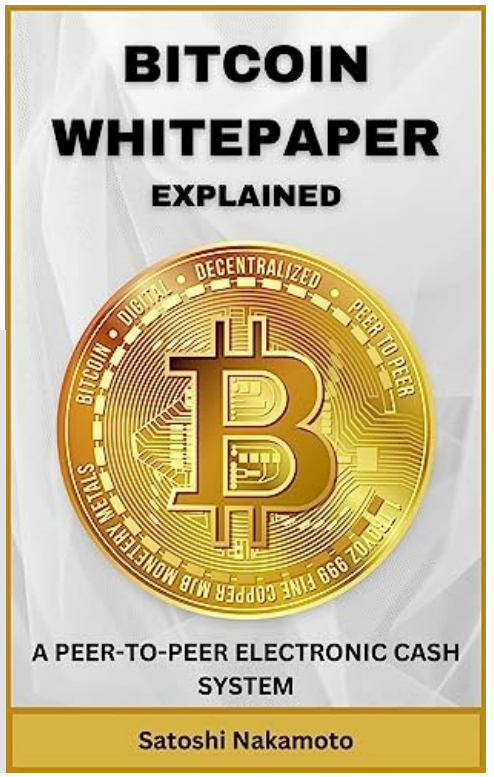
Basic Concepts
Philosophy of Blockchain Technology

- Historical Role of Data Records
  - Maintaining Order in Expanding Societies
- Governance and Documentation of Relationships
  - Crucial in Expanding Civilizations
- Formation of Organizations and Structures
  - To Create, Control, and Operate Records
  - Including Clubs, Foundations, Businesses, and States

Basic Concepts
Philosophy of Blockchain Technology

- Satoshi Nakamoto's Technical Paper
  - "Bitcoin: A Peer-to-Peer Electronic Cash System"
- Timing: Published After Lehman Brothers' 2008 Bankruptcy
- Key Message:
  - Secure Data Recording System
  - Decentralized Structure
  - Resistance to Manipulation and Corruption
  - Reliance on Mathematics and Technology





Basic Concepts
Philosophy of Blockchain Technology

- Understanding Blockchain Philosophy
  - Decentralized and Secure Data Recording
- Foundational Knowledge
  - Data, Databases, Communication Networks, Cryptography
- Implementing Decentralized and Secure Systems
- Transition to Blockchain Technology Operations

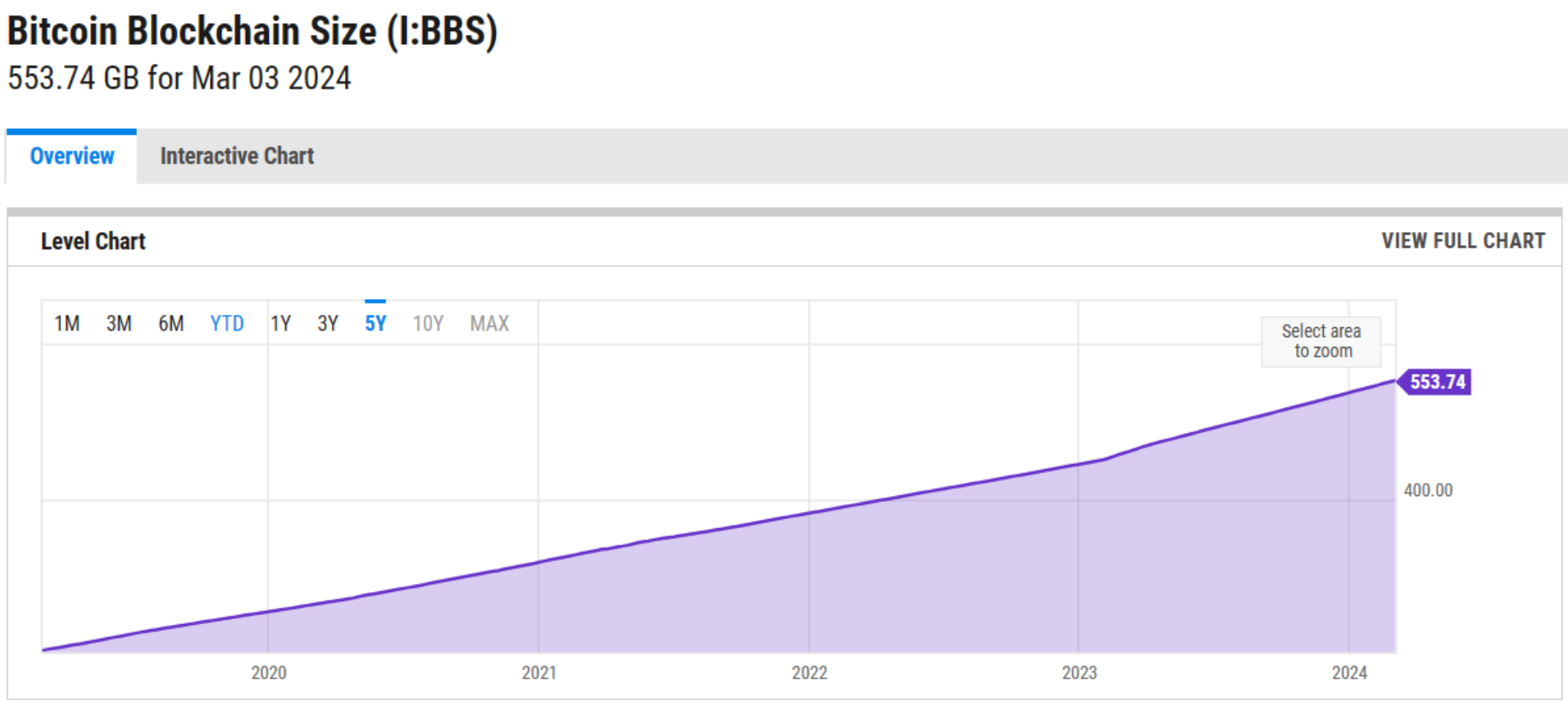
Introduction to the Blockchain World!

- Let us review all we have discussed.
  - No more central data storage.
  - Alternatively, we can store data in cloud or P2P services.
  - Cloud and P2P databases exist.
  - Since we have rapid communication networks, data can be transferred everywhere, regardless of size.
- This presents the first step necessary to enter the world of Blockchain.

Introduction to the Blockchain World!

- Blockchain as an expanding network
  - Comprising encrypted data chunks
- Chronological encryption of process data
- Blockchains as sequences of data blocks
  - Containing information of previous blocks
- Decentralized and distributed databases
- Data storage in blocks
- Timestamping of records
- Formation of new blocks when current one is full

Introduction to the Blockchain World!



- The Bitcoin blockchain file, which records all network transactions.

source: https://ycharts.com/indicators/bitcoin_blockchain_size

Introduction to the Blockchain World!
Phase 1: The Evolution of Digital Records

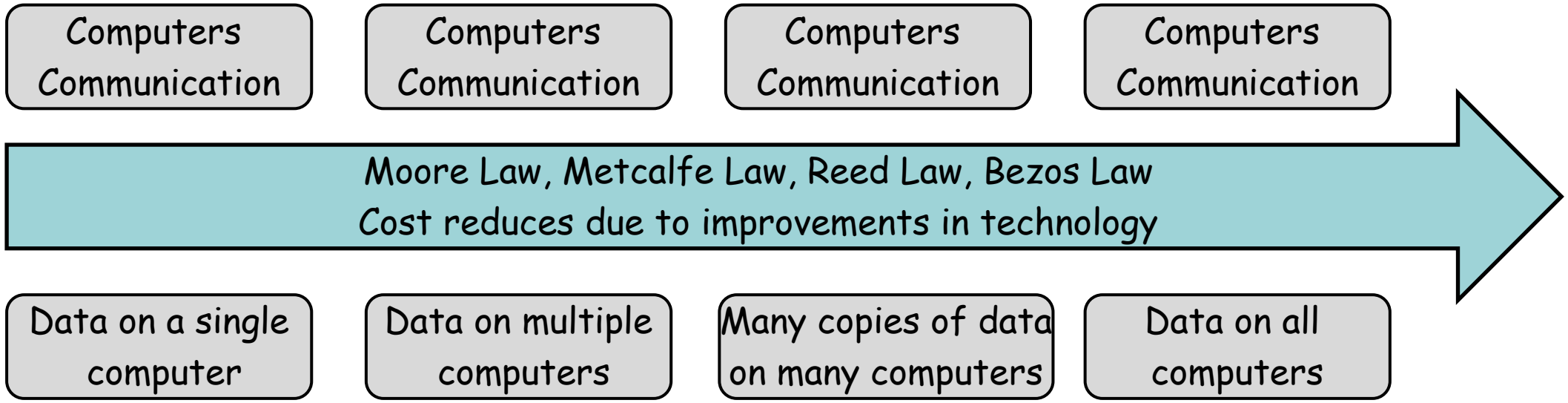


Figure 1: Evolution of Digital Records

Introduction to the Blockchain World!
Phase 1: The Evolution of Digital Records

- Moore's, Metcalfe's, Reed's, and Bezos' Laws
  - Rapid Technological Advancements
  - Cost Reduction Over Time

- Impact on Data Distribution
  - Use of Inexpensive Communication Networks

- Widespread Data Transfer Across Systems

Introduction to the Blockchain World!
Phase 1: The Evolution of Digital Records

- `Distributed Ledger` method
- Usage in eDonkey and BitTorrent
- Concerns about unsecured data
  - Open access
- Encryption of distributed ledger data
  - Limited access
- Benefits reserved for encryptor
- Possibility of data discrepancies due to network node updates
- Transition to the next phase

Introduction to the Blockchain World!

Phase 2: Attributes and Processes in a Distributed Ledger

- Data Standards in Multi-Party Systems
  - Preserving System Integrity
- Incorporating Unfamiliar Parties in Distributed Structures
  - Adhering to System Rules
- Rule Establishment During System Design
  - Flexibility for Necessary Changes
- "Consensus Structure" for Each Application
  - Overseeing Rule Set
- "Consensus Process" for Stakeholder Compliance in Consensus-Based Systems

Introduction to the Blockchain World!

Blockchain Transaction Structure

Figure 2: Tag

Introduction to the Blockchain World!

Blockchain Transaction Structure

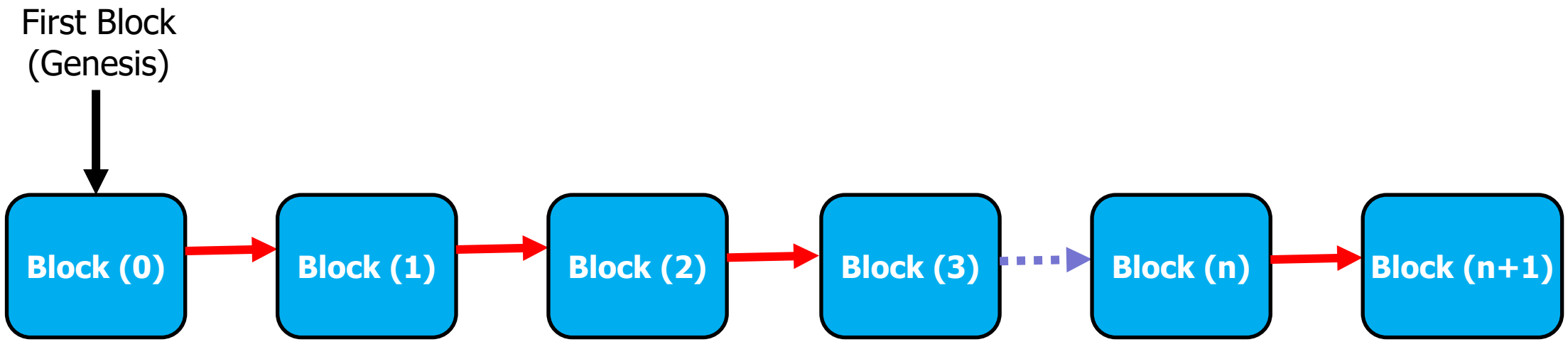


Figure 3: Structure in which all blocks follow each other after the *first block* (*Genesis*) record

Introduction to the Blockchain World!
Blockchain Transaction Structure

Transactions:

- Content Information in Blockchain Structure
  - Varied Types (e.g., Money Transfer, Fixture, Customer Records)
- Blockchain Design Specific
- Example: Digital Currencies
  - Records: Money Transfer Information
  - User-to-User Money Transfers
- Recording New Transfer Requests
  - Queueing and Inclusion in the Chain

Introduction to the Blockchain World!
Blockchain Order Structure

- Analogous Example: Labels and Rope
- Tag Removal Process
  - Shredding or Unknotting
  - Reknotting Remaining Tags
- Ability to Reposition Deleted Label
- Feasible but Challenging
- Recognizing the Threat
- Rebuilding the "Consensus Structure"
  - Adding New Rule to Tag Chain
- Iterative Play to Eliminate the Threat

Introduction to the Blockchain World!

Blockchain Order Structure

Figure 2: Tag

Introduction to the Blockchain World!

Blockchain Order Structure

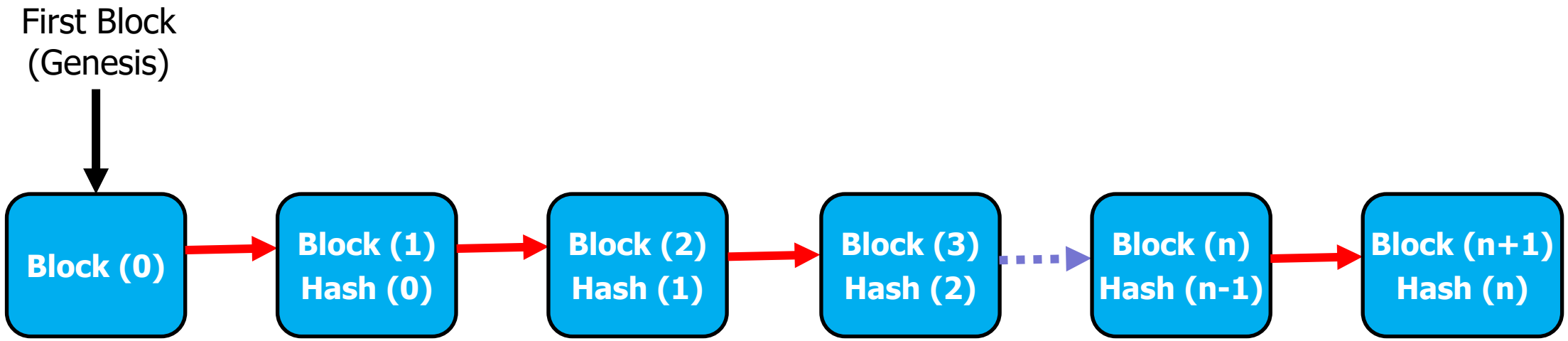


Figure 5: Structure in which all new blocks follow each other after the first block (Genesis) record, including the digital signature of the previous block

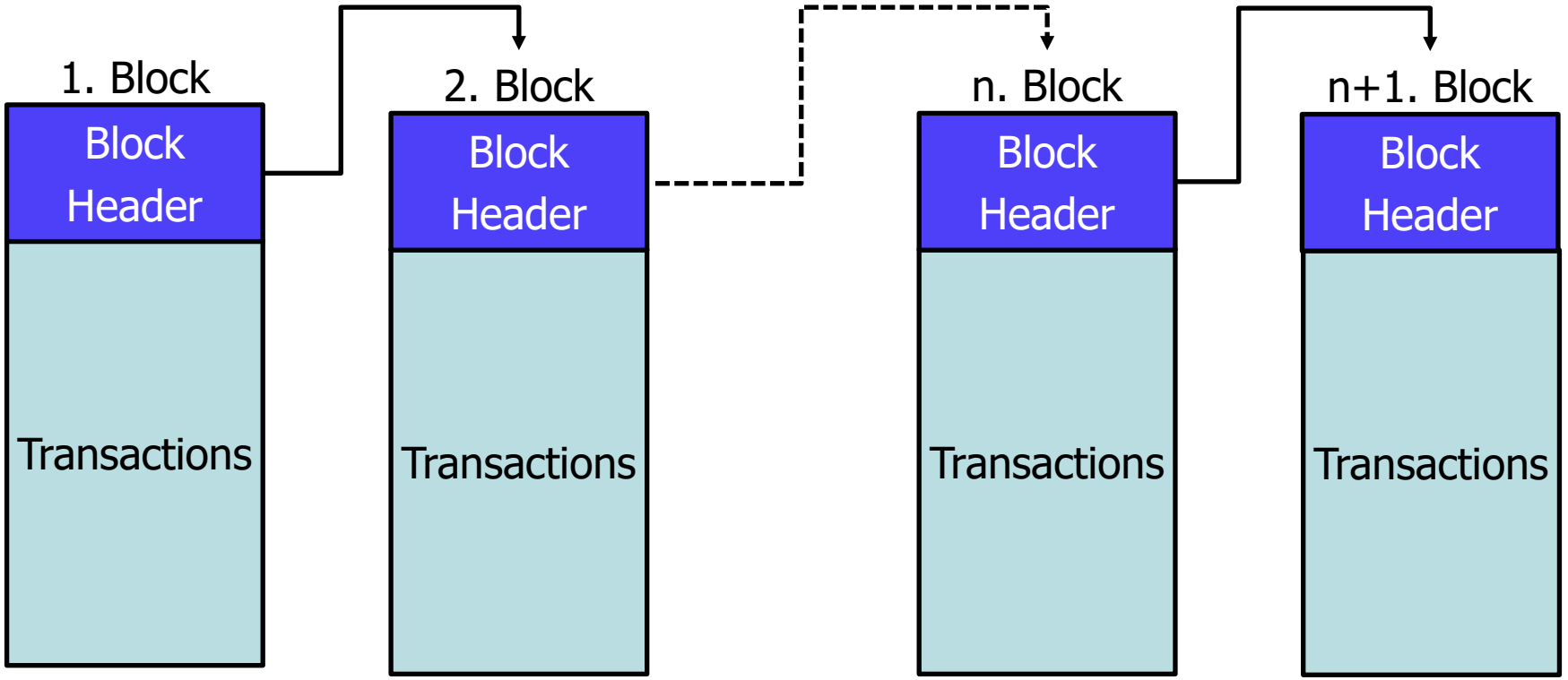
Introduction to the Blockchain World!
Blockchain Block Structure

Blocks:

- Record Processing and Block Writing
  - Regular Intervals
- Criteria for Block Creation
  - Determining Records and Transactions
- Utilization of Cryptographic Hash Techniques
  - Digital Signatures in Block Formation
- Chronological Linking of Blocks
  - Inclusion of Digital Fingerprints
- Ensuring Record Validation

Introduction to the Blockchain World!

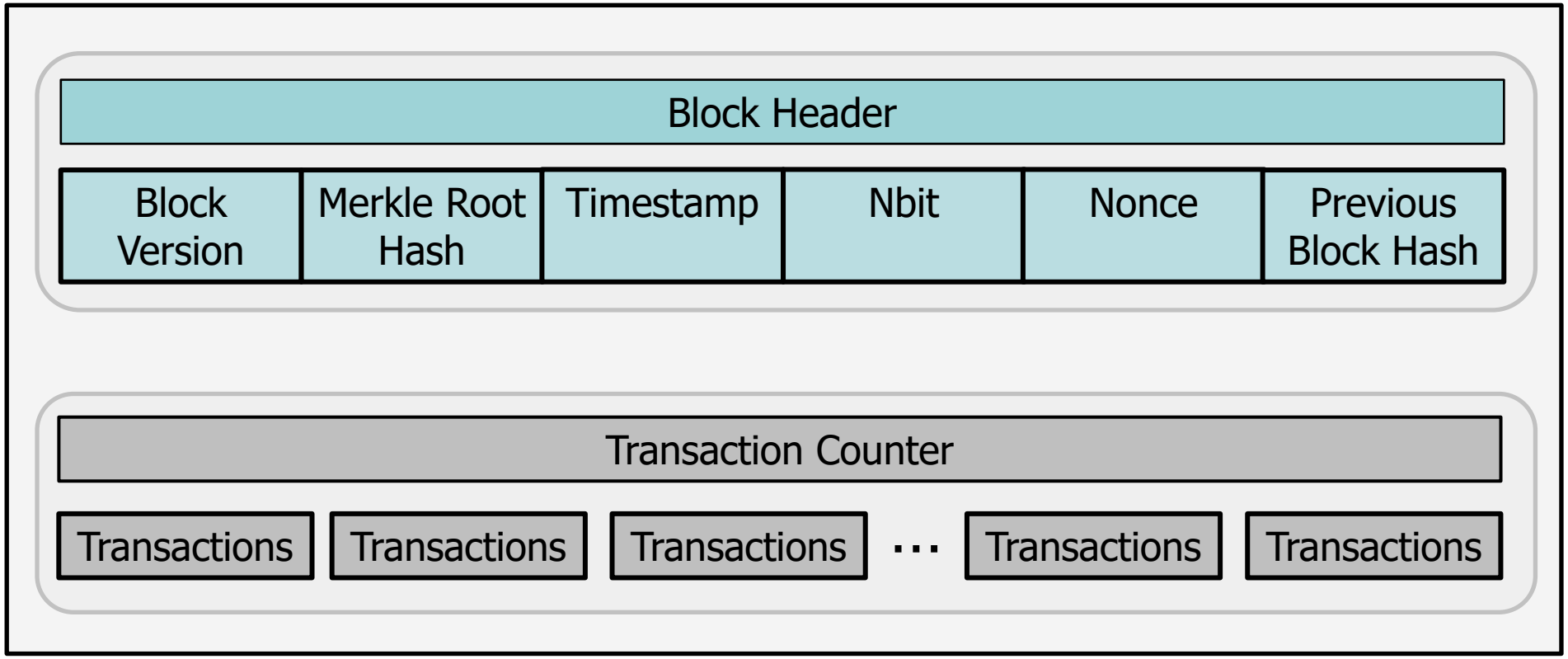
Blockchain Block Structure



General Block Structure (Representative)

Introduction to the Blockchain World!

Blockchain Block Structure



Block Header Structure (Representative)

Introduction to the Blockchain World!
Blockchain Block Structure

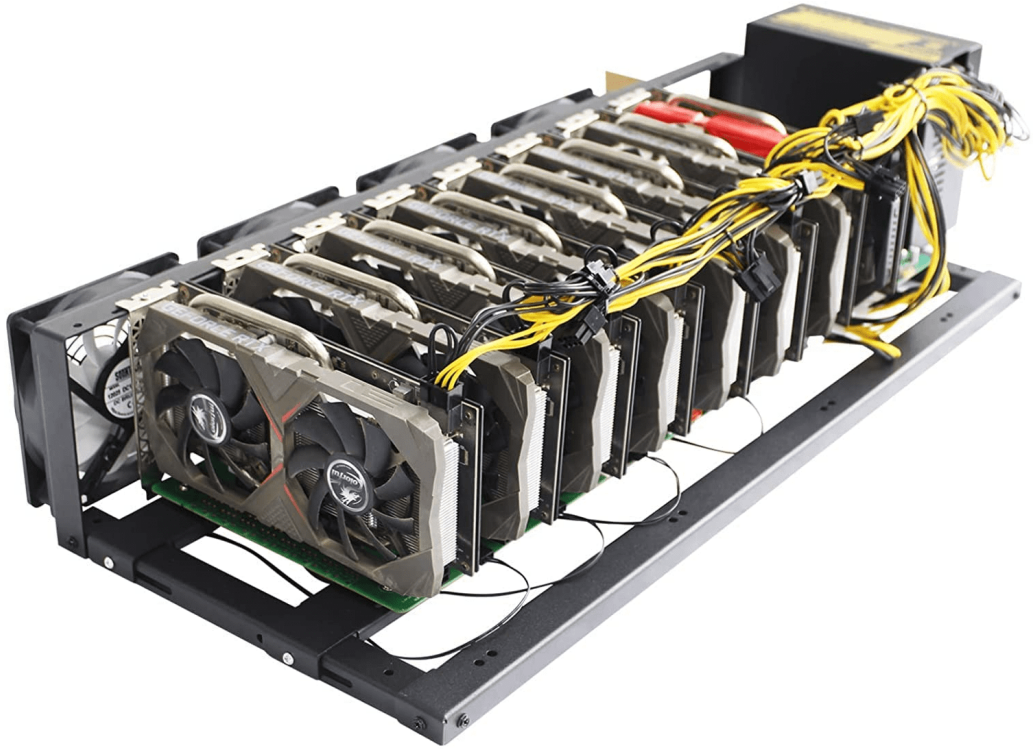
- Information in Block Header
  - Block Version
    - Determines Block Validation Rules
  - Merkle Root Hash
    - Holds Hash of All Transactions
  - Timestamp
    - Current Time in Universal Seconds
  - Nbit
    - Threshold Info for Valid Block Hash
  - Nonce
    - 4-Byte Field, Typically Starts at 0
    - Incremented for Each Calculation
  - Previous Block Hash
    - 256-Bit Value for Previous Block in Chain

Introduction to the Blockchain World!
The Concept of Mining and Its Use in Blockchain

- Mining and Blockchain Expansion
  - Addition of New Blocks and Transactions
- Competitive Mining
  - Race to Discover Hash Function Result
  - Determined by Difficulty Number
- Creation of Fresh Cryptocurrency
  - Utilizing the Blockchain
- Miners' Roles
  - Transaction Validation
  - New Block Creation

Introduction to the Blockchain World!

The Concept of Mining and Its Use in Blockchain



Mining equipment with GPU hardware

Mining equipment with ASIC system

Introduction to the Blockchain World!
Blockchain Distributed Structure

- Tag Example Scenario
- Peace of Mind for Most Participants
- Concerns for the Last-Place Participant
- Awareness of Signature Imitation
- Potential for Changing Record Order
- Necessity for a New "Consensus Procedure" Structure
- Suggestion of a Unique "Consensus Method" by Another Participant
- Addressing Signature Copying Abilities

Introduction to the Blockchain World!

Blockchain Distributed Structure

Ahmet's copy

Lale's copy

Serkan's copy

Buse's copy

Figure 6: In the tag game, everyone now has a copy of the tag chain.

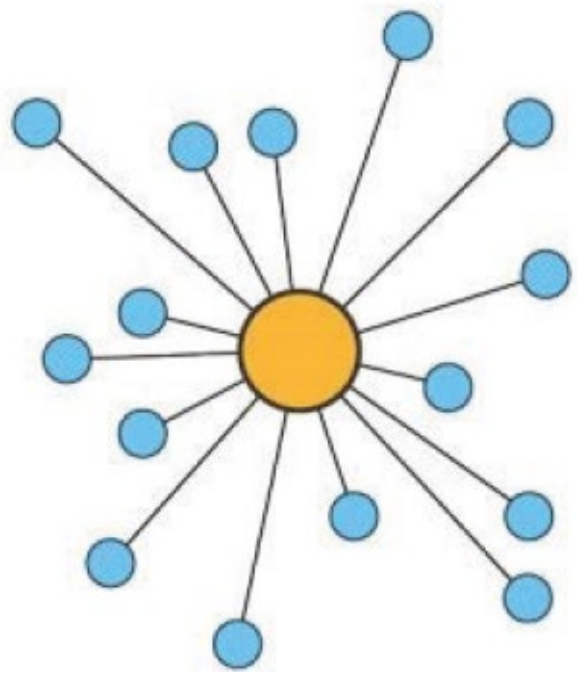
Introduction to the Blockchain World!
Blockchain Distributed Structure

- Distribution of Consensus Structure and Queue
- Copies of the Generated Chain Shared with All
- Prevention of Manipulation or Cheating
- Majority's Ability to Compare Records
- Sustaining Trust in Majority-Agreed Structure
- Exclusion of Cheaters and Rule Violators from the Game

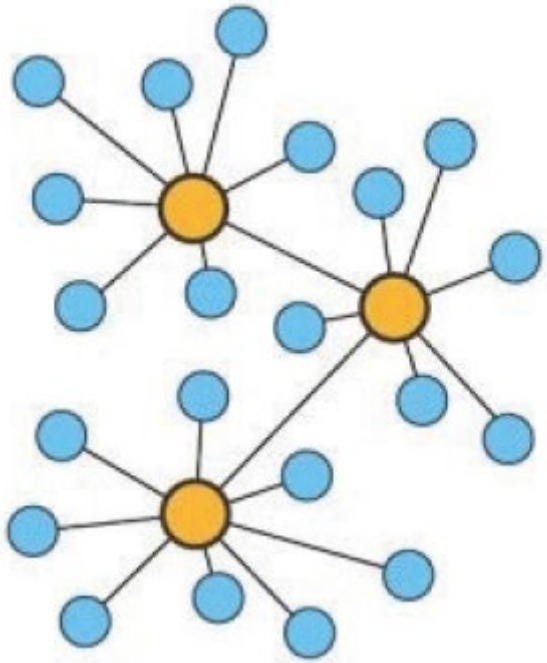
Introduction to the Blockchain World!

Blockchain Distributed Structure

Centralized



Decentralized



Distributed

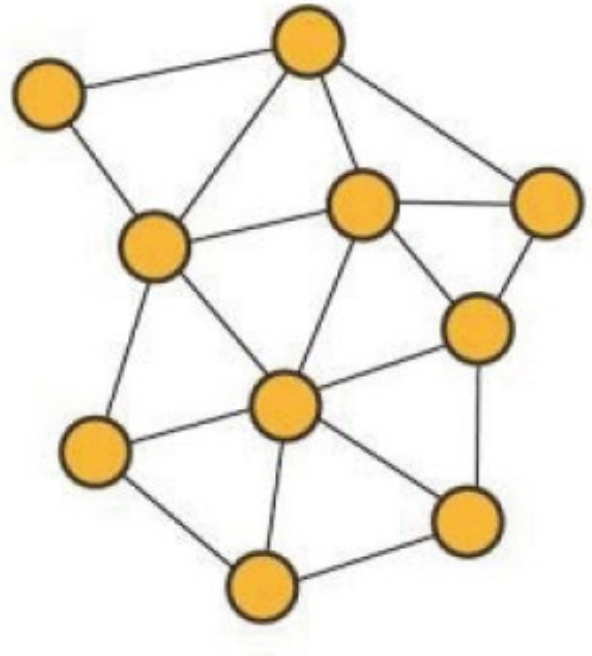


Figure 7: Network Structure

Introduction to the Blockchain World!
Blockchain Distributed Structure

- Blockchain framework
- Data recording by all system participants
- No requirement for participants to know each other
- Trust established via dissemination of record chain
- Based on the system's initial regulations

Introduction to the Blockchain World!
Blockchain Distributed Structure

- Uncorrupted System
  - Due to Communication Between Blockchain Record Distribution Sites

- Impact of Link Changes
  - Data Chain Structure Integrity
  - Removal of Point with Broken Link

- Continuity of the Chain
  - Rest of the System's Use
  - Based on Consenting to Sustain the Chain

Introduction to the Blockchain World!
Blockchain Types

- Comparison to Internet Technologies
  - Emphasizes Revolutionary Aspects
- Blockchain as a Single Infrastructure
  - Similar to Multiple Websites on the Internet
- Versatile Technology Technique
  - Enables Numerous Apps
- Adaptation Across Various Platforms and Approaches
- Four Categories for Classifying Platforms and Applications

Introduction to the Blockchain World!
Blockchain Types

Type 1: Fully Permissionless Blockchain Networks

- Fully Permissionless Blockchain Networks
  - Open Access, Reading, and Block Creation
- Inclusivity in "Consensus Mechanism"
  - Aiming to Engage All Participants
- Enhanced Security with More Network Users
  - Increased Data Chain Copies Across Points

Introduction to the Blockchain World!
Blockchain Types

- Demonstration with Public Plaza Tag Game
- Participants Must Present a Copy of Established Chain
- Immediate Inclusion in Ongoing Activity
- Benefits of the Network for Participants
  - Required Interest
- Emphasis on Value in Fully Permissionless Blockchain Networks

Introduction to the Blockchain World!
Blockchain Types

- Use of Bitcoin Platform in Fully Permissionless Blockchain Networks
- Participation in "Consensus Process" on Bitcoin Network
- Carrying the Data Chain for Network Security
- Verification of New Block "Consensus Structure"
- Rewards for Contributors of New Blocks
  - In Compliance with Network Rules
- Rewards in Bitcoin

Introduction to the Blockchain World!
Blockchain Types

Type 2: Partially Permissionless Blockchain Networks

- Partially Permissionless Blockchain Networks
  - Permission Required for Block Addition and "Consensus Process"
  - Aligned with Network's "Consensus Structure"
- Valuable Data in These Networks
- Networks Often Designed for Specific Objectives

Introduction to the Blockchain World!
Blockchain Types

- Analogy: Playing Tag with Close Friends
- Sharing Recordings as Memories
- Example: News Source Security
  - Global Significance
- Challenges with Large News Outlets
- Risk of Misinterpretation, Especially in Social Media News

Introduction to the Blockchain World!
Blockchain Types

- Introducing "Safe News Blockchain Network"
  - Focused on News Integrity
- Data Storage in Blocks
- Open Access for All to Read
- Involving Official News Agencies
  - "Consensus Framework" for News Addition
- Block Addition Upon Approval by Three Independent News Organizations
  - Consensus Procedure to Ensure Accuracy

Introduction to the Blockchain World!
Blockchain Types

- Blockchain Platform for Independent Musicians
- Open Access to Music Tracks
- "Consensus Structure" Limits Track Additions to Independent Musicians
- Professional Associations Ensure Originality
- Interests: Accessing Music and Recording Works
- Focus on Copyright and Potential Revenue Processes

Introduction to the Blockchain World!
Public and Private Blockchain Networks

- **Fully and Partially Permissionless Blockchains = Public**
- Inconvenient for Institutions
- Data Encryption Possible but with Security Concerns
- Enter Private Blockchain Networks
- Private Blockchains Require Permission to Access Data

Introduction to the Blockchain World!
Public and Private Blockchain Networks

Type 3: Partially Permissioned Blockchain Networks

- Partially Permission Blockchain Networks
- Need Permission to Access Data
- Open "Consensus Process" for Everyone
- Secure Data Recording Among Network Participants
- Analogy: Playing Tag with Invited Friends in a Closed Area

Introduction to the Blockchain World!
Public and Private Blockchain Networks

- Example: Bank's Internal Remittance System
- Utilizing a Bank-Specific Blockchain Network
- Branches Exclusively Participate
- Involvement in "Consensus Structure" and "Consensus Process"
- Facilitating Secure Remittance Transactions
- Data Records Transmission to All Branches for Enhanced Infrastructure

Introduction to the Blockchain World!
Public and Private Blockchain Networks

Type 4: Fully Permissioned Blockchain Networks

- Fully Permissioned Blockchain Networks
  - Permission Required for Data Reading, Block Creation, and "Consensus Process"

- Limited Access to Recorded Data and "Consensus Process"

- Creation of Multi-Layered Secure Data Recording Mechanism

Introduction to the Blockchain World!
Public and Private Blockchain Networks

- Analogy: Playing Tag in a Closed Area with Invited Friends
- Limited Chain Record Keepers
- Increasing Difficulty with More Participants
- Example: Bank EFT Transactions
  - Exclusive Private Blockchain Network for EFT Transactions
  - Access Restricted to Banks Only
  - Data Writing Privileges for Two Banks
  - Preservation of Bank and Branch Records

Introduction to the Blockchain World!
Public and Private Blockchain Networks

- "Consensus Structure" Limited to Two Branches for Record Creation
- Data Reading Access for All Banks and Branches
- Similar Appearances, Distinct Consensus Preference and Reason Layers

Introduction to the Blockchain World!

Public and Private Blockchain Networks

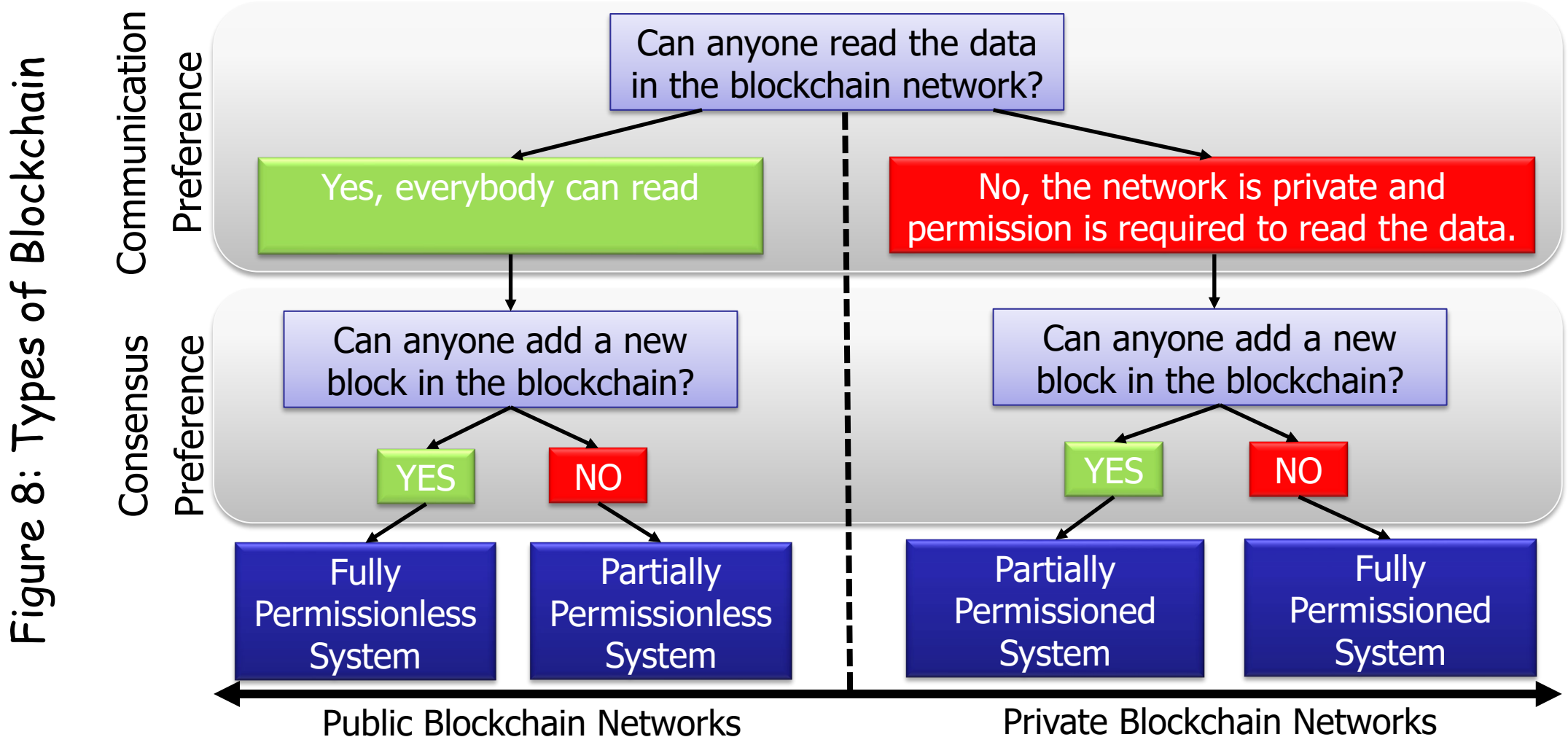


Figure 8: Types of Blockchain

Introduction to the Blockchain World!

Public and Private Blockchain Networks

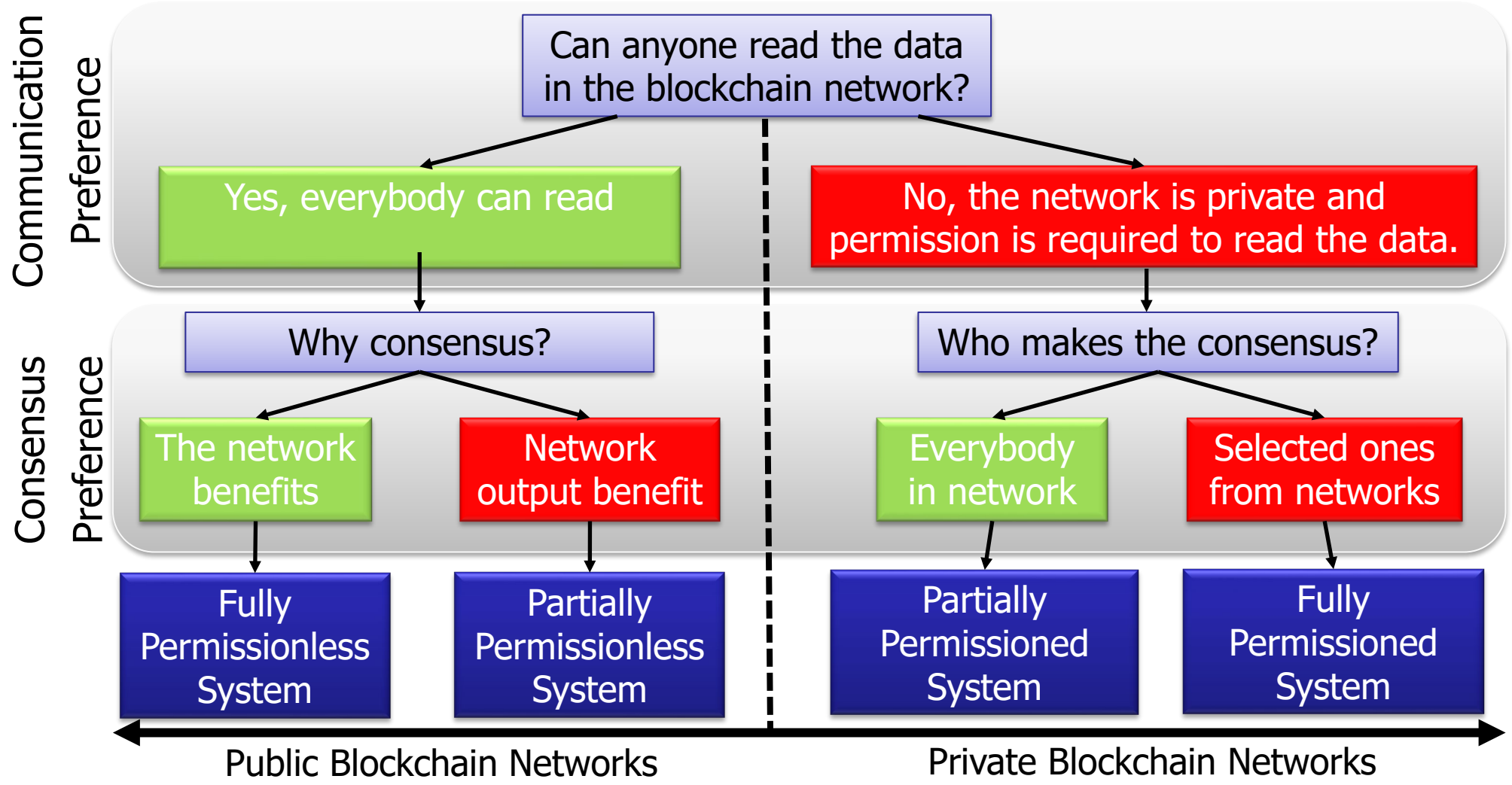


Figure 9: Consensus Interest

Introduction to the Blockchain World!
Encryption in Blockchain Networks

- No In-Depth Encryption Coverage
- Cryptography: Complex, Involving Math, Numerical Systems, Programming
- Cryptology Origin: Ancient Greek "Kryptos" (Concealment)
- Applied for Data Privacy
- Key Objective: Data Security from Unauthorized Access

Introduction to the Blockchain World!
Encryption in Blockchain Networks

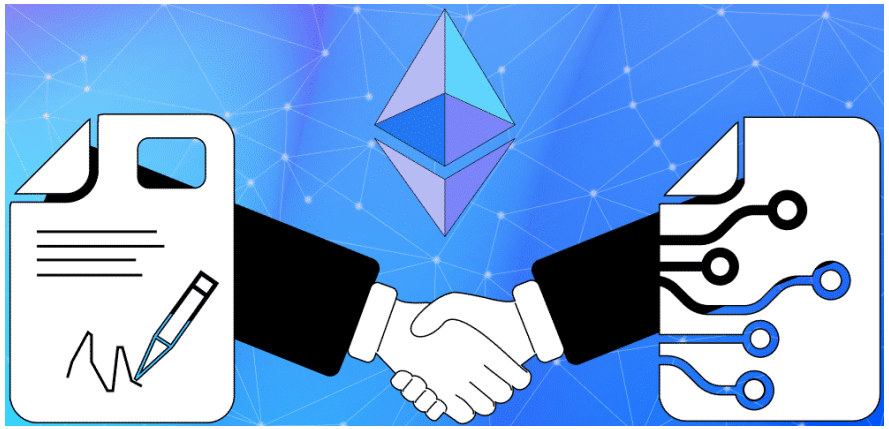
- Simplest Encryption: Key-Locking a Safe
- Key Required to Unlock the Safe
- Unlocking via Key Exchange or Brute Force (Depends on Encryption Strength)
- Relevance of Vault Example to Data Storage
- Key Needed to Share Data from the Safe
- Concerns: Theft and Key Loss
- Key Copying May Compromise Security
- Practicality of Sending the Lock, Not the Key, in Encryption

Introduction to the Blockchain World!
Encryption in Blockchain Networks

- Secure Data Sharing with Locking Approach
- Blockchain Networks Use Similar Method
- Encrypt Data with Recipient's Lock for Privacy
- Incomprehensible Data for Others
- Recipient Unlocks with Their Key
- Security in Open Blockchain Networks
- Upcoming Topic in Subsequent Lectures

Introduction to the Blockchain World!
Smart Contracts on Blockchain Networks

- Beyond Data Recording: Running Programs
- Applications on Blockchain Networks
- Smart Contracts on Blockchains
- Automating Actions with Smart Contracts



Introduction to the Blockchain World!
Smart Contracts on Blockchain Networks

- Current Title Deed Transfers
- Limitations of Notaries
- Money Transfer Challenges
- Blockchain and Smart Contracts
- Eliminating Fraud with Blockchain

Introduction to the Blockchain World!
Smart Contracts on Blockchain Networks

- Smart Contract for Title Deed Transfer
- Parties' Actions on Blockchain
- TR ID and E-Government Passwords
- Title Ownership and Bank Account Verification
- Automatic Land Registry Updates
- Secure Money Transfer on Blockchain

Introduction to the Blockchain World!
Smart Contracts on Blockchain Networks

- Smart Contracts and Legal Proof
- Interconnected Systems
- Streamlined and Secure Processes
- Implications for Notaries
- Potential Role of Notaries

Introduction to the Blockchain World!
Privacy and Anonymity in Blockchain Networks

- Bitcoin's Pseudonymous Nature
- Limited User Identification
- Encryption and Privacy
- Debatable Anonymity

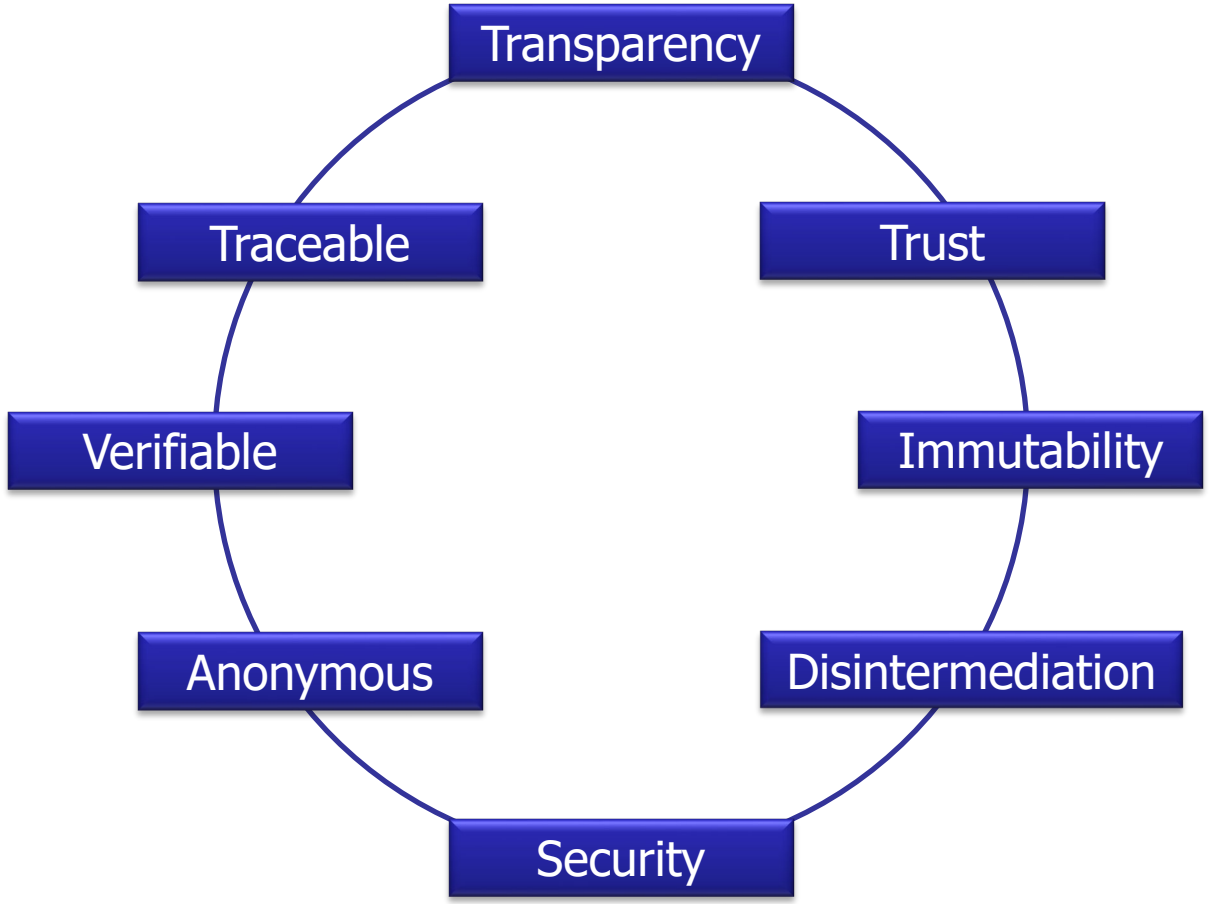
Introduction to the Blockchain World!
Privacy and Anonymity in Blockchain Networks

- Encrypted Blockchain Data
- Analysis and Data Models
- Cryptocurrency Exchanges
- User Identification

Introduction to Blockchain World!
Features of Blockchain Technology

- Transparency, Trust, Immutability
- Aliasing, Verifiability, Controllability, Security
- No Central Authority
- Blockchain Advantages and Disadvantages

Introduction to Blockchain World!
Features of Blockchain Technology



Features of blockchain technology (Lapointe and Fishbane, 2019).

Q/A


WHEN?
HOW?
WHERE?
WHO?
WHAT?
WHEN?
WHAT?
WHERE?
WHAT?
WHERE?
When?
HOW?
WHEN?
What?
Where?
When?
WHERE?
ANY
WHERE?
What?
QUESTIONS?
What?
When?
When?
Why?
WHEN?
When?
WHAT?
When?
Why?
HOW?
WHAT?
Where?
When?
What?
WHEN?
Why?
WHERE?
When?
HOW?
Why?