BLOCKCHAIN FUNDAMENTALS: A PRIMER

Luong Thai Bao, SBF, NEU

in collaboration with

Pham Thanh Phong, 2+2 Fintech student, SBF, NEU

Hanoi, May 2019

Contents

1. Introduction
2. Blockchain use cases with focus on bank
3. A practical approach to study of blockchain
4. Non-technical approach to blockchain

Introduction

Objectives:

- Provide an overview of potential blockchain applications in financial services industry.
- Set a "grounding framework" to further explore and study of blockchain.
- Explain technical concepts of the blockchain such as transactions, hash values, data structures, peer-to-peer systems, distributed systems, system integrity in a nontechnical fashion. (limited)

The four high grounds of “internet finance”

Infrastructure	*Payment system (medium)*: AliPay, WeChat Pay, Tenpay, Momo Pay *Credit system*: Sesame Credit *Underlying asset matching platform*: Renrendai
Platform	*Service integration*: Encompasses payment, financial management, fee payment, and other services *Navigation*: Helping customers to find the required applications *Personalization*: Providing services based on the personal characteristics of the customers *Social interaction*: WeChat, Alipay Living
Channel	*Multi-channel integration*: Banking Transformation Toolkit (BTT) by IBM
Scenario	*Application scenario and product*: WeChat Red Envelope, Alipay School Life

Source: Guo and Liang (2016)

Blockchain benefits in banking industry

	Traditional banking businesses	Internet finance businesses (Fintech 1.0)	Blockchain + banks (Fintech 2.0)
Customer experience	Uniform scenarios Homogenous service Poor customer experience	Rich scenarios Personalised service Good customer experience	Rich scenarios Personalised service Good customer experience
Efficiency	Many intermediate links Complex clearing process Low efficiency	Many intermediate links Complex clearing process Low efficiency	Point-to-point transmission, disintermediation Distributed ledger, transaction = clearing High efficiency
Cost	Large amount of manual inspection Many intermediate links High costs	Small amount of manual inspection Many intermediate links High costs	Completely automated Disintermediation Low costs
Safety	Centralized data storage Can be tampered Easy to leaks users' personal information Poor safety	Centralized data storage Can be tampered Easy to leaks users' personal information Poor safety	Distributed data storage Cannot be tampered Use of asymmetric encryption. Users' personal information is more secure Good safety

Source: Guo and Liang (2016)

Categories of blockchain

	Public blockchains	Consortium blockchains	Private blockchain
Degree of centralization	Decentralized	Multi-centralized	Decentralized
Participants	Anyone can freely participate and leave	Specific group of people who agree to enter an alliance	Central controller decides member that can participate
Credit mechanism	Proof of work	Collective endorsement	Self-endorsement
Bookkeeper	All participants	Participants decide in negotiation	Self-determined
Incentive mechanism	Needed	Optional	Not needed
Prominent advantage	Self-established credit	Efficiency and cost optimization	Transparency and traceability
Typical application scenario	Bitcoin	Clearing	Audit
Load capacity	3-20 times/second	1000-10000 times/second	

Source: Guo and Liang (2016)

Taxonomy of the maturity assessment – Explanation

	1. Initial	2. Repeatable	3. Defined	4. Managed	5. Optimized
Technology	• Ad hoc, chaotic • Emerging • Lack of understanding	• Methodology establishment • Controlled and coordinated • Reactive	• Standardized and documented • Proactive	• Quality metrics establishment • Consolidated and reliable	• Continuous improvement • Share of knowledge and information
Market	• Focus on function • High cost	• Focus on reliability • Transactional customers • Broad no-target promotion	• Focus on assured delivery of services • Prices settle down • Requirements are measured	• Standard services • Price with incentives and outcome metrics • Customers are grouped with profiles • Promotion is targeted	• Empathy in dealing with emerging business needs • Create the product special influents in industry
Regulation	• Less supervision • Competition is forbidden	• Rules have been borrowed from related domains	• Regulation rules and laws are defined	• Measurements on regulation is set up • Competition is encouraged under supervision	• Free competition • Market based on well-established legal system

Source: Wang et al. (2016)

Blockchain maturity model - Desired Objectives

	Initial (stage 1)	Repeatable (stage 2)	Defined (stage 3)	Managed (stage 4)	Optimizing (stage 5)
Networks		Network load	Reliability		
Information system	Architecture Upgrading Integration	Maintenance Storage Scalability		Business efficiency	
Computing methodology	Standardization	Computational complexity			
Security and Privacy			Privacy	Data security Transaction security	

Source: Wang et al. (2016)

Non-technical approach to blockchain: 2/4 stages

- Stage 1: Terminology and Technical Foundations

  Explain major concepts of software engineering and set the terminology necessary for understanding the succeeding steps. Provide an overview of the fundamental concepts and an appreciation of the big picture in which blockchain is located.

- Stage 2: Why the Blockchain is Needed

  Explain why the blockchain is needed, what problem it solves, why solving this problem is important, and what potential the blockchain has.

STEP 1: THINKING IN LAYERS AND ASPECTS

- Layers of a Software System
  - Application vs. Implementation
    - Application: user's need (e.g listening to music, taking photos)
    - Implementation: making things happen (e.g converting digital information into acoustic signals, recognizing the color of a pixel in a digital camera)
  - Functional vs. Nonfunctional Aspects
    - Functional aspects: sending data, taking photos, playing music
    - Nonfunctional aspects: beautiful graphics user interface, fast-running software, ability to keep user data private and save.

STEP 1: THINKING IN LAYERS AND ASPECTS

Example of Mentally Layering a Mobile Phone

Layer	Functional aspects	Nonfunctional aspects
Application	Taking photos Making phone calls Sending e-mails Browsing the Internet Sending chat messages	The graphical user interface looks beautiful Easy to use Messages are sent fast
Implementation	Saving user data internally Making a connection to the nearest mobile connector Accesing pixels in the digital camera	Store data efficiently Saving energy Maintaining integrity Ensure user privacy

STEP 1: THINKING IN LAYERS AND ASPECTS

Integrity

- An important nonfunctional aspect of any software system.
- Has three major components:
  - Data integrity: The data used and maintained by the system are complete, correct, and free of contradictions.
  - Behavioural integrity: The system is behaved as intended and free of logical errors.
  - Security: The system is able to restrict access to its data and functionality to authorized users only.

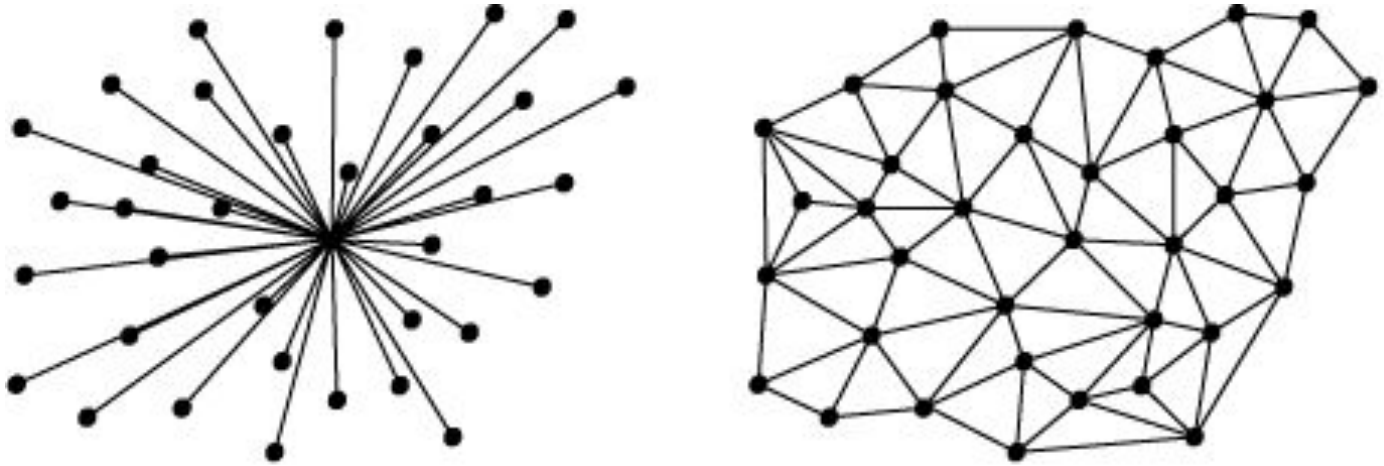
STEP 2: SEEING THE BIG PICTURE

Aspects and Layers of a Payment System

Layer	Functional Aspects	Nonfunctional Aspects
Application	Deposit money Withdraw money Transfer money Monitor account balance	The graphical user interface looks beautiful Easy to use Transfer of money is done fast System has many participants
Implementation	?	Available 24 hours a day Fraud resistant Maintaining integrity Ensure user privacy

STEP 2: SEEING THE BIG PICTURE

Two types of Software Architecture



centralised

distributed

STEP 2: SEEING THE BIG PICTURE

Advantages and Disadvantages of Distributed Systems

Advantages	Disadvantages
Higher computing power Cost reduction Higher reliability Ability to grow naturally	Coordination overhead Communication overhead Dependency on networks Higher program complexity Security issues

STEP 2: SEEING THE BIG PICTURE

Distributed Peer-to-Peer Systems and the Purpose of Blockchain

Peer-to-Peer Networks

- A special kind of distributed systems
- Consist of individual computers called nodes
- Make computational resources directly available to all members
- All nodes are equal concerning their rights and roles
- All are both suppliers and consumers of resources
- Application: file sharing, content distribution, privacy protection, etc.

The purpose of blockchain is to achieve and maintain integrity in distributed systems

STEP 3: RECOGNIZING THE POTENTIAL

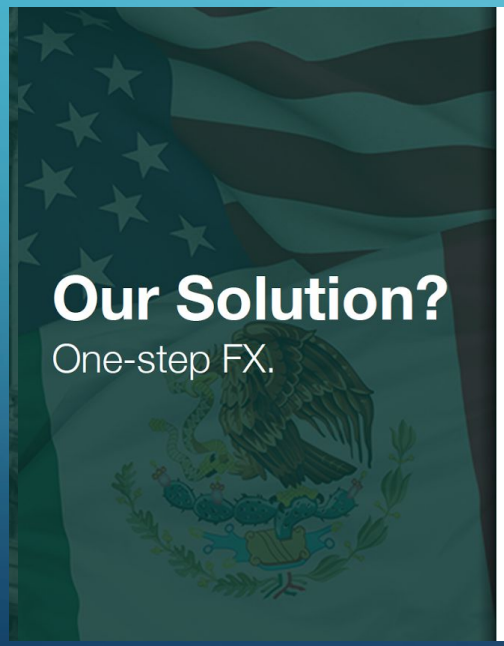
How a Peer-to-Peer System changed a whole industry

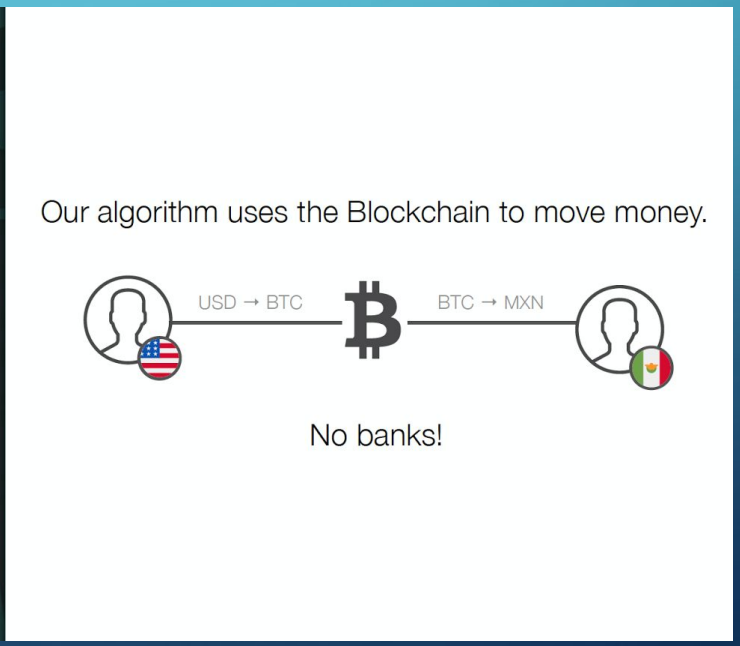
STEP 3: RECOGNIZING THE POTENTIAL

The potential of Peer-to-Peer systems

Idea: Replacing the middle-man with peer-to-peer interactions

Example: The financial industry





STEP 4: DISCOVERING THE CORE PROBLEM

The daydreams of cat herders

STEP 4: DISCOVERING THE CORE PROBLEM

Trust and Integrity in Peer-to-Peer Systems

- Integrity: a nonfunctional aspect of a system to be safe, complete, consistent, and free of corruption and errors.
- Trust: the firm believe of humans in the reliability, truth, or ability of someone or something

Achieving and maintaining integrity in purely distributed systems depends on:

- Knowledge about the number of nodes or peers
- Knowledge about the trustworthiness of the peers

STEP 4: DISCOVERING THE CORE PROBLEM

Integrity Threats in Peer-to-Peer Systems

- Technical failures
- Malicious peers

STEP 5: DISAMBIGUATING THE TERM

Four ways to define the blockchain:

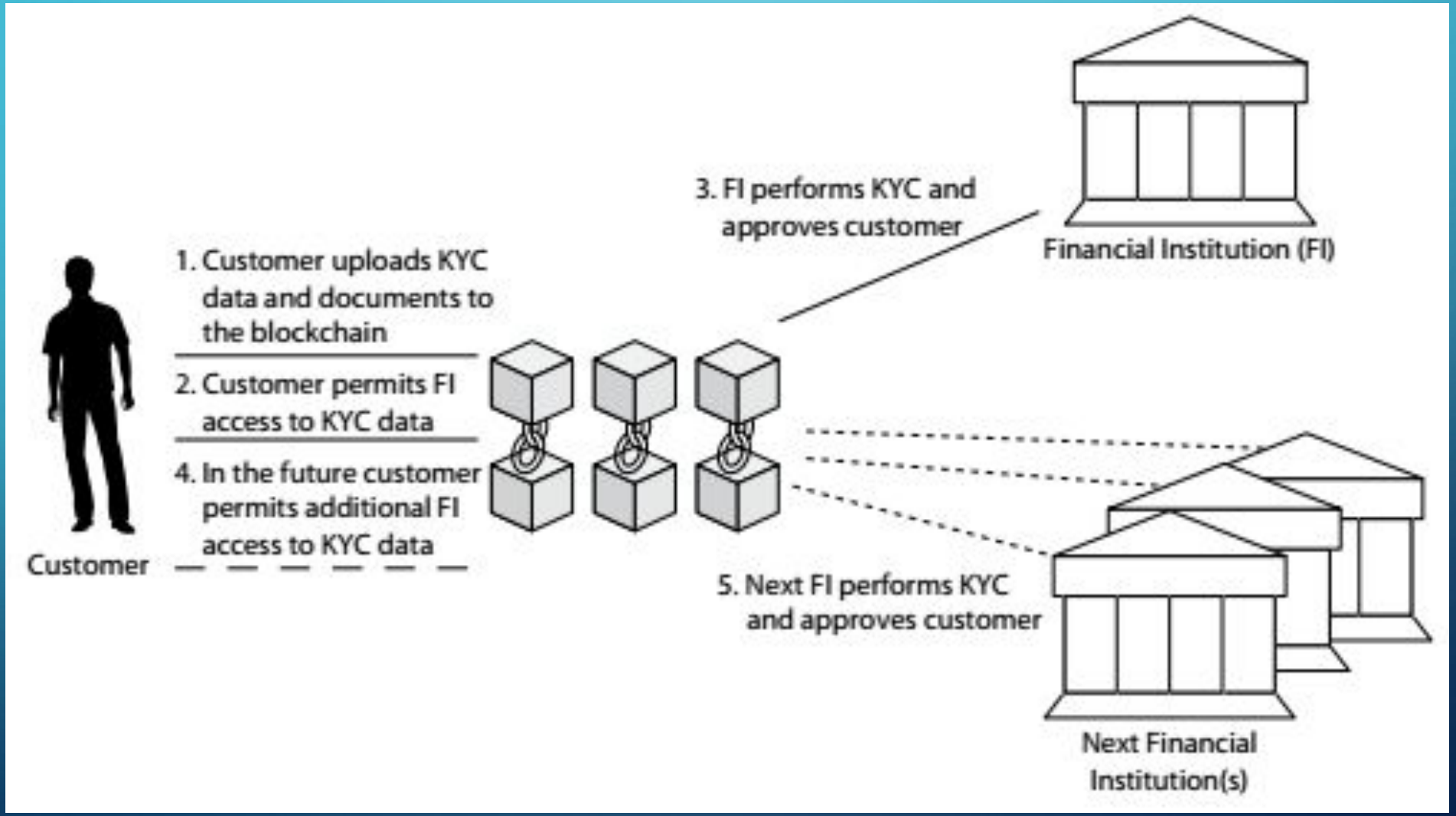
- As a name for a data structure
- As a name for an algorithm
- As a name for a suite of technologies
- As an umbrella term for purely distributed peer-to-peer systems with a common application area

STEP 5: DISAMBIGUATING THE TERM

Provisional Definition

The blockchain is a purely distributed peer-to-peer system of ledgers that utilizes a software unit that consist of an algorithm, which negotiates the informational content of ordered and connected blocks of data together with cryptographic and security technologies in order to achieve and maintain its integrity.

Know your customer (KYC) use case solution



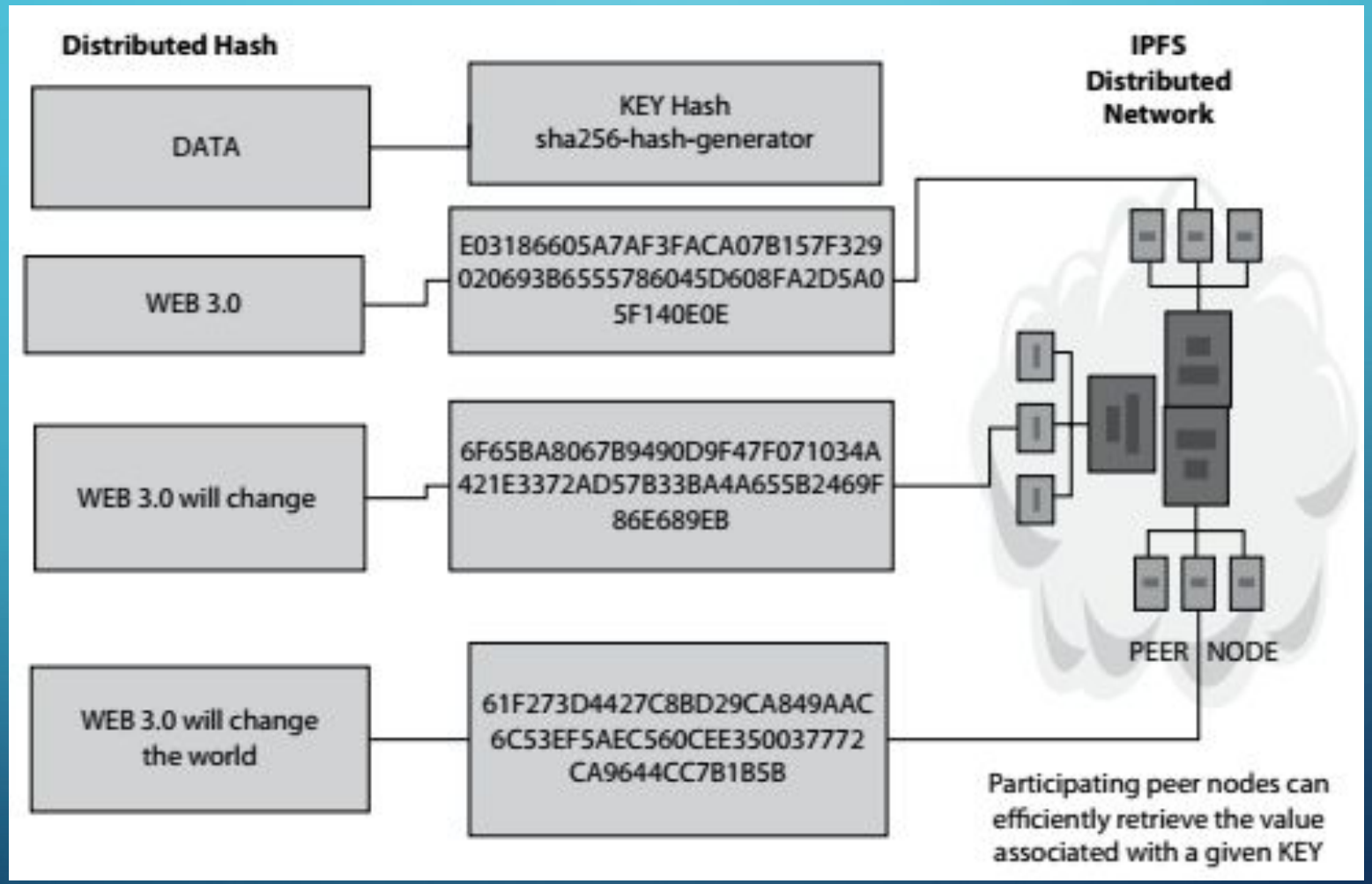
Source: Bambara and Allen (2018)

Core components of different types of blockchain

	Permission-less	Permissioned
Public	**Consensus**: Proof-of-X **Permission management** • Blockchain layer • Application layer (optional) **Incentive**: Blockchain layer	**Consensus** • Proof-of-X • PBFT, Federated consensus, Round Robin *etc.* **Permission management** • Blockchain layer • Application layer (optional) **Incentive**: • Blockchain layer • Governance around permissions
Private	**Consensus** • Proof-of-X • PBFT, Federated consensus, Round Robin *etc.* **Permission management:** • Blockchain layer • Network layer • Application layer (optional) **Incentive**: Governance around access	**Consensus** • Proof-of-X • PBFT , Federated consensus, Round Robin *etc.* **Permission management:** • Blockchain layer • Network layer • Application layer (optional) **Incentive**: Governance around access permissions

Source: Xu et al. (2019)

Distributed hash table with content address derived by hashing content



Source: Bambara and Allen (2018)

STEP 6: UNDERSTANDING THE NATURE OF OWNERSHIP

Why we know what we own?

STEP 6: UNDERSTANDING THE NATURE OF OWNERSHIP

Foundations of Ownership

- An identification of the owner
- An identification of the object being owned
- A mapping of the owner to the object

STEP 6: UNDERSTANDING THE NATURE OF OWNERSHIP

Ledger	
Proof of Ownership	Transfer of Ownership
Transparency	Privacy
Reading Data	Writing Data
Consuming Historic Data	Creating New Data
Maitaining the State	Changing the State

Purposes and Properties of a Ledger

- A means for proving ownership
- Document any transfer of ownership

STEP 6: UNDERSTANDING THE NATURE OF OWNERSHIP

Ownership and the Blockchain

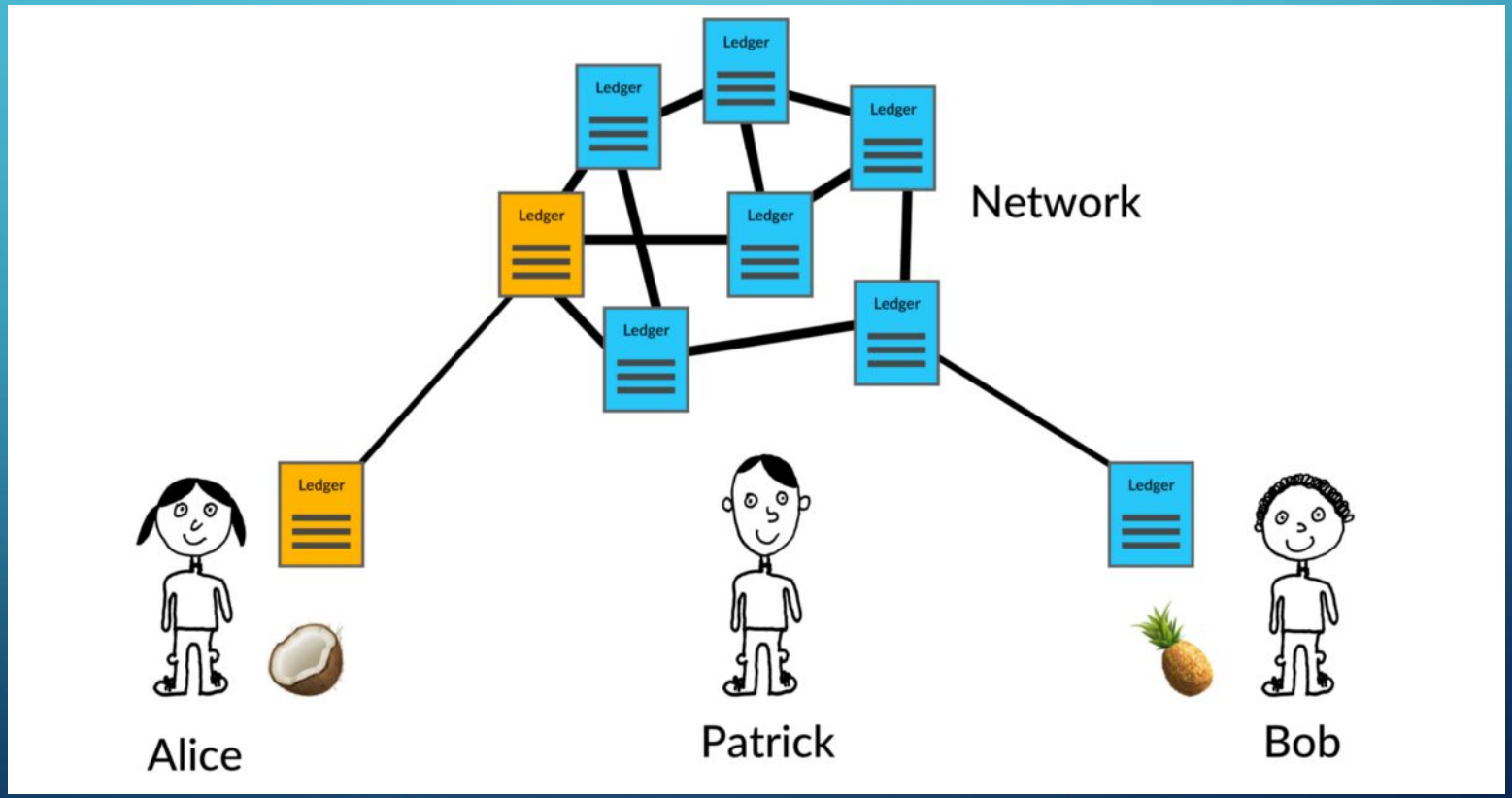
- Problem: One single ledger can be forged, damaged, or destroyed
- Solution: Using a purely distributed peer-to-peer system of ledgers

The relation between managing ownership with a ledger and blockchain:

- Each blockchain-data-structure represents one ledger and is maintained by one node in the system.
- The blockchain algorithm is responsible for letting individual nodes arrive at one consistent version of the state of ownership.
- Cryptography is necessary for ensuring data security.

STEP 7: SPENDING MONEY TWICE

The double spending problem



STEP 7: SPENDING MONEY TWICE

The term *double spending* refers to the following concepts:

- A problem caused by copying digital goods
- A problem of distributed peer-to-peer systems of ledgers
- An example of violated integrity in purely distributed peer-to-peer systems

Q&A

Comments and questions are welcomed!