The Blockchain Opportunities and Obstacles for ICT Security

Fangfang Dai@CAICT

12 October 2017
Beijing, China

CONTENTS

- Overview of Blockchain
- Value and Security Concerns
- What We Can Do in the Future

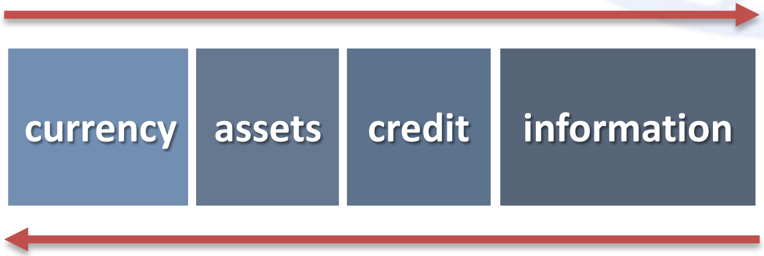
Blockchain: Trust Machine behind Digital Fiat Currency

“It appears that once again, the technological genie has been unleashed from its bottle…to transform the economic power grid and the old order of human affairs for the better. ”

—Blockchain Revolution, Don Tapscott, Alex Tapscott, May 2016

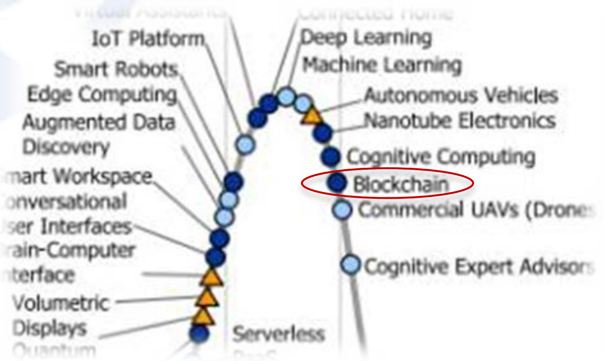
- The inherent tamper-proofing, decentralization and transparency of blockchain have motivated its development through a peak of inflated expectation phase.

Driven by crypto-currency



currency assets credit information

Driven by ICT application



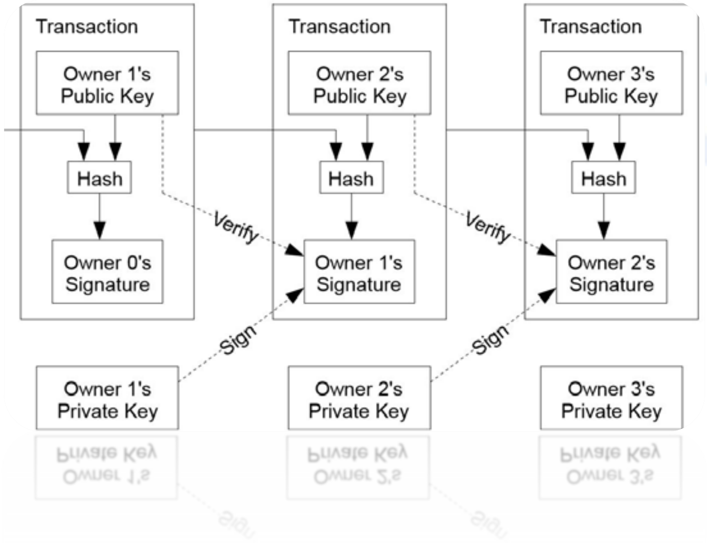
Gartner, Hype Cycle 2017

Secure and Trusted Underlying Technical Framework

As a revolutionary data storage, transportation and management mechanism, blockchain enables users to participate in the ***computation***, ***storage*** and ***mutual authentication*** of data.

- a reliable transfer of data and value;
- decentralized and no need of trusted intermediary.

A typical blockchain system:

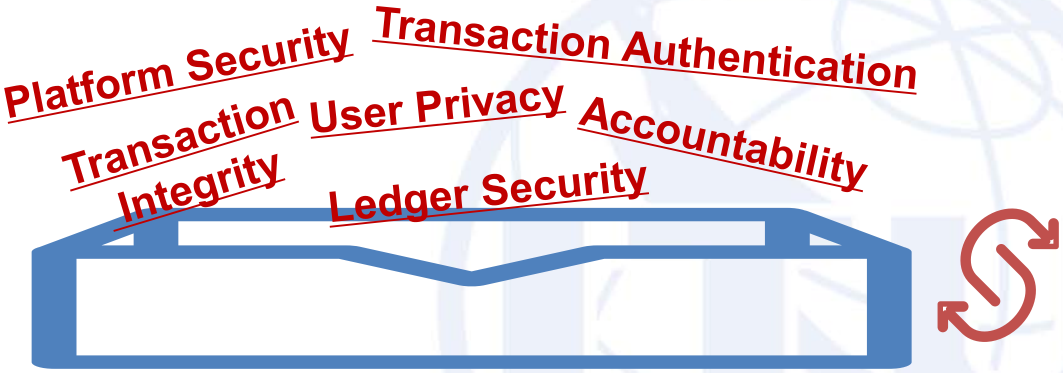


- **block:** data unit
- **chain:** data structure of consecutive block in chronological order;
- **record:** approve by more than half of users, network-wide synchronization
- **modify or delete:** not allowed after synchronization

CONTENTS

- Overview of Blockchain
- Value and Security Concerns
- What We Can Do in the Future

Security Value Provided by Blockchain (1)



Platform Security

Transaction Authentication

Transaction Integrity

User Privacy

Accountability

Ledger Security

BLOCKCHAIN

Distributed Data Storage
P2P Network
Cryptography
Consensus Mechanism

Tamper-proofing： achieved by data structure and data writing mechanism

- Chained data structure, modification before timestamp is forbidden;
- Consensus mechanism to decide whether a transaction can be recorded, normally need approval of 50%+ nodes.

Security Value Provided by Blockchain (2)

Disaster Recovery： improve reliability and fault-tolerance by decentralized and distributed storage

- open source sharing protocols, data recorded and stored synchronously at all users’ side ;
- centralized database vs. redundancy storage, sacrifice moderate computing power, bandwidth or storage resources for security.

Privacy Protection： ensure user anonymity by cryptography

- asymmetric encryption ， take hash of user’s public key as ID indicator, keep personal identity information safe;
- invertible hash process, impossible to calculate user’s public key or private key from ID indicator.

Risk and Security Concerns (1)

Technical Limitations

- controversy between bigger (more difficult to run blockchain nodes) or smaller (more reliable to a third-party payment solutions) block capacity;
- distributed storage creates a boarder attack surface;
- consensus mechanism may trigger a cooperative attack.

Potential Risk of Cryptography Application

- the problem of private key management is not solved;
- wide application of cryptographic algorithm ECC/RSA may introduce unknown backdoors or vulnerabilities;
- new computing technologies like quantum computer will increase the chance of cracking the asymmetric encryption algorithms.

Risk and Security Concerns (2)

Blockchain Platforms Attract Intensive Attacks

- as an underlying technology of upper-layer applications, blockchain platform supports interoperation of applications and users, huge economic benefits motivate hackers flocking to digging open source platform vulnerabilities.

Security Management of Self-organization and Anonymity

- distributed data storage may cause autonomous and frequent data cross border;
- anonymity mechanism may trigger attack backtrack problem, difficult to verify and trace a user’s true identity.

CONTENTS

Overview of Blockchain

Value and Security Concerns

What We Can Do in the Future

Future Work

Standards for Security Requirements and Technology Testing

- the ”know yourself and know your enemy” principle;
- observe, check and analysis testing objects such as blockchain platforms, applications and protocols;
- think outside the box and act like an adversary, perform predetermined methods and tools.

Mechanism for Securing the Business Flow

- better understand digital fiat currency threat scenarios, providing security recommendations to help choose appropriate countermeasures.

Clarify Security Operations

- proper private key management methods (multi-signature, private key split storage…);
- log audit, authentication of platform and application…

Thanks for listening ！

daifangfang@caict.ac.cn