



ITUKALEIDOSCOPE

NANJING 2017

Challenges for a data-driven society

Blockchain and its Standardization work

Subin SHEN

Nanjing University of Posts and Telecommunications

sbshen@njupt.edu.cn

Nanjing, China

27-29 November 2017





Topics to be discussed

- Why is the topic of the **Blockchain so hot?**
- **Key techniques** of the Blockchain
- **Architecture** of the Blockchain
- **Issue of interoperability** of the Blockchain
- **Current standardization work** on the Blockchain
- **Suggestions** on the Blockchain standardization



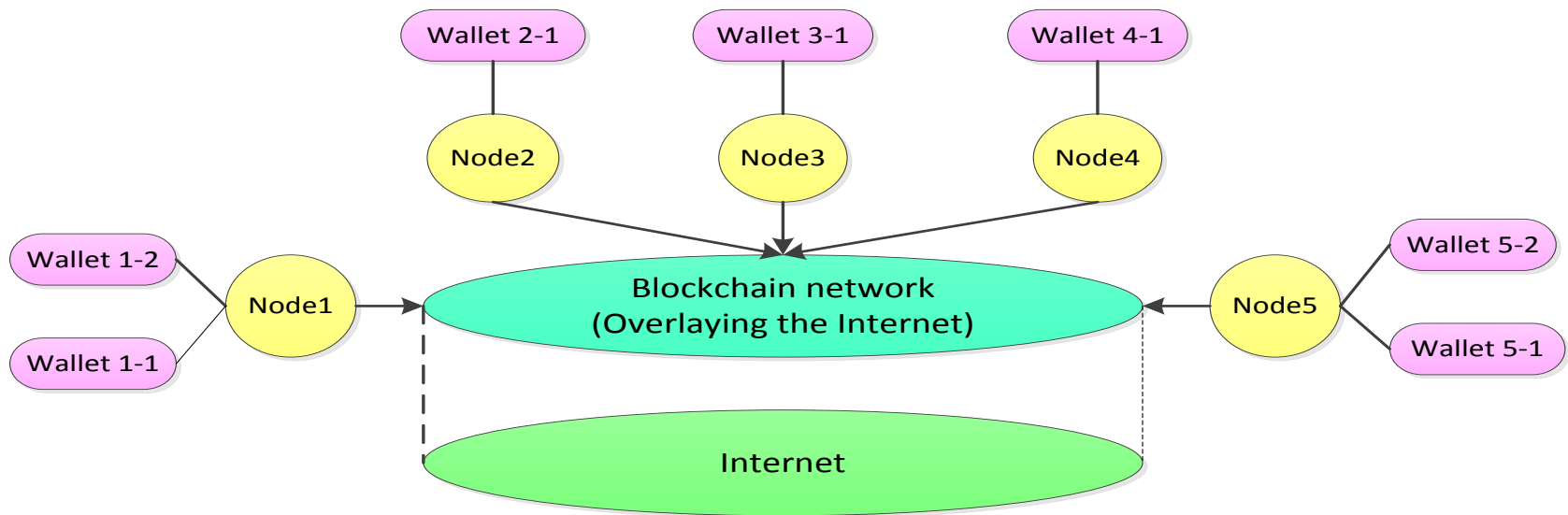
Why is the topic of the Blockchain so hot?

- The **innovative capabilities** provided by the Blockchain
 - Decentralized data management
 - Decentralized trust management
 - Data integrity and trust can be verified by every participant
- The **issues** resolved by the Blockchain
 - Data Integrity verified in decentralized way in Internet
 - Data Provenance verified in decentralized way in Internet
- The suitable **application domains**
 - Supply chain management,
 - Agricultural product tracking,
 - Cooperative manufacturing, etc.



Key techniques of the Blockchain (1)

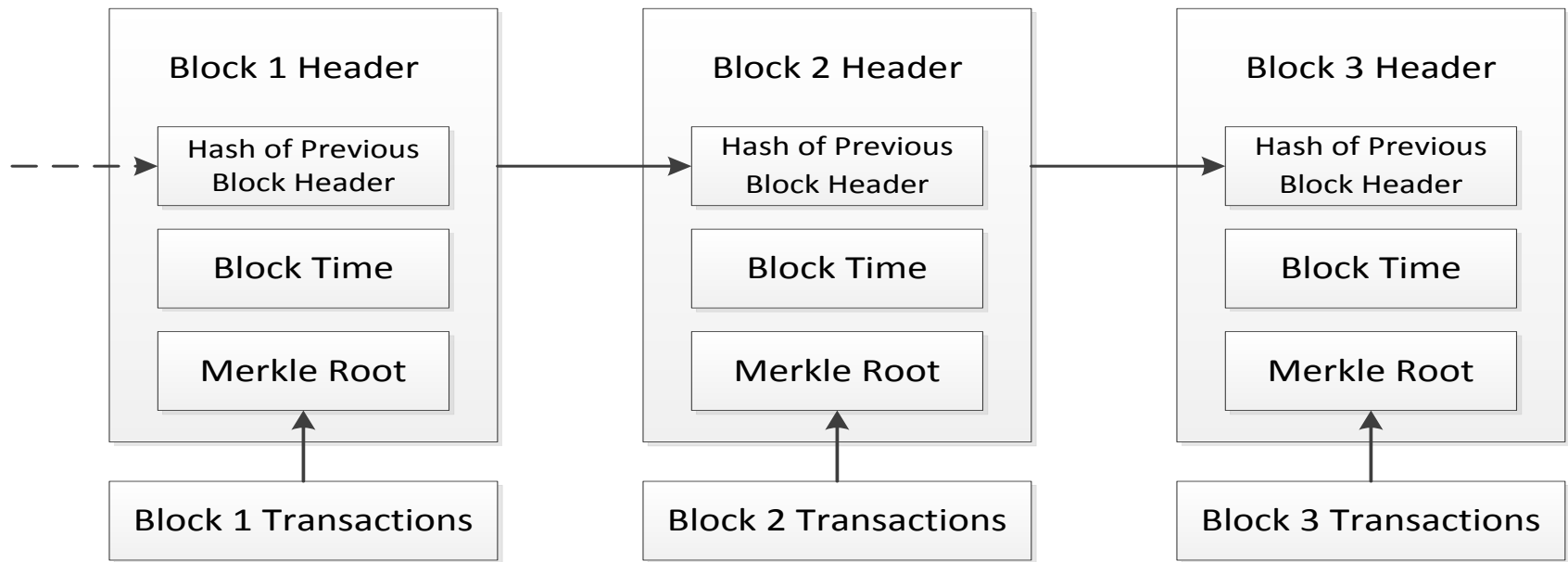
- A framework (from **Bitcoin system**) of a **blockchain network**, and its functional entities (**overlay network**, **nodes**, **wallets**)





Key techniques of the Blockchain (2)

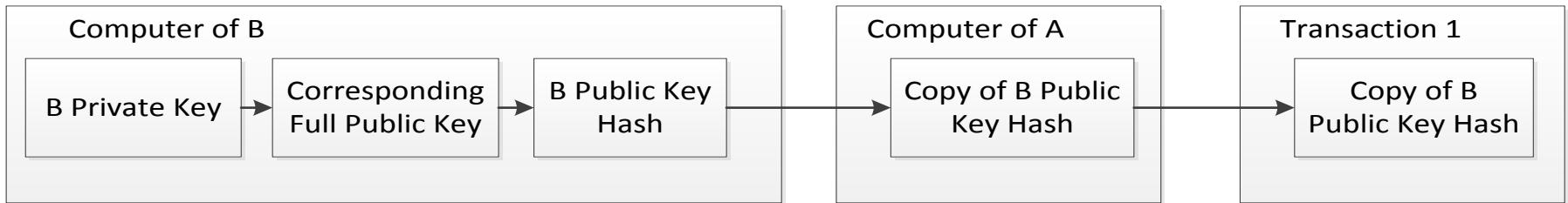
- Following is the example of a Blockchain from Bitcoin system
- The **hash algorithms**, and **consensus protocols** for connecting a block into the Blockchain are the Key techniques.



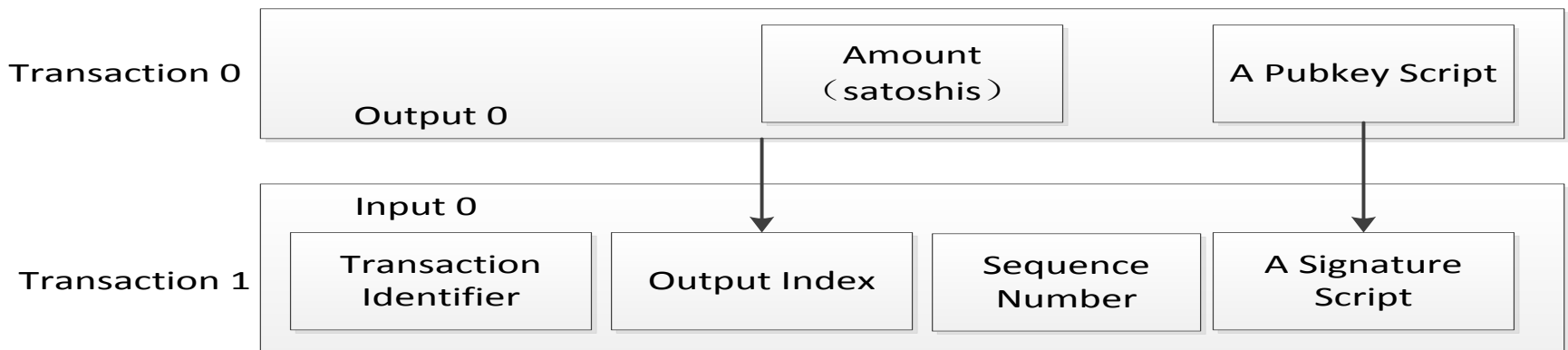


Key techniques of the Blockchain (3)

- The **public encryption** algorithms, **digital signature** algorithms, and **transaction protocols** are the key techniques.



Creation of the public key hash of B to receive payment from A in Bitcoin system

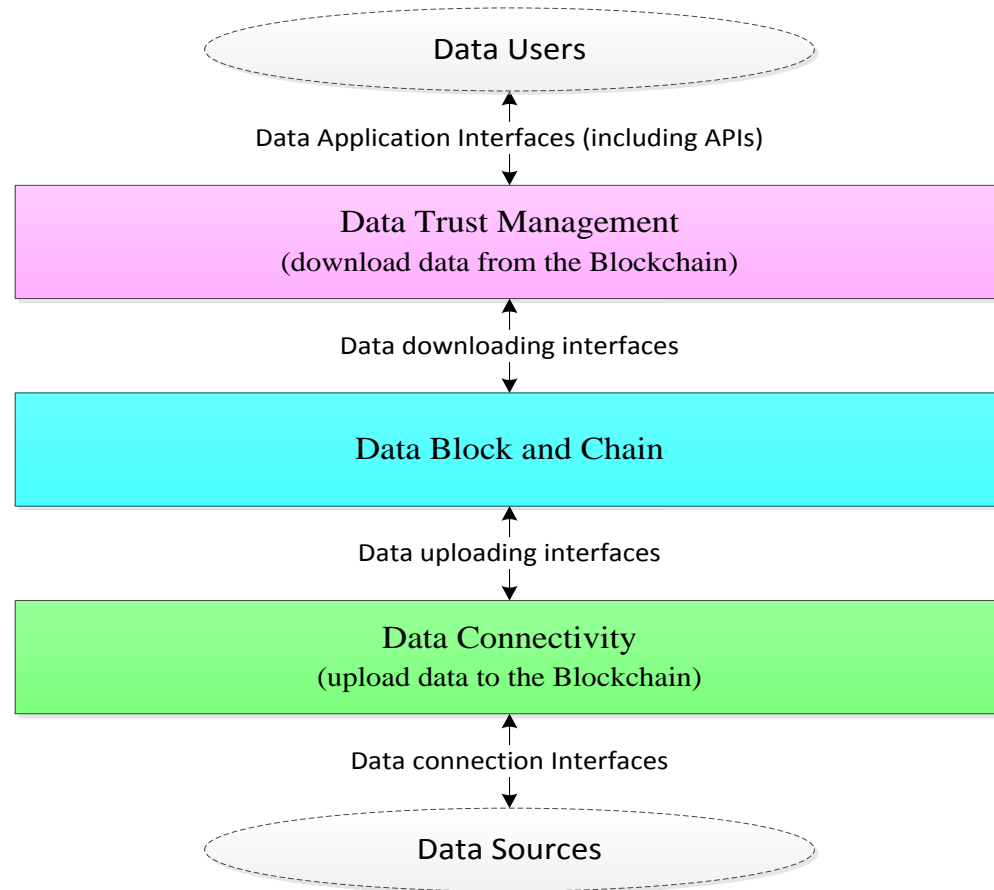


Example: Input spending that the output's paying in Bitcoin system



A Framework of the Blockchain Architecture

- The **functional layers** of the Blockchain architecture
 - Data trust management
 - Data block and chain
 - Data connectivity
- The **four interfaces** of the Blockchain architecture
 - Data application interfaces
 - Data downloading interfaces
 - Data uploading interfaces
 - Data connection interfaces





Issue of interoperability of the Blockchain

- **Data connectivity** interoperability
 - It requires that the data source identifier, data item identifier, and the binding protocol between data source identifier and data item identifier should be standardized.
- **Data block and chain** interoperability
 - The different applications may require different mechanisms and protocols of the Blockchain, so there may be several different types of data block and chain functionalities coexisted in Internet. **Different standards are required** on public encryption, digital signature, hash algorithms, and consensus protocols for different types of the Blockchain.
- **Data trust management** interoperability
 - It requires that the user interfaces and application support interfaces based on the capabilities of data trust management should be standardized. The application programmable interfaces (APIs) are also required to be standardized.



Current standardization work on the Blockchain

- **ITU-T** has established a focus group on distributed ledger technology (FG-DLT) that will **develop a standardization roadmap** for interoperable DLT-based services.
 - <https://www.itu.int/en/ITU-T/focusgroups/dlt/>
- **ISO** has also recently launched a technical committee (TC) 307 on blockchain and distributed ledger technologies.
 - <https://www.iso.org/committee/6266604.html>
- **IEEE** has formed a blockchain member interest group to coordinate and disseminate information on activities in this area.
 - <http://blockchain.ieee.org>
- **W3C** has also initiated its work on distributed ledger technology, the W3C's Web Ledger Protocol.
 - <https://w3c.github.io/web-ledger/>



Suggestions on the Blockchain standardization

- **Suggestion 1:** The **definition, requirements and capabilities** of the Blockchain should be standardized.
 - There are too many instances of the Blockchain and applications, and there is too much confusion on the definition and its capabilities of Blockchain.
- **Suggestion 2:** The **data connectivity interfaces** between the Blockchain and data sources should be standardized in order to use existing blockchain service platform globally for application development.
- **Suggestion 3:** The **data trust management interfaces** between the Blockchain and data users should be standardized in order to develop blockchain-based applications easily and quickly.



ITUKALEIDOSCOPE

NANJING 2017

Challenges for a data-driven society

Comments and Questions are Welcome!
Thank Your!