RISC-V Blockchain SIG meeting

2021-Sep-7th

Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: https://riscv.org/regulations/

If you have questions about these matters, please contact your company counsel.

RISC-V®

Collaborative & Welcoming Community

RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate. We are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

https://riscv.org/risc-v-international-community-code-of-conduct/

RISC-V®

Conventions

- Unless it is a scheduled agenda topic, we don’t solve problems or detailed topics in most meetings unless specified in the agenda because we don’t often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unillaterly. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, …
- Where appropriate and possible, meeting minutes will be added as speaker notes within the slides for the Agenda

Agenda for Today

Cui Can

Brief introduction of blockchain.

Thomas Jin

Introduction of cryptographic algorithms in popular public and consortium blockchain platform.

Gary Xu

Introduction of the data connection from IoT devices to blockchain.

Patty Tu

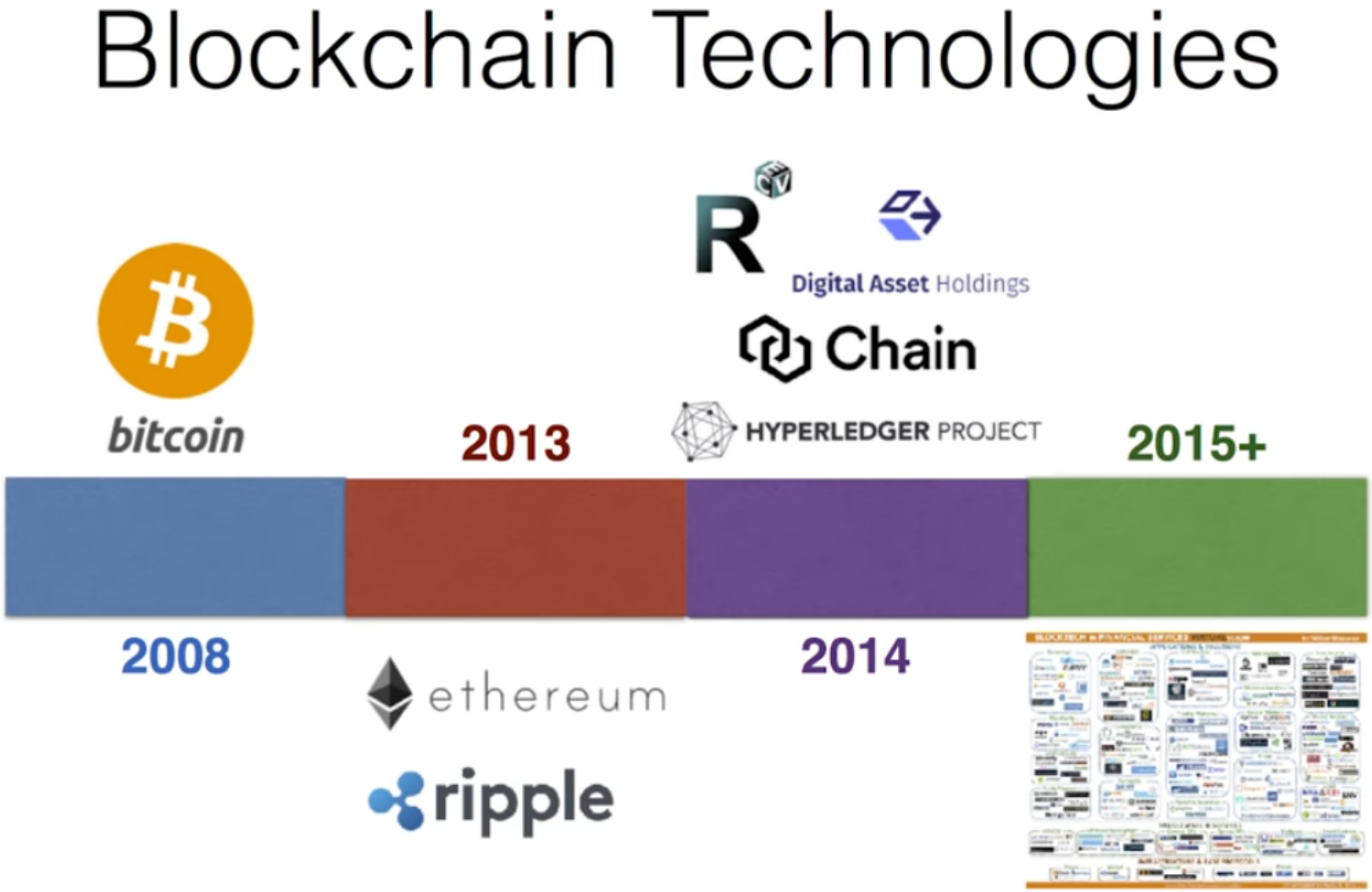
Introduction of blockchain applications with IoT.

All

Open discussion of the next steps.

RISC-V®

History


Blockchain Technologies
bitcoin
Digital Asset Holdings
Chain
HYPERLEDGER PROJECT
2013
2015+
2008
2014
ethereum
ripple

Properties

- **Decentralization**
  - No central server
  - Self-verification, data transmission and management
  - Distributed storage
- **Openess**
  - Open-source
  - Traceability of records
- **Immutability**
  - Hard to be tampered
- **Security**
  - Smart contract, encryption and consensus algorithms make it safe for data exchange among nodes

Types

- **Public Blockchain**
  - Permissionless
  - Economic incentives
  - PoW, PoS
- **Consortium Blockchain**
  - Permissioned (membership)
  - Economic incentives is optional
  - e.g. Hyperleger, PlatONE
- **Private Blockchain**
  - Permissioned (ownership)
  - Usually no economic incentives

Architecture

1) Data Structure

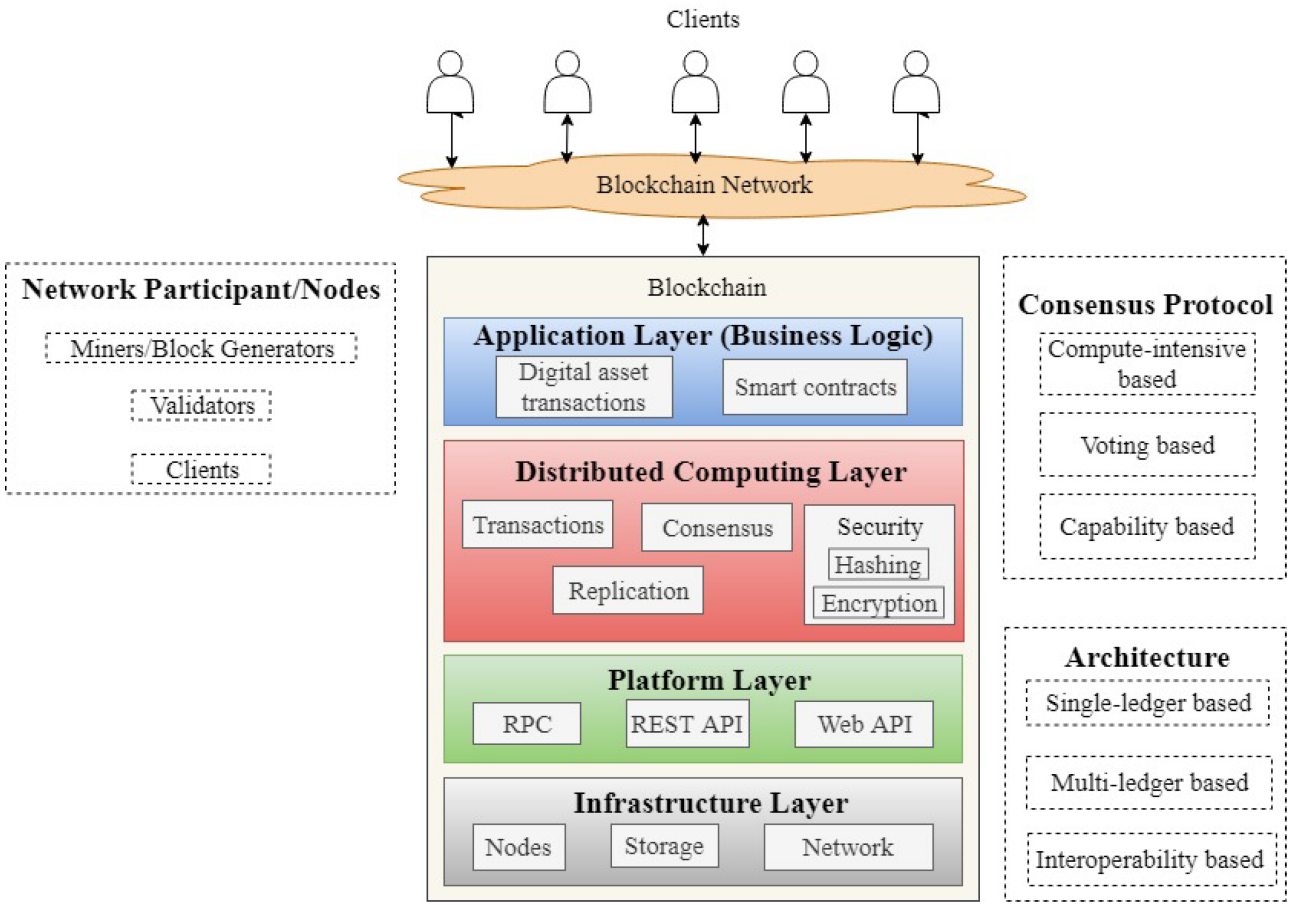
2) Peer-to-Peer Network

3) Consensus Algorithms

4) Smart Contract

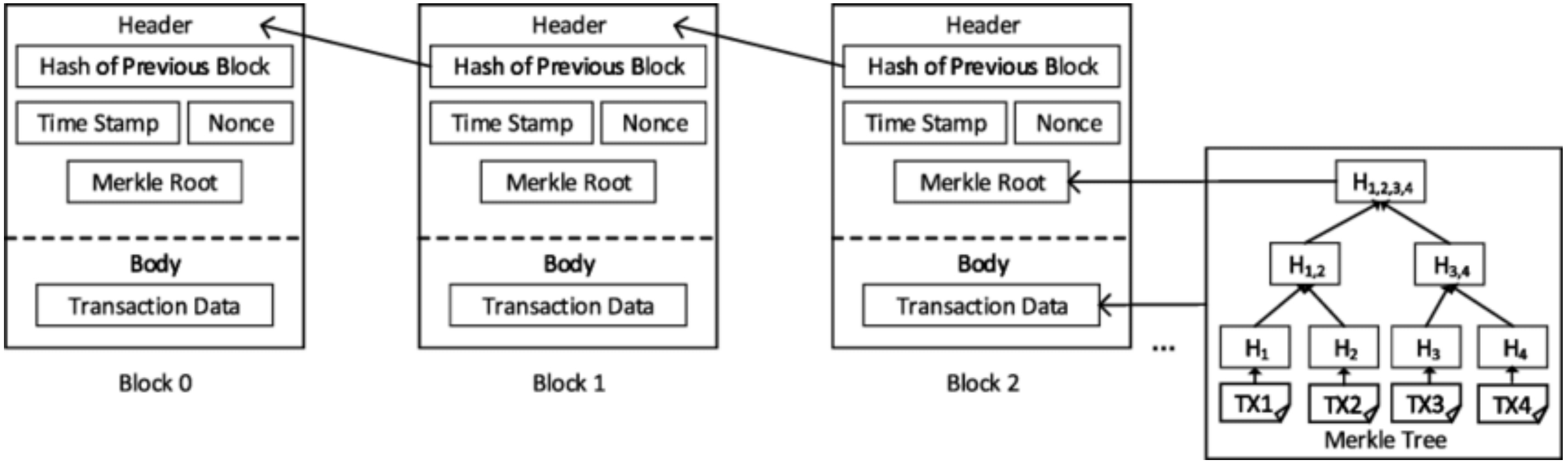
5) Cryptography

6) Transaction



Architecture - Data Structure

- Hash
- Nonce
- Merkle Tree
- Transaction Data



Architecture

1) Data Structure

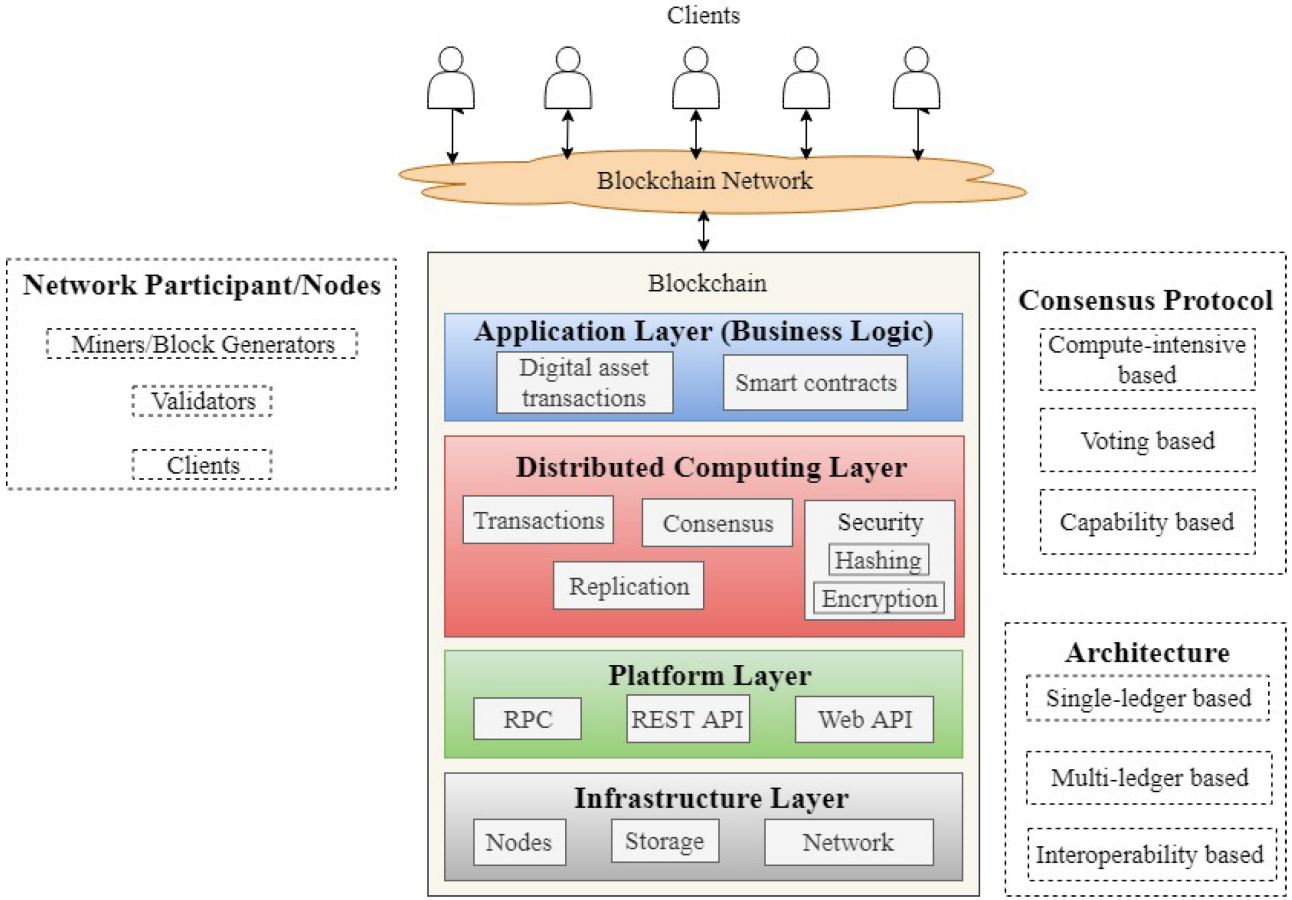
2) Peer-to-Peer Network

3) Consensus Algorithms

4) Smart Contract

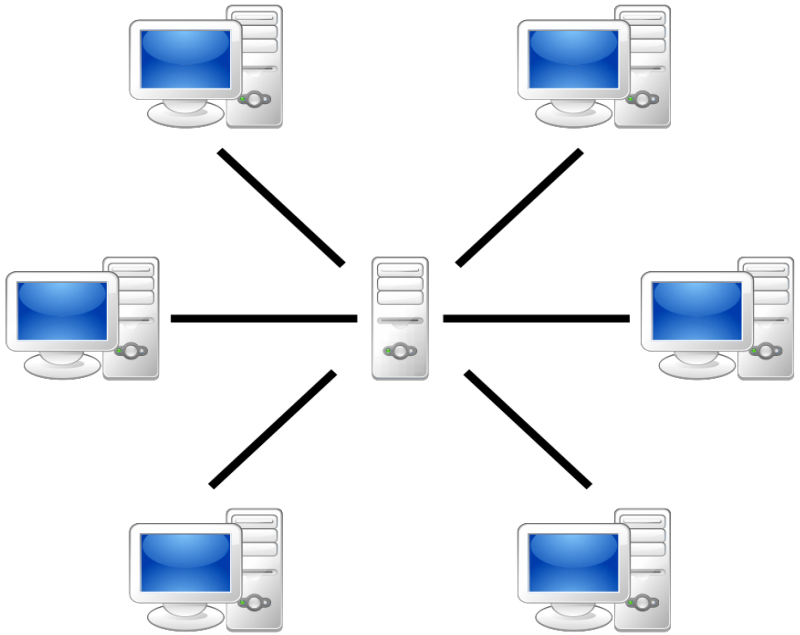
5) Cryptography

6) Transaction

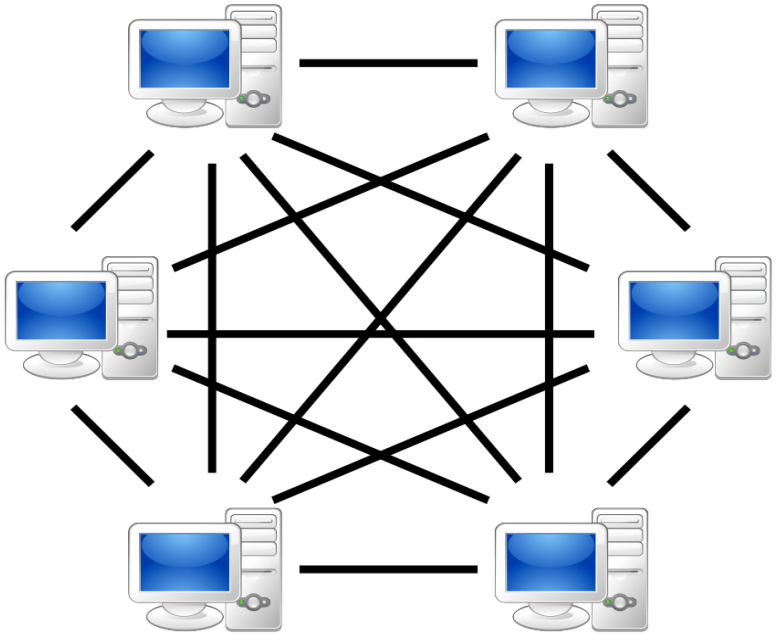


Architecture - Peer-to-Peer Network

- **Decentralization**
  - Resources and services are distributed over all nodes
  - Data exchange are among nodes, no central server, avoid potential bottleneck
- **Robustness**
  - Fault tolerance, node failures have little influences to the network



Server-based



P2P-network

Architecture

1) Data Structure

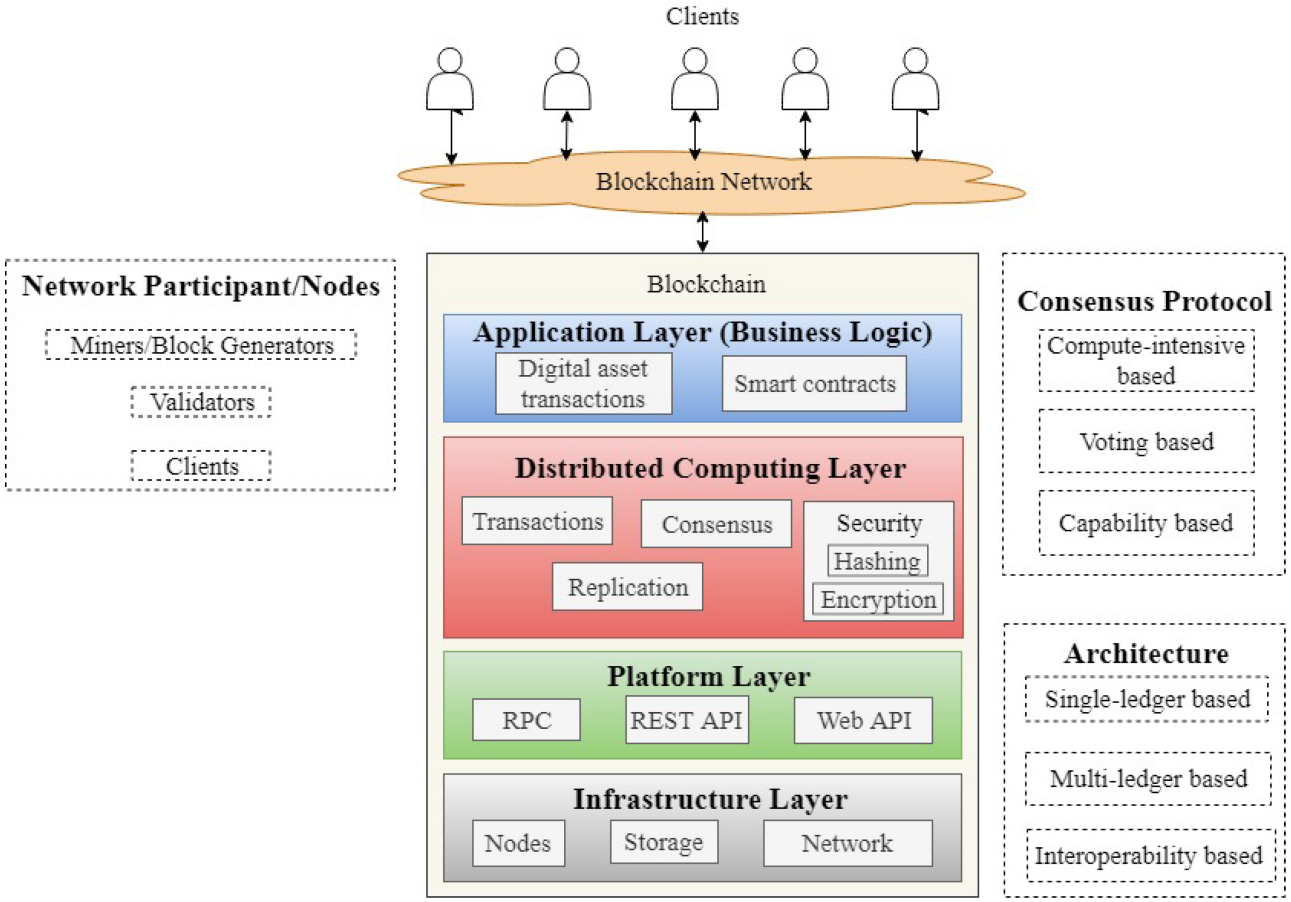
2) Peer-to-Peer Network

3) Consensus Algorithms

4) Smart Contract

5) Cryptography

6) Transaction



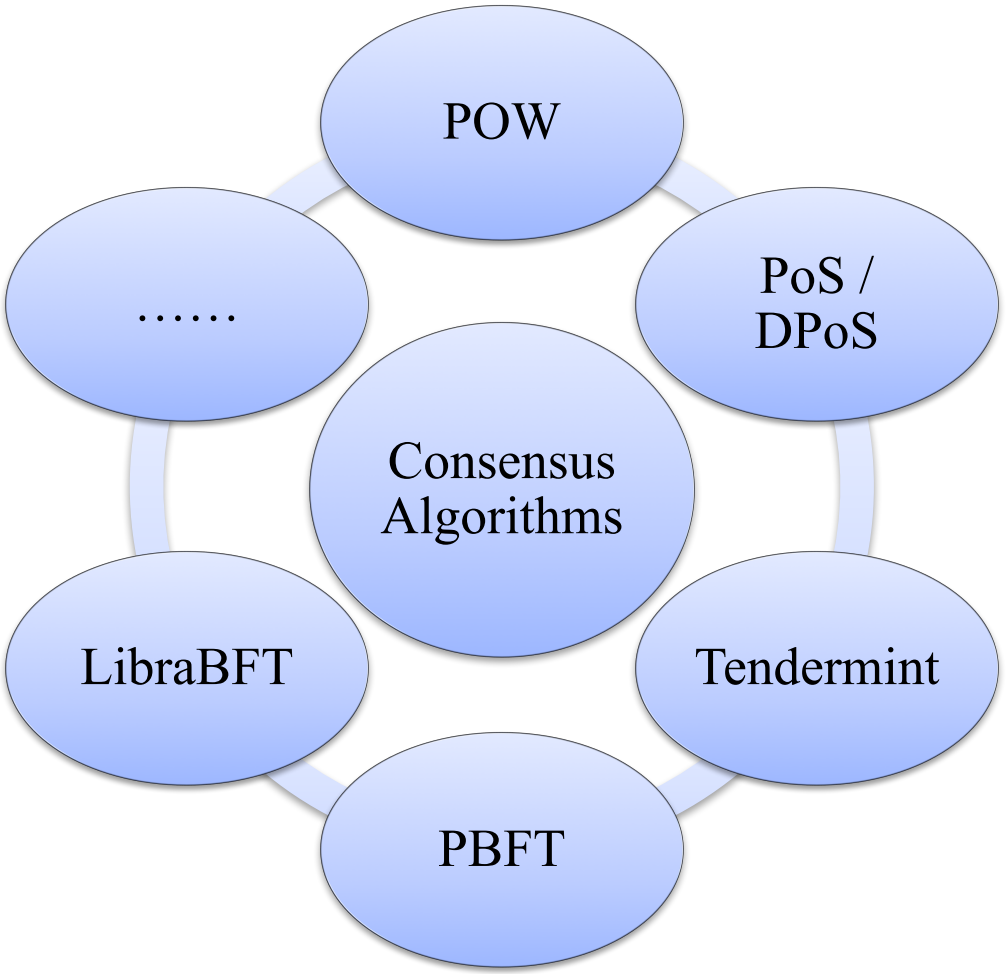
Architecture - Consensus Algorithms

Consensus in blockchain :

- **Validation -** Transaction is verified
- **Consistency -** Existence and relative order of transactions is consistent in every node

Architecture - Consensus Algorithms

- Crash Fault Tolerance
  - Paxos, Raft, ZAB
- **Byzantine Fault Tolerance**
  - PoW, PoS, DPoS
  - PBFT, IBFT, etc



Architecture

1) Data Structure

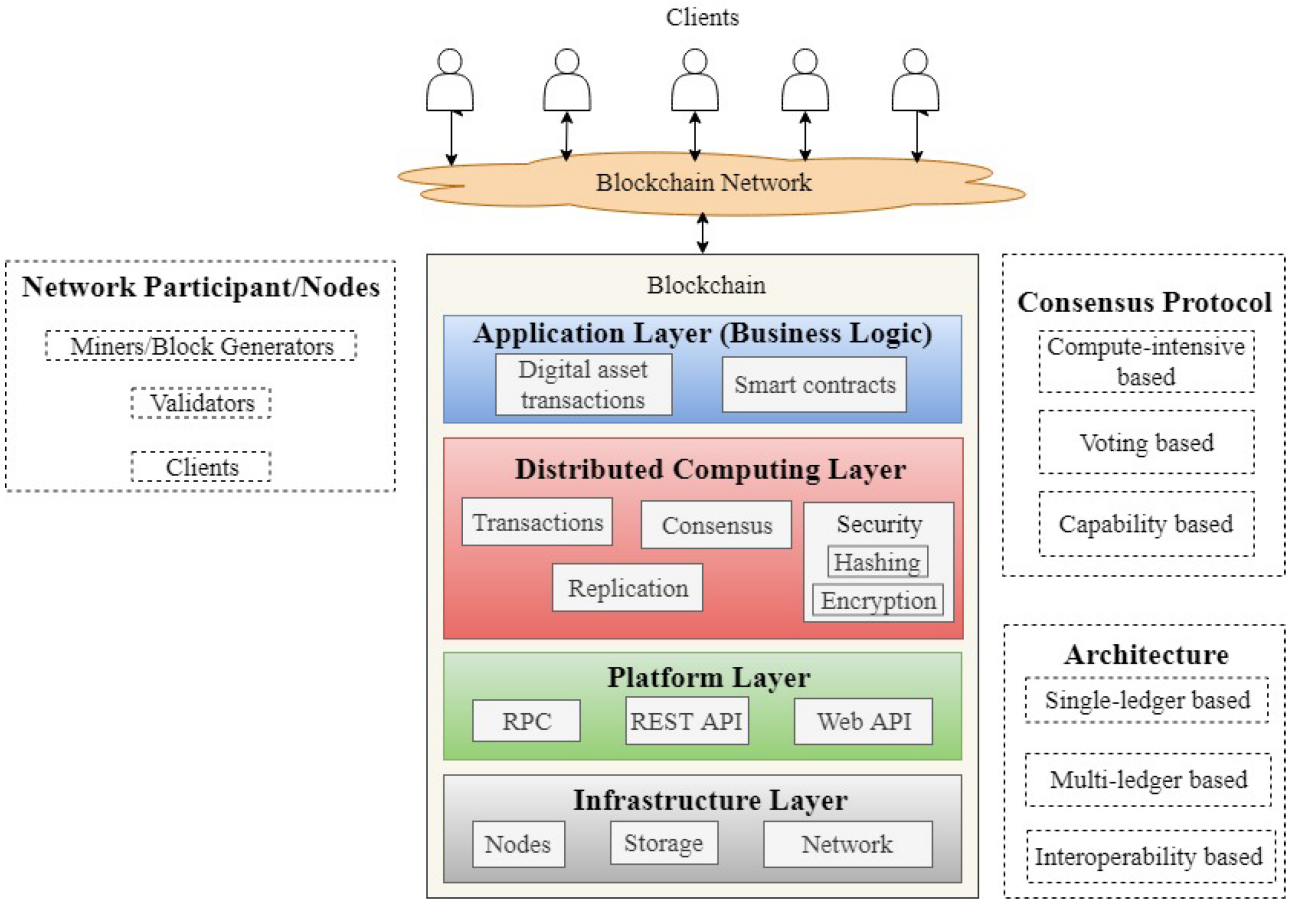
2) Peer-to-Peer Network

3) Consensus Algorithms

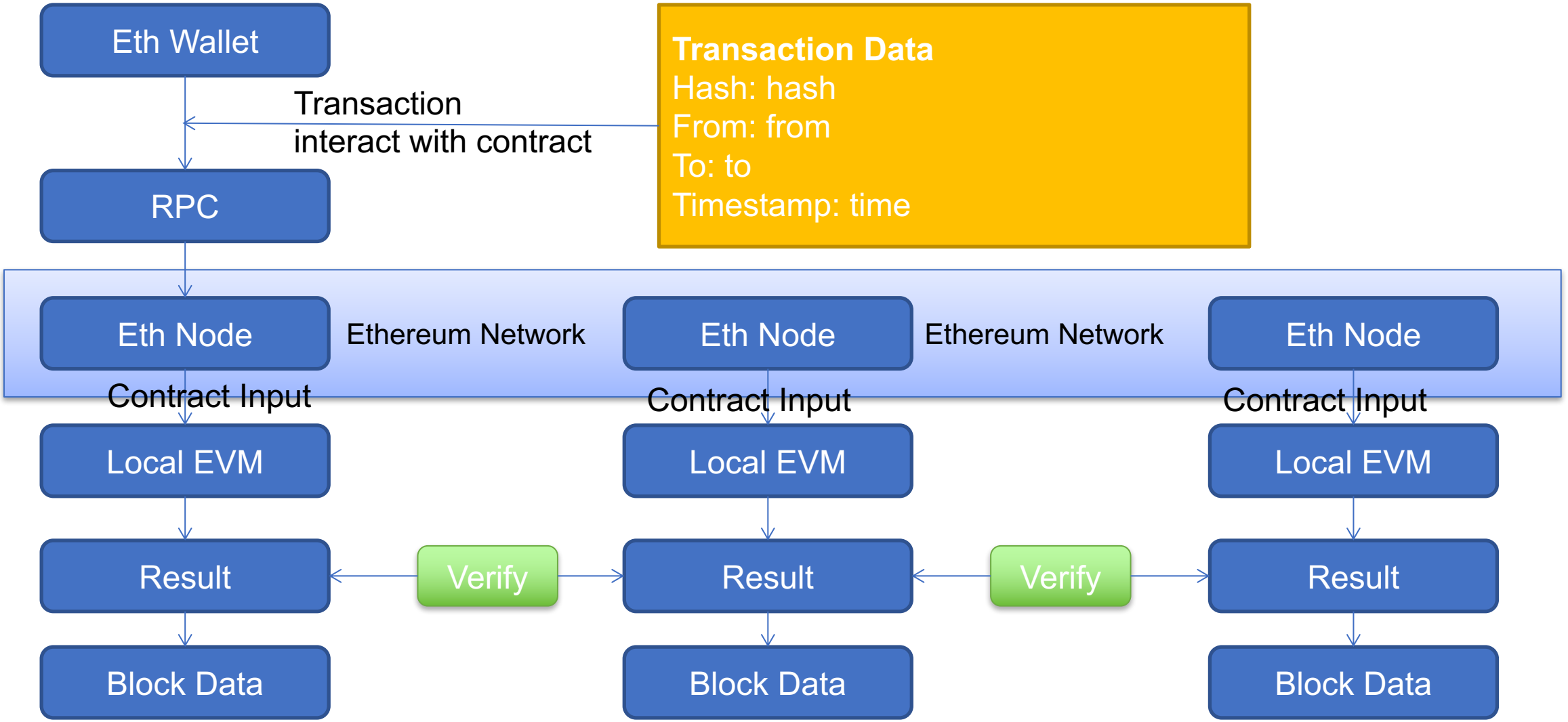
4) Smart Contract

5) Cryptography

6) Transaction



Architecture - Smart Contract



Architecture

1) Data Structure

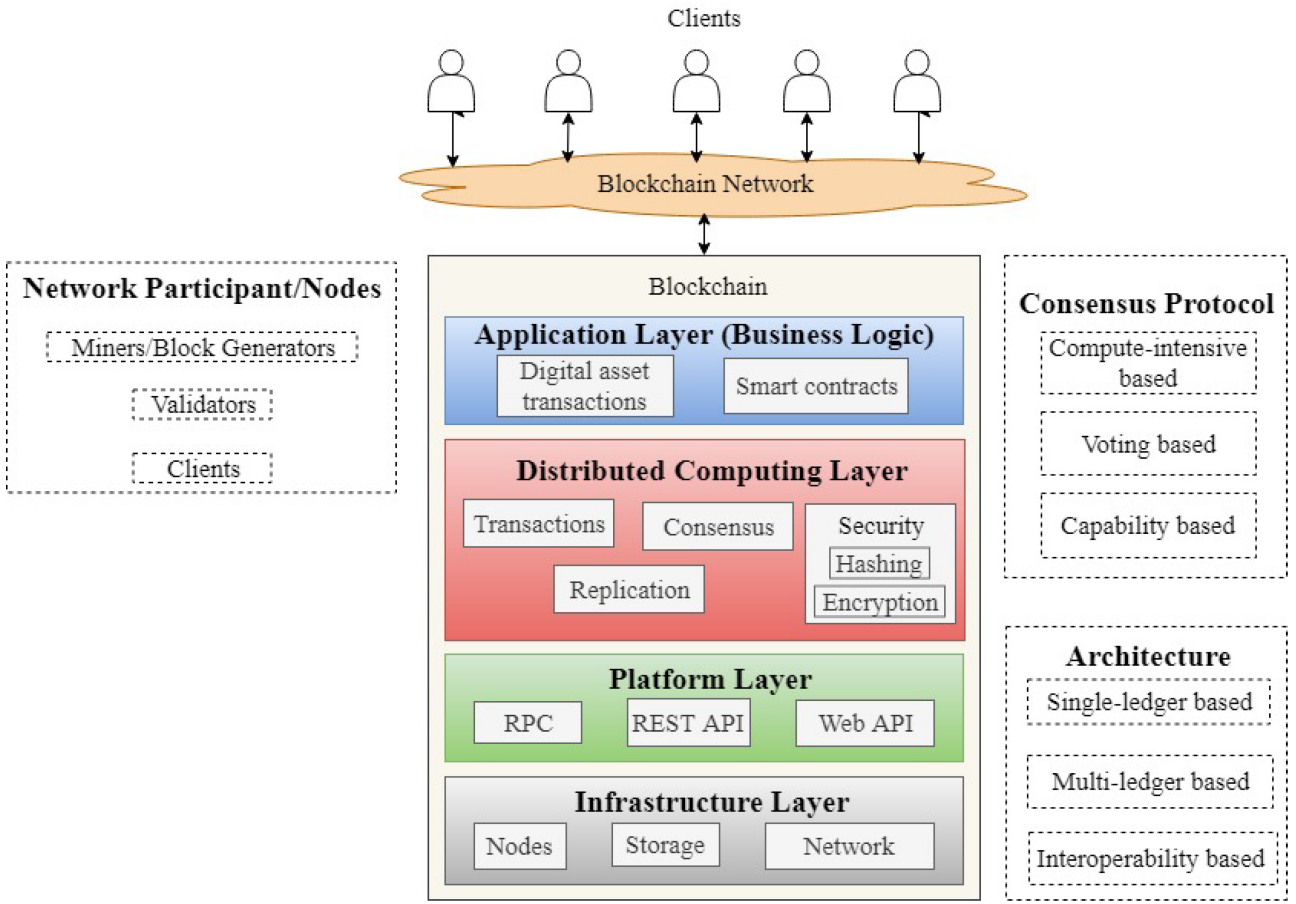
2) Peer-to-Peer Network

3) Consensus Algorithms

4) Smart Contract

5) Cryptography

6) Transaction



Architecture - Cryptography

Hash

MD5 , SHA1 , SHA256 , SHA3

- Easy to compute output
- Hard to get input from output
- Different input has different output*

Signature

ECDSA , RSA , BLS

- Can't be faked
- Can be verified by anyone

Encryption

3DES , AES , RSA-OAEP , ECIES

- Symmetric vs Asymmetric

Architecture

1) Data Structure

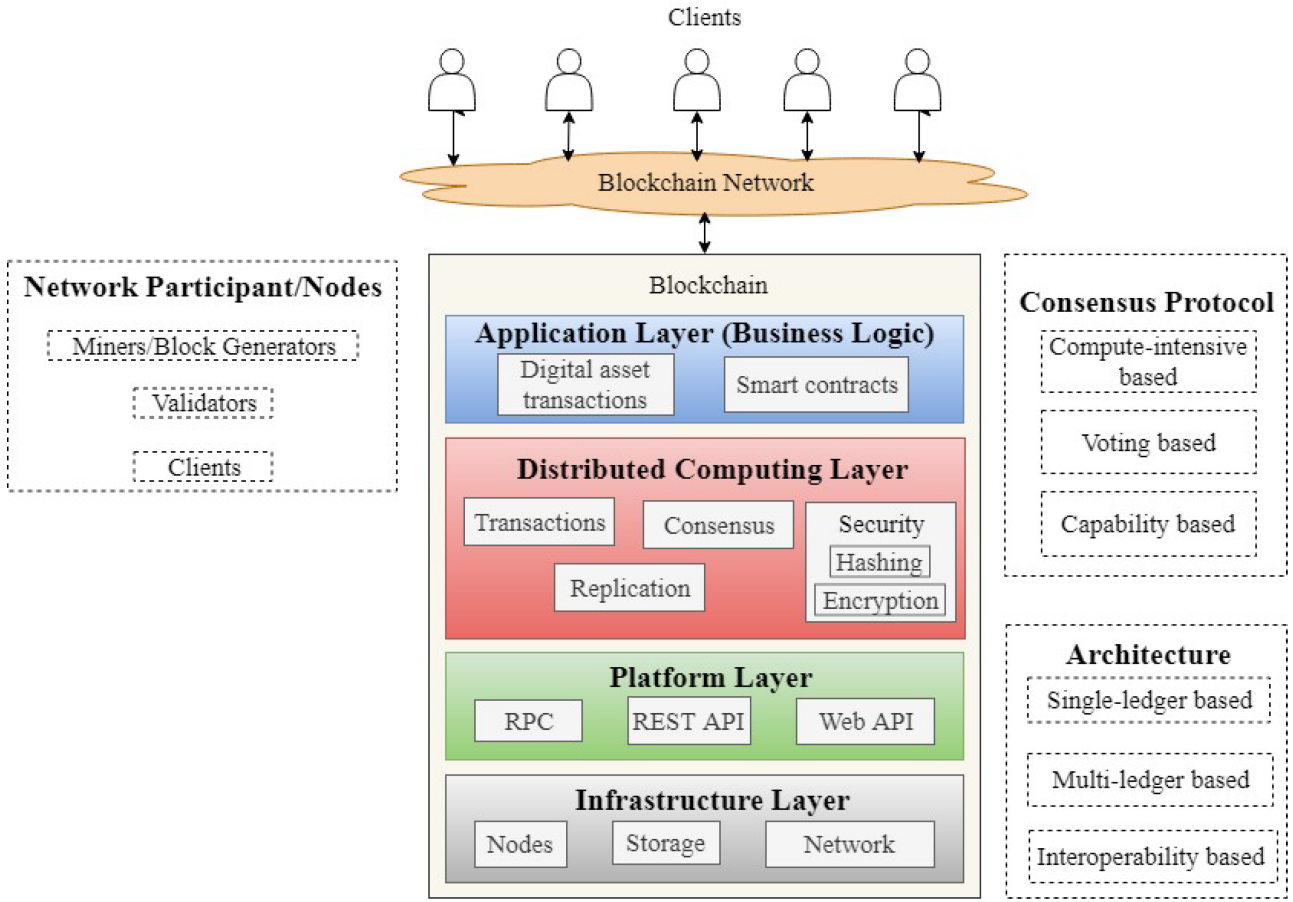
2) Peer-to-Peer Network

3) Consensus Algorithms

4) Smart Contract

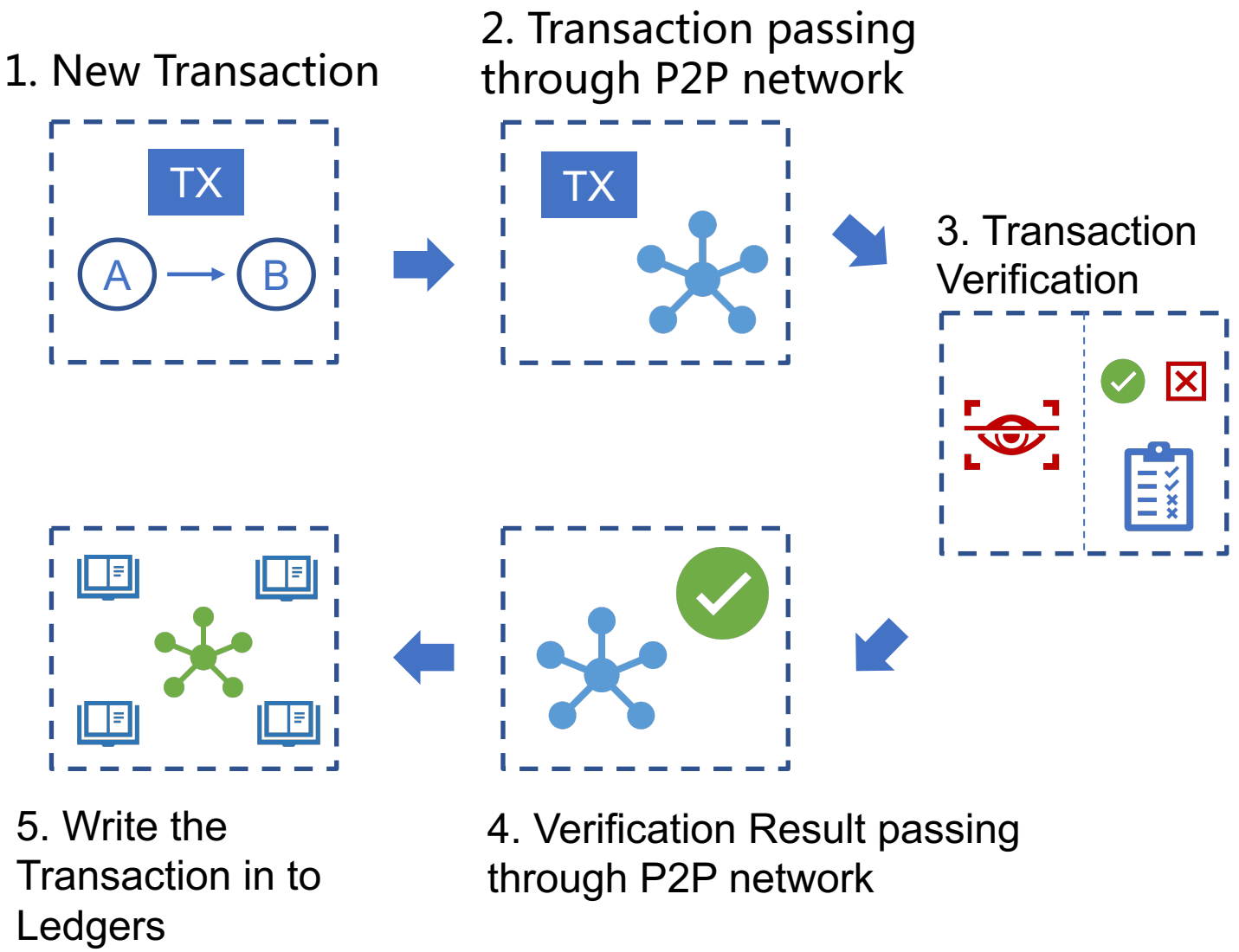
5) Cryptography

6) Transaction



Architecture - Transaction

1. **Create Tx & Sign**
2. **Broadcast**
3. **Tx Verification**
4. **Block Verification**
5. **Write to local**



Agenda for Today

Cui Can

Brief introduction of blockchain.

Thomas Jin

Introduction of cryptographic algorithms in popular public and consortium blockchain platform.

Gary Xu

Introduction of the data connection from IoT devices to blockchain.

Patty Tu

Introduction of blockchain applications with IoT.

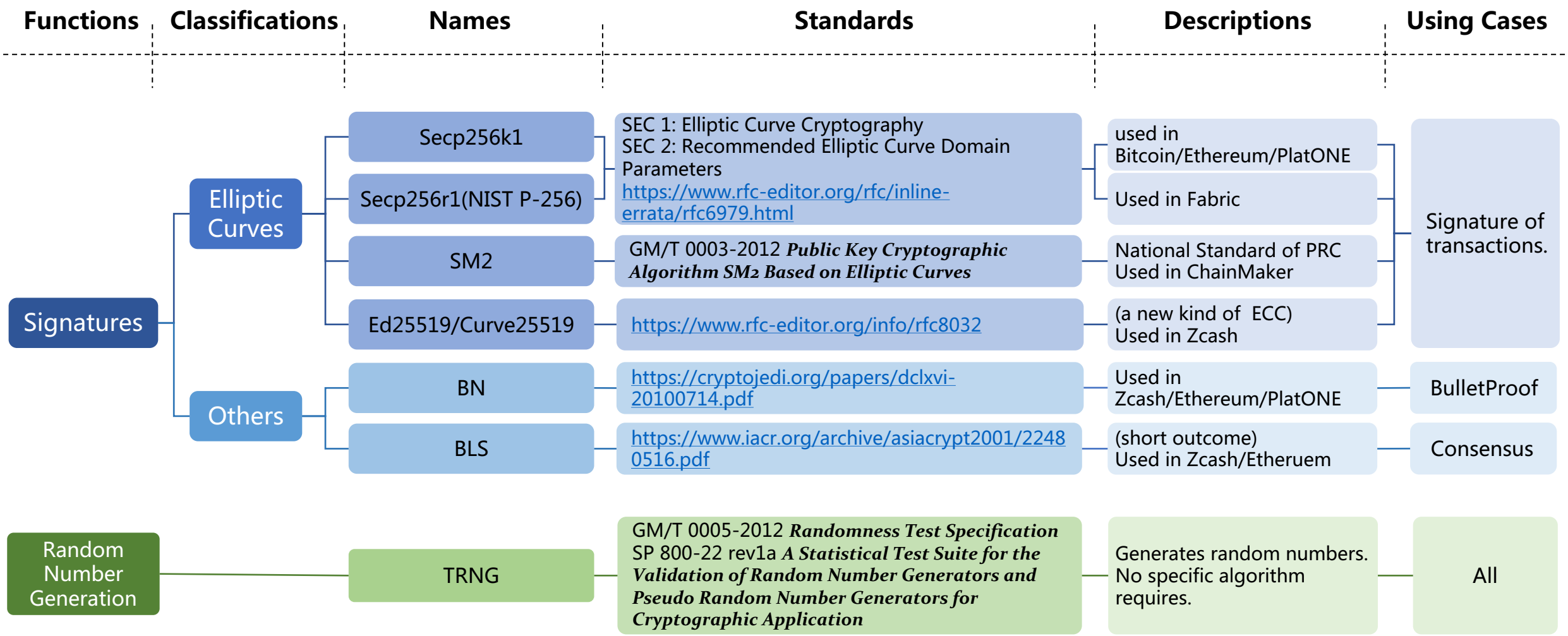
All

Open discussion of the next steps.

RISC-V®

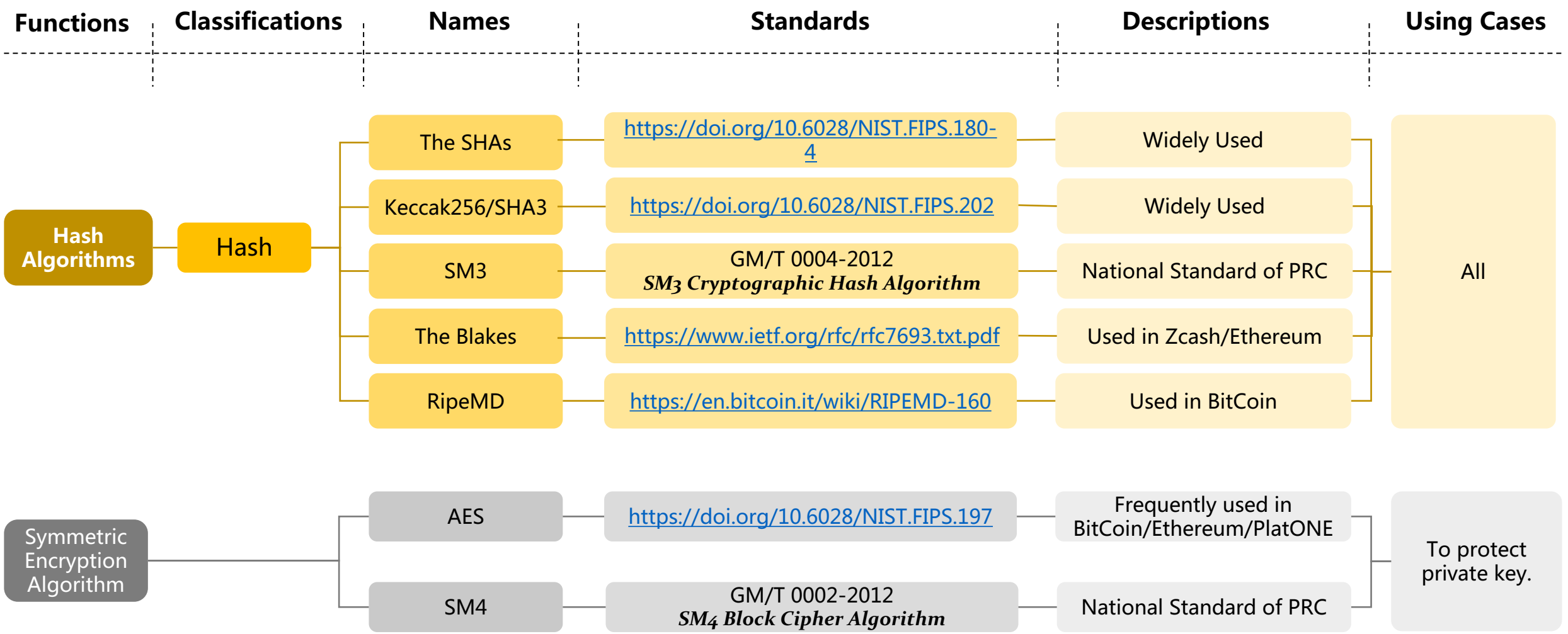
The Cryptographic Algorithms of Blockchain(1/2)

WANXIANG BLOCKCHAIN 万向区块链



RISC-V®

The Cryptographic Algorithms of Blockchain(2/2)



Agenda for Today

Cui Can

Brief introduction of blockchain.

Thomas Jin

Introduction of cryptographic algorithms in popular public and consortium blockchain platform.

Gary Xu

Introduction of the data connection from IoT devices to blockchain.

Patty Tu

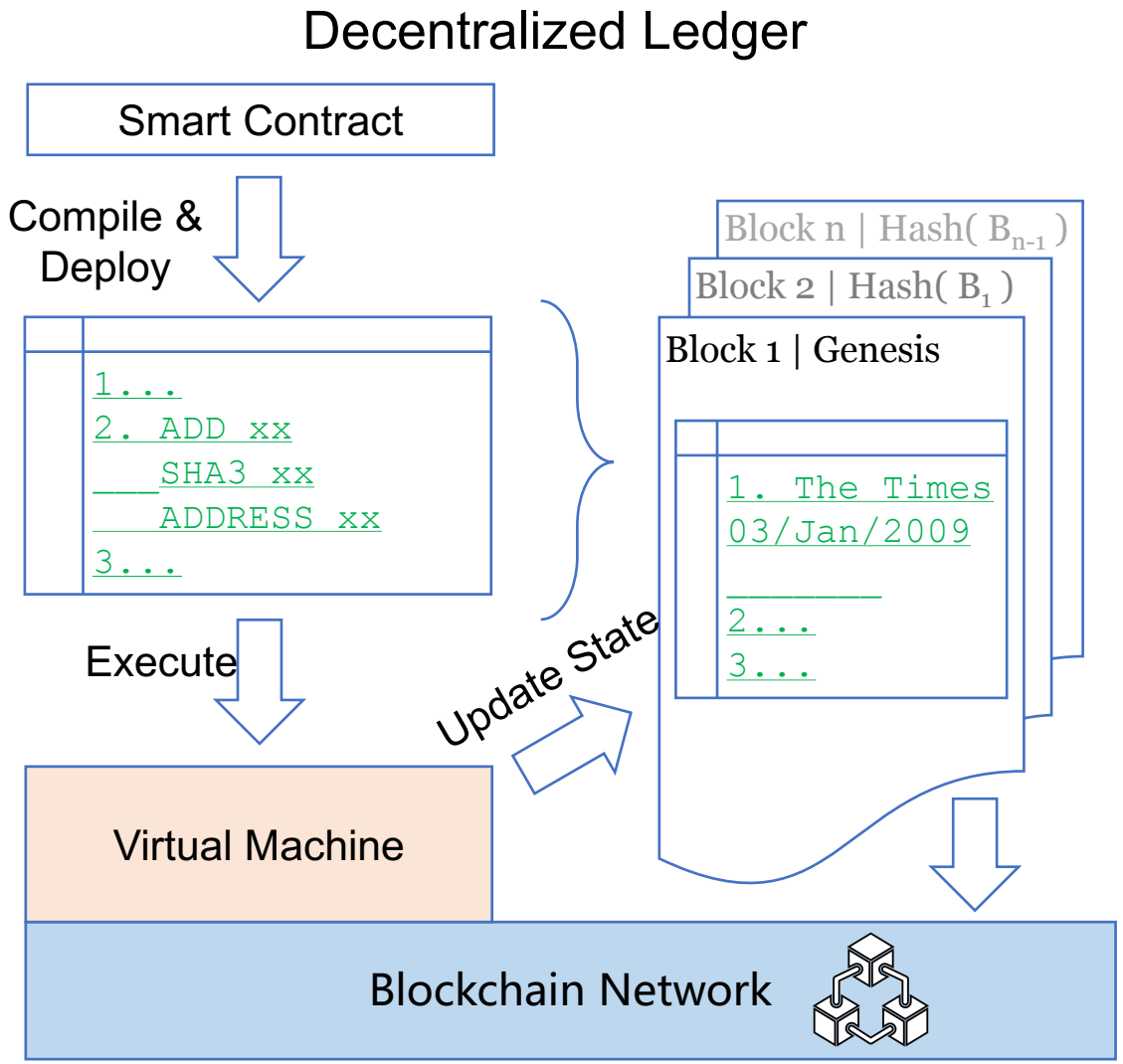
Introduction of blockchain applications with IoT.

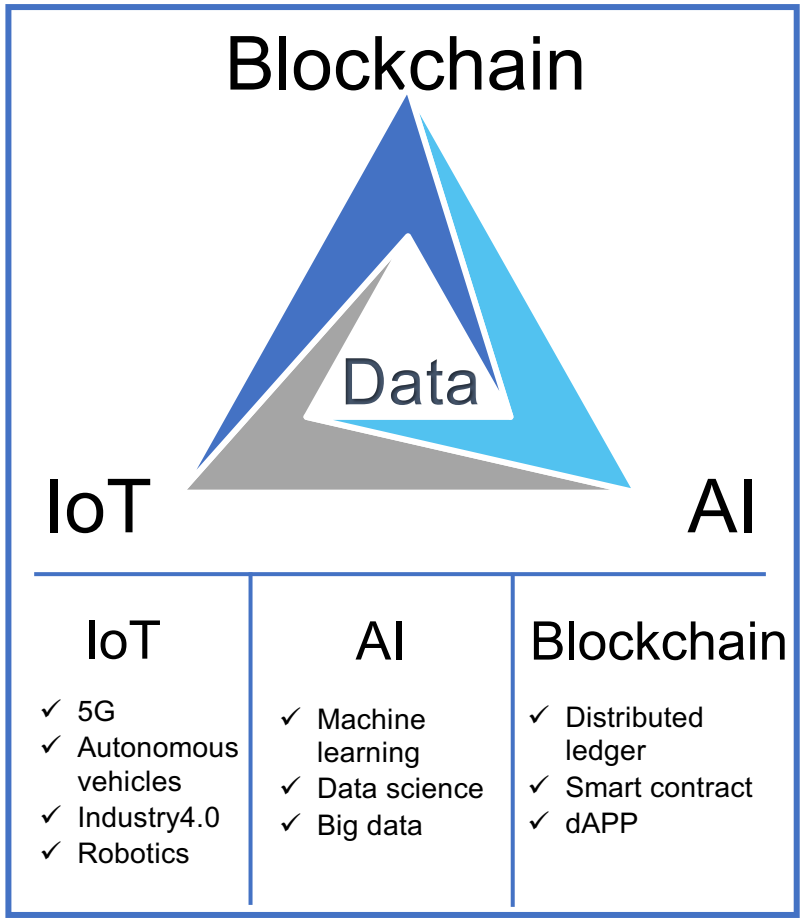
All

Open discussion of the next steps.

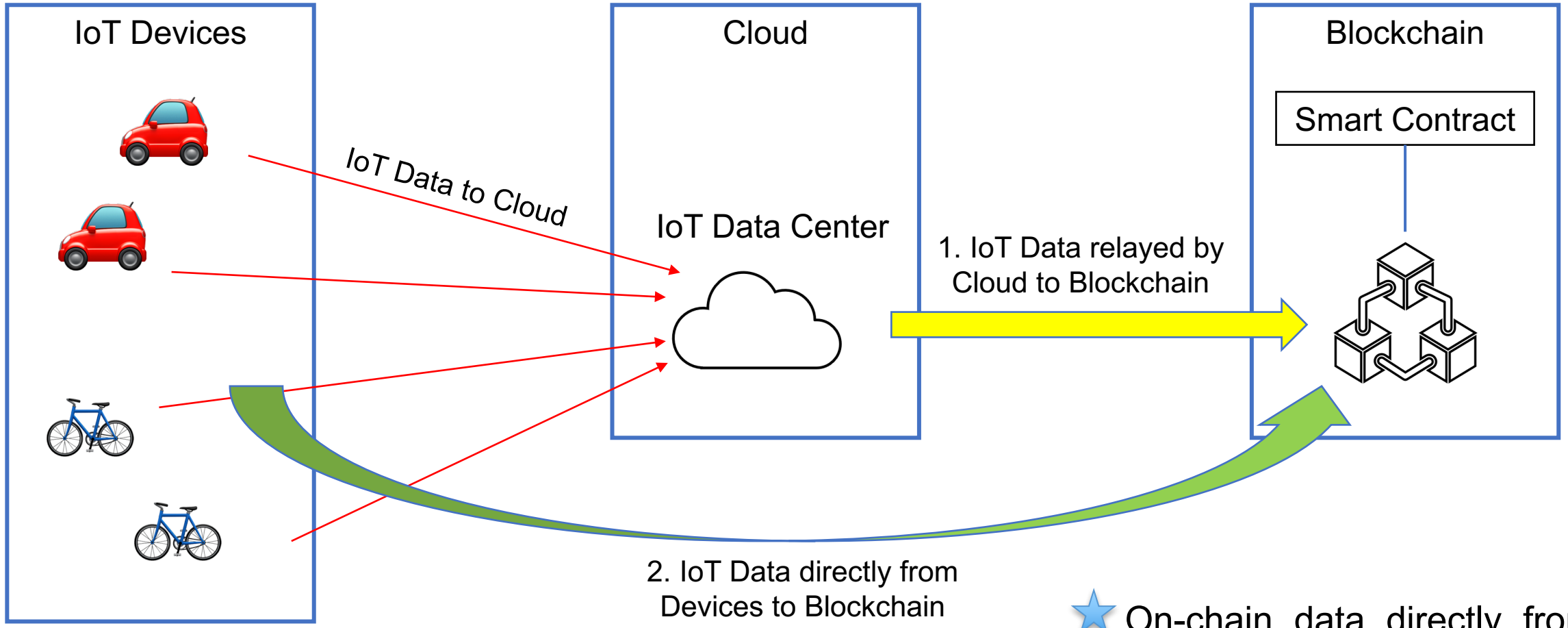
RISC-V®

Blockchain and Smart Contract



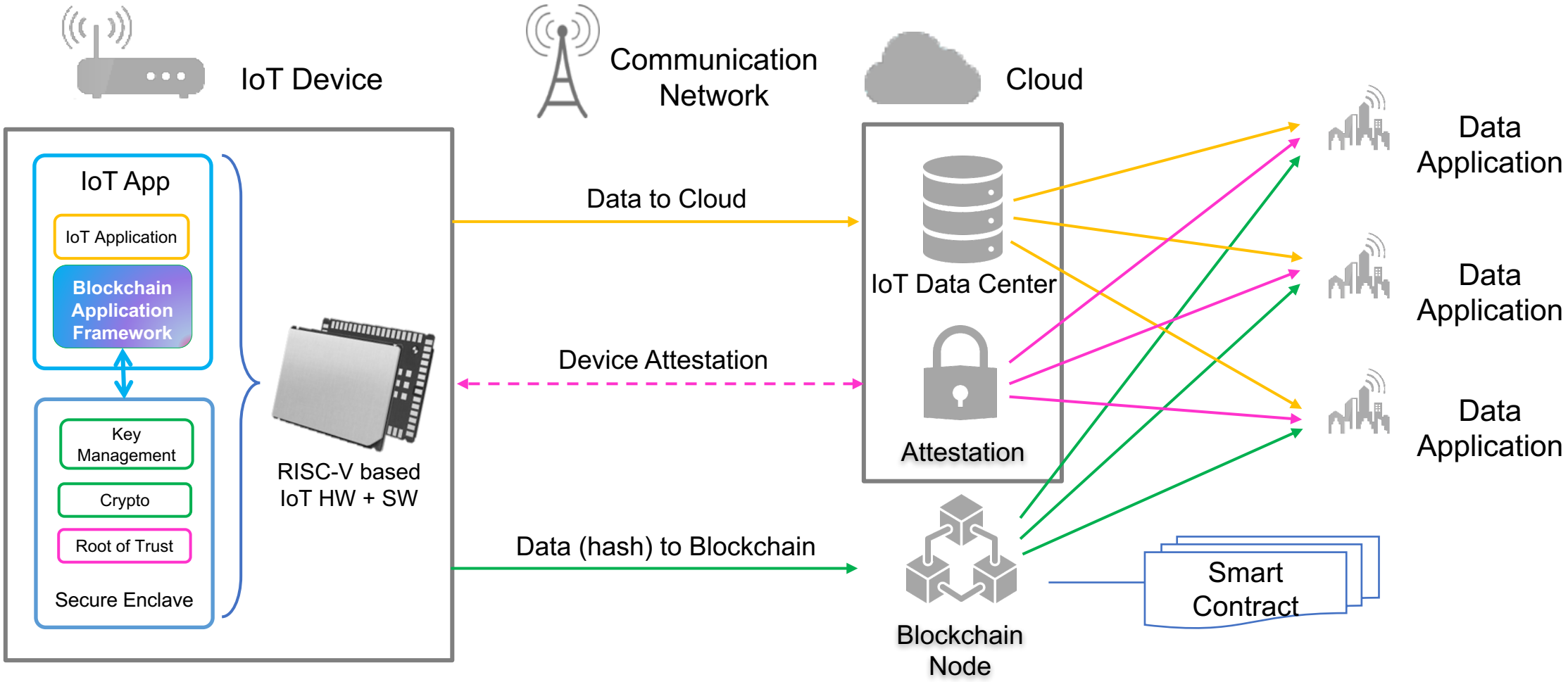


Blockchain + IoT Data Center or IoT Devices



★ On-chain data directly from devices are more trustworthy than those relayed by cloud

Blockchain + IoT Typical Usage



The RISC-V crypto extension may consider accelerating fundamental mathematic computation (e.g. bignum arithmetic) that is essential for elliptic cryptographic algorithm.

Agenda for Today

Cui Can

Brief introduction of blockchain.

Thomas Jin

Introduction of cryptographic algorithms in popular public and consortium blockchain platform.

Gary Xu

Introduction of the data connection from IoT devices to blockchain.

Patty Tu

Introduction of blockchain applications with IoT.

All

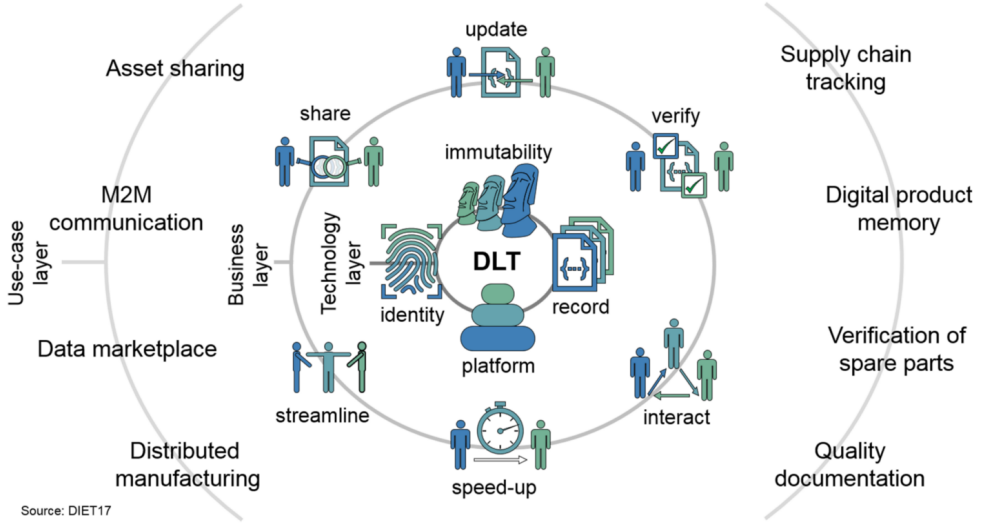
Open discussion of the next steps.

RISC-V®

What Brought Us to Blockchain?
– *the Ultimate Distributed System Logic*

The Case for Blockchain:

- Distributed Ledger: permanent tamper-free data records
- Smart contract: establish automated execution of prior agreement with set conditions; data accessible but not replicable
- Cryptography: data protection across domains
- Consensus: easily establish network of the willing without heavy IT and legal costs.



How to derive DLT use-case

Image: © WZL | Anton Shirobokov

Particularly Relevant to the Industrial Space

- Curated data sharing: addresses one of industrial internet's biggest challenges – why surrender your data.
- Seamless and real-time brokering of value exchange: from supply chain to value chain, cross-domain data utilization business model.
- Beyond data: could be used to allocate compute resources, in addition to running and training A.I. on mobile devices.

RISC-V®

Case Study:
Vision For A Distributed Energy Infrastructure

Battery Life Cycle- *Breaking Down Data Silos with Blockchain*

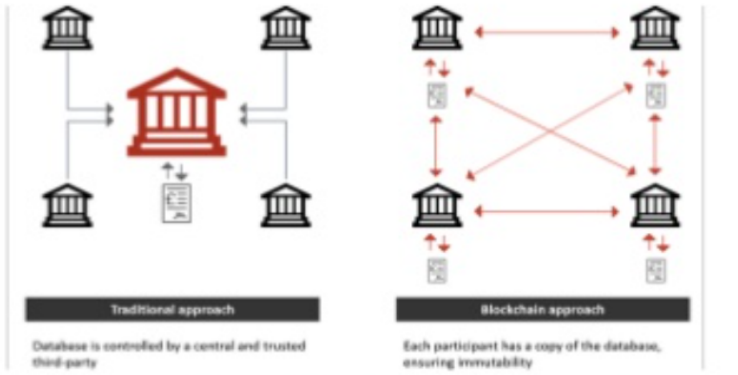
Problem: data collection across data silos, owned by enterprises in different industries.

Solution:

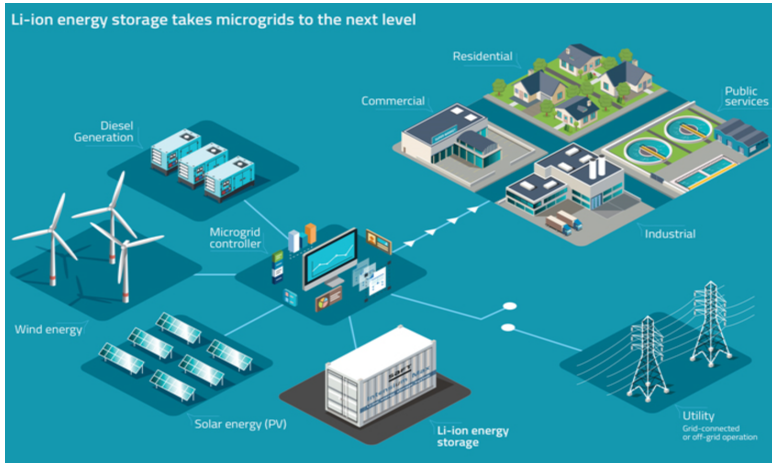
- Blockchain is used to track battery spec, recharge time, performance measurement and risk assessment. Tamper-free, permanent record of data.
- Assetize battery: calibrate remaining value of battery via charge time and max capacity

Improve transparency. Assure safety. Establish accountability.

Data Coll> Charging St



Traditional vs blockchain databases



China unicom

WANXIANG BLOCKCHAIN 万向区块链

GSMA

A123 SYSTEMS

Agenda for Today

Cui Can

Brief introduction of blockchain.

Thomas Jin

Introduction of cryptographic algorithms in popular public and consortium blockchain platform.

Gary Xu

Introduction of the data connection from IoT devices to blockchain.

Patty Tu

Introduction of blockchain applications with IoT.

All

Open discussion of the next steps.

RISC-V®

Thank You