Blockchain Technology Report for Tencent, 2017

Rujia Li
November 17, 2017

CONTENT

01

Introduction

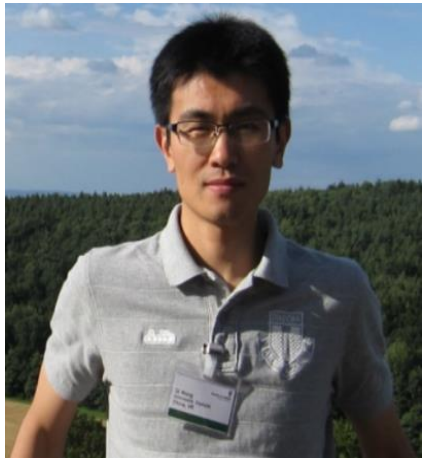
Team member

About me

Team member

Prof. Mark Ryan

Professor in Computer Security at UOB, EPSRC Leadership Fellow



Dr. Qi Wang

Assistant Professor at Southern University of Science and Technology

Dr. David Galindo

Senior Lecturer in Computer Security at University of Birmingham

Rujia Li

Ph.D. candidate at UOB and Sustech.

About me

Rujia Li

Web: http://rujia.uk
Blog: http://ehcoo.com

Blockchain, Applied cryptography, Consensus protocol, Distributed network, Key management

Education

•CSE, SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY
Ph.D. candidate 01/2018 - 01/2021
•CS, UNIVERSITY OF BIRMINGHAM
Master of Advanced Computer Science 09/2016 - 01/2018
•LJCS, WUHAN UNIVERSITY
Bachelor's Degree in Computer Science 09/2009-07/2013
•SEM, WUHAN UNIVERSITY
Dual Bachelor's Degree in Business Administration 09/2009-07/2013

Employment

•UNIVERSITY OF BIRMINGHAM INNOVATION CENTRE
Position: Internship 06/2017-09/2017
•STATE GRID INFORMATION & TELECOMMUNICATION CO,.LTD
Position: Secure Architect Assistant 12/2014-08/2016
•STATE GRID ELECTRIC POWER RESEARCH INSTITUTE
Position: R & D Engineer 04/2013-11/2014

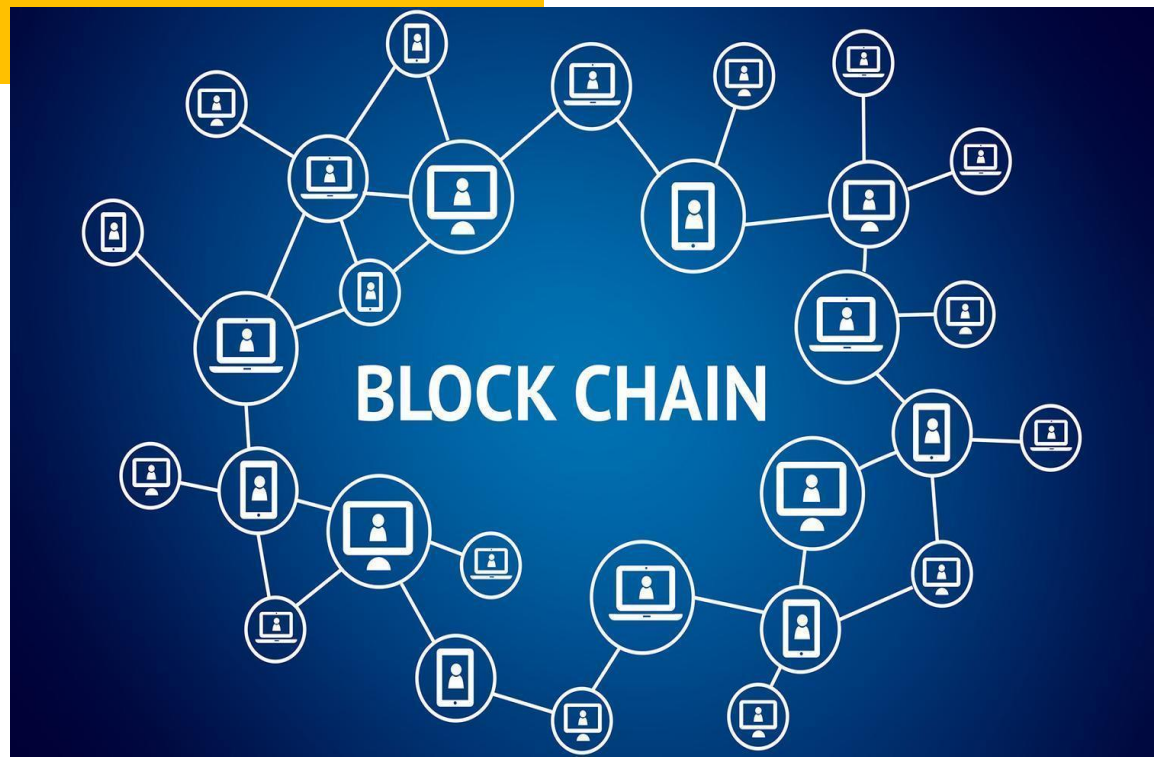
02 Blockchain Overview

Bitcoin & Blockchain

How does Blockchain works

Four elements characterize Blockchain

Bitcoin & Blockchain



a peer to peer electronic cash system

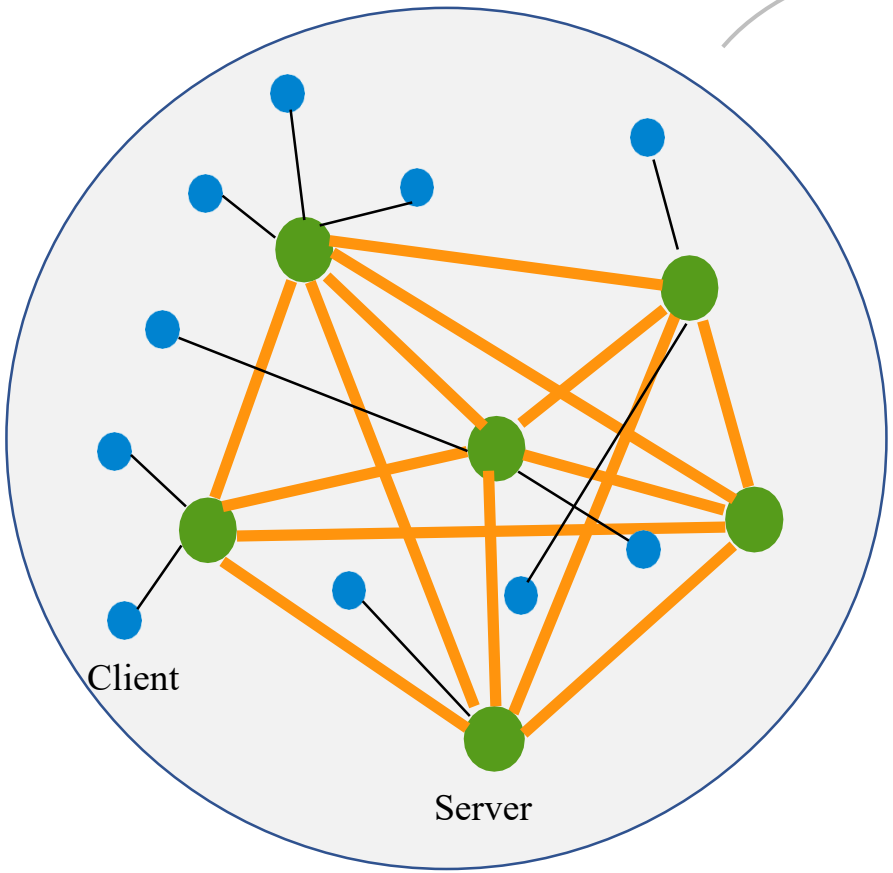
Bitcoin

Bitcoin is software-based online payment system described by Satoshi Nakamoto in 2008. and introduced as open-source software in 2009 [1].

Blockchain

Blockchain is a distributed database that maintains a keep-growing list of ordered records called block. [1]
Each block contains a header and a list of transactions .
Each header includes a timestamp, a link to a previous block and nonce.

How does the Blockchain works - Workflow



- Grab the least transaction state form the Blockchain
- Generate a raw transaction by protocol
- Broadcast the transaction to the P2P network
- Collect and verify the transaction, relay to other nodes
- Merge the transaction to the block and append the block to the blockchain
- Broadcast the new blockchain state to other nodes

How the Blockchain works - Transaction

Transaction structure

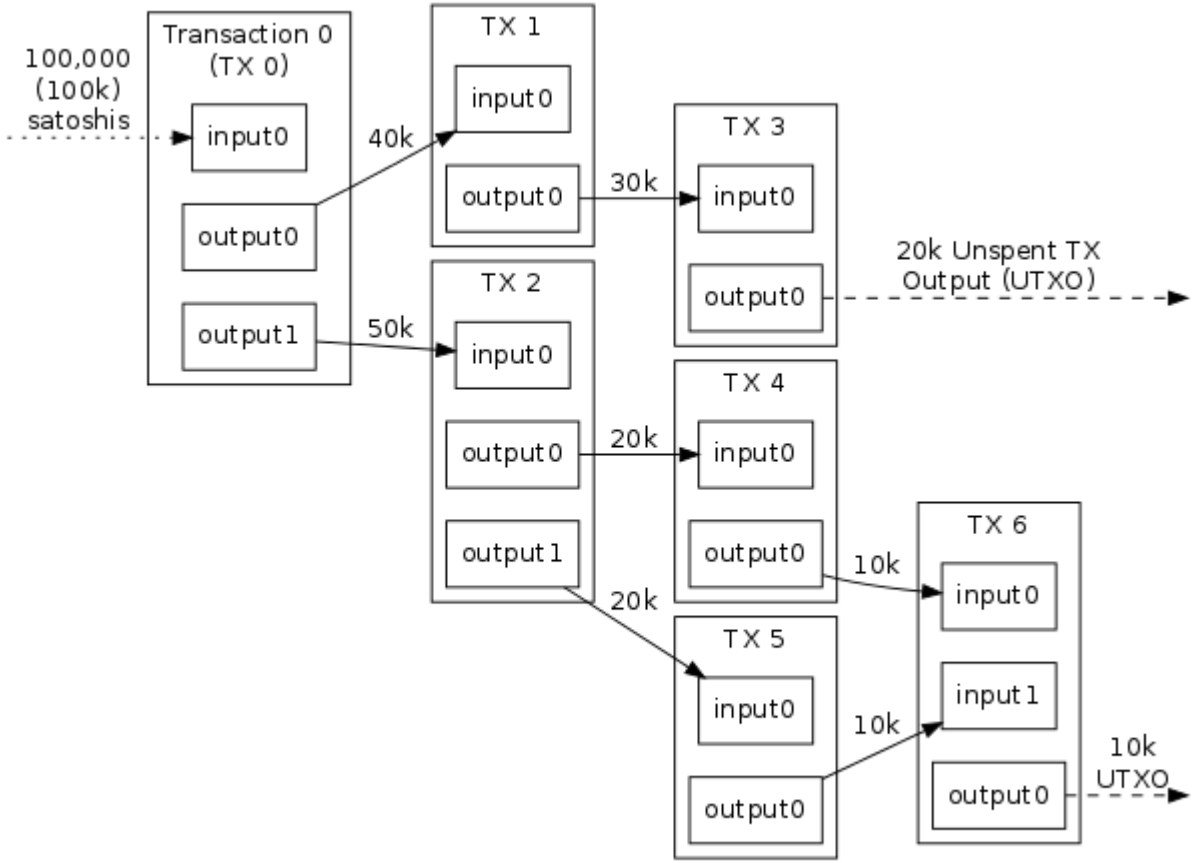
Type	Size
Version number	4 bytes
In-counter	1 - 9 bytes
list of inputs	<in-counter>-many inputs
Out-counter	1 - 9 bytes
list of outputs	<out-counter>-many outputs
lock_time	

Inputs

- Privious_output
- ScriptSig
- Sequence
- …..

Outputs

- value
- Script
- …..



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Image source: https://21.co/learn/the-blockchain/

How the Blockchain works -Script

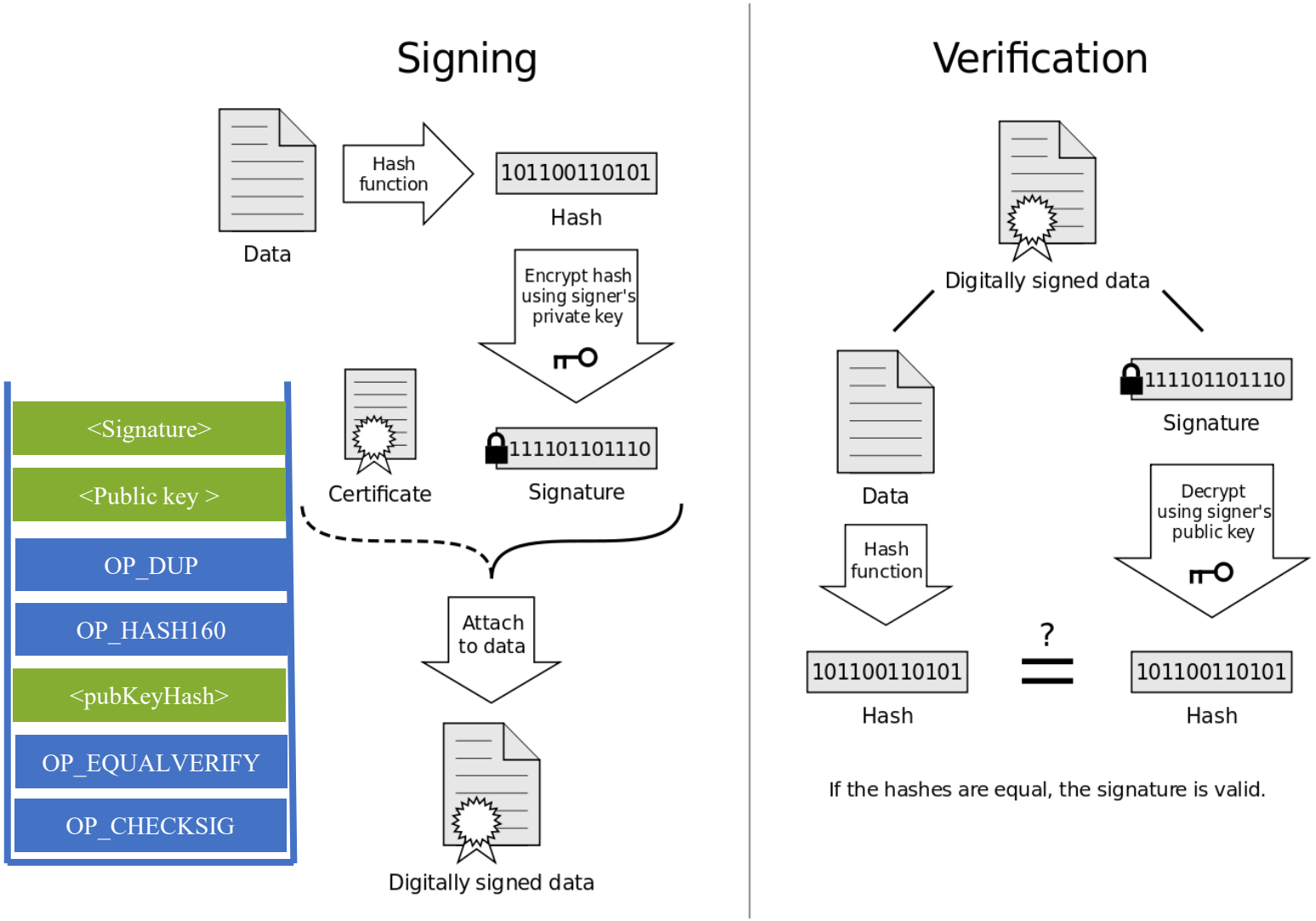


Image source: https://commons.wikimedia.org/wiki/File:Digital_Signature_diagram.svg

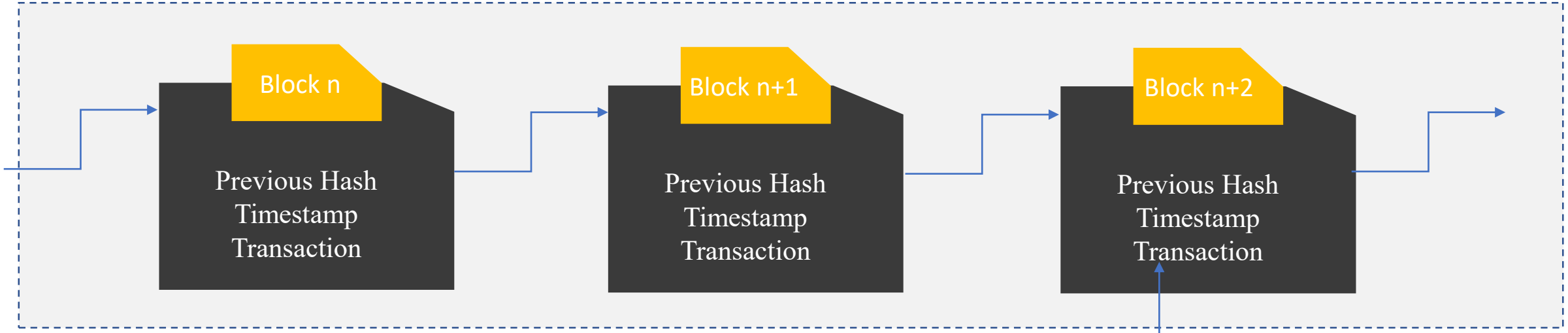
Locking script

A locking script is an encumbrance placed on an output, and it specifies the conditions that must be met to spend the output in the future.

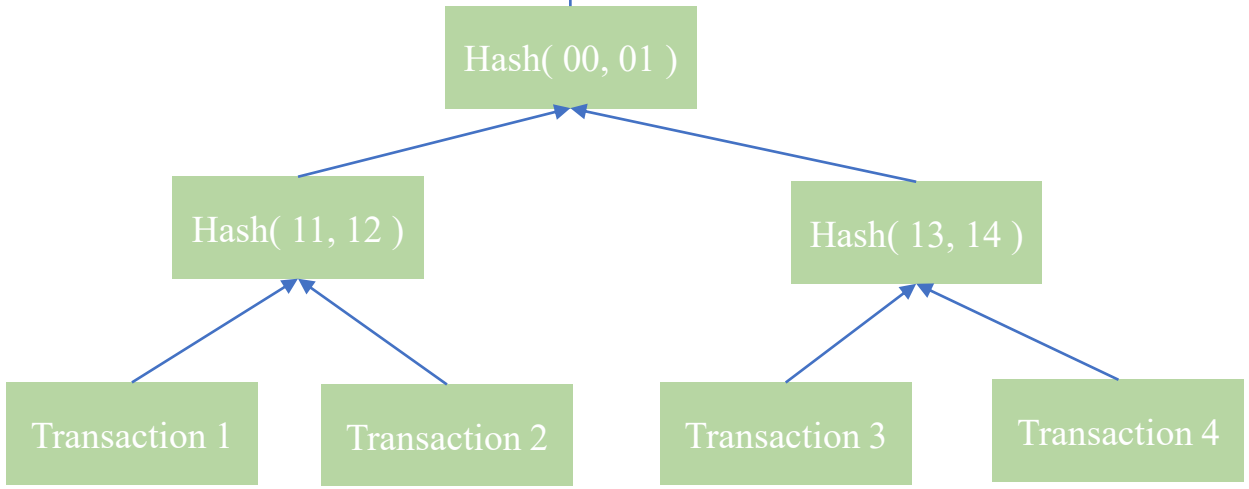
Unlocking script

An unlocking script is a script that "solves," or satisfies, the conditions placed on an output by a locking script and allows the output to be spent.[10].

How the Blockchain works –Block data structure



The blockchain data structure is an ordered, back-linked list of blocks of transactions. The blockchain can be stored as a flat file, or in a simple database. Blocks are linked "back," each referring to the previous block in the chain. [10].



Four elements characterize Blockchain

Replicated ledger

History of all transactions

Append-only with immutable past

Distributed and replicated

Cryptography

Integrity of ledger

Authenticity of transactions

Identity of participants

Consensus protocol

Decentralized protocol

Shared control tolerating disruption

Transactions validated

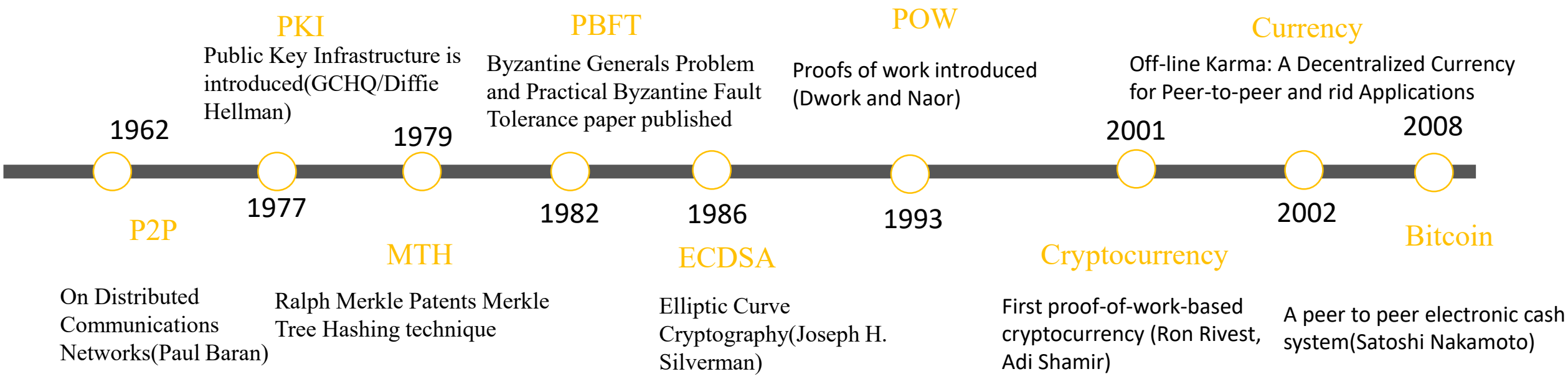
Business logic

Logic embedded in the ledger

Executed together with transactions

Self-enforcing "smart contracts" [4]

Blockchains underpinned by academic innovation



03

Blockchain Research

Blockchain issues

Blockchains research in academia

Our research

Blockchain issues

- **Technical Issues.**

Transaction speed, platform interoperability, verification process, and data storage will be crucial in making blockchain widely acceptable [6].

- **Security, Privacy and Control Issues.**

Ensuring data security & privacy among parties are main concerns. As the blockchain transactions are recorded in the distributed public ledger, it offers hackers a larger attack surface to gain access to critical and sensitive information.

- **Interoperability**.

There will be many implementations of blockchain systems. Platforms and apps will need to talk to each other. Different systems on different platforms should be able to allow the data flow.

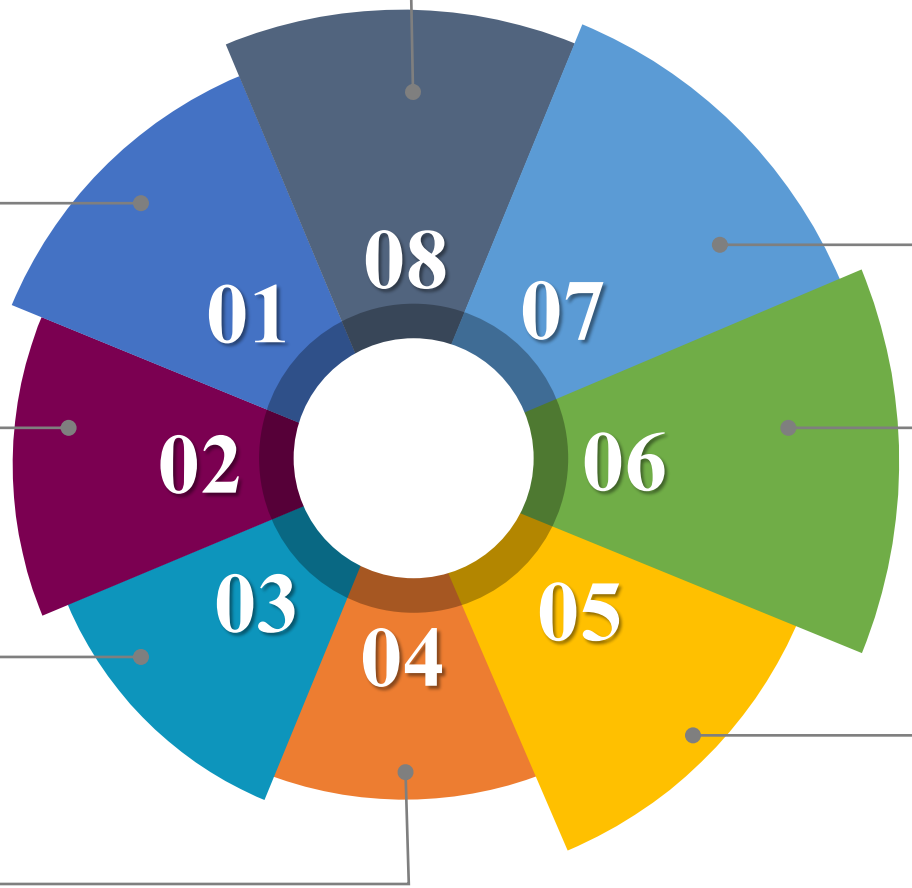
- **Governmental Regulation.**

A decentralized approach to identity and transaction management reduces the control of governments and corporations.

- **Cultural Change.**

Changing from legacy systems may be hard. Blockchain will change business processes, models, and perhaps entire industries

Blockchains research in academia



01 The data in blockchain is trusted, immutable, traceable and transparent.

02 Smart Contract based application

03 Security(Network, data), Privacy and Control Issues

04 Performance, scalability (consensus algorithm gossip protocol)

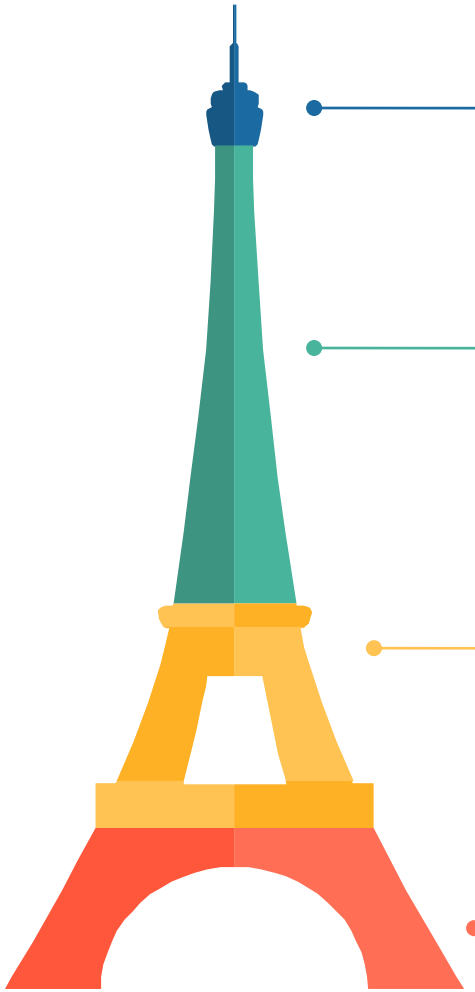
05 Digital Currency and its economic impact analysis[7]

06 The Blockchain as a Software Connector; Blockchain based system architecture

07 Decentral applications (Filecoin, IPFS)

08 Cryptographic protocol (Homomorphic encryption, Zero knowledge proof)

Our Research at Sustech and Birmingham



Engineering

The Systematic application of scientific and technological knowledge, methods, and experience to the design, implementation, testing, and documentation of software.

System

A system has Components as its structure and observable inter-process communications as its behavior. Such as Bitcoin, Ethereum.

Protocol

A protocol is a set of Rules that governs how a system operates. The rules establish the basic functioning of the different parts[12]. Such as POW and Kademlia.

Algorithm

An algorithm is an unambiguous specification of how to solve a class of problems in Mathematics [11]. Such as SHA, ECDSA.

Our Research at Sustech and Birmingham

Immutable data and traceability

- An academic certificate authentication using blockchain technology
  Collaborator: MIT Media Lab, ITIC Birmingham
- An e-voting system based on blockchain and ring signature
  Collaborator: Yifan Wu, SC at University of Birmingham

Consensus algorithm analysis

- blockchain consensus algorithm analysis (proof of authority)
  Collaborator: Beijing HuaLian Technology Co., Ltd.

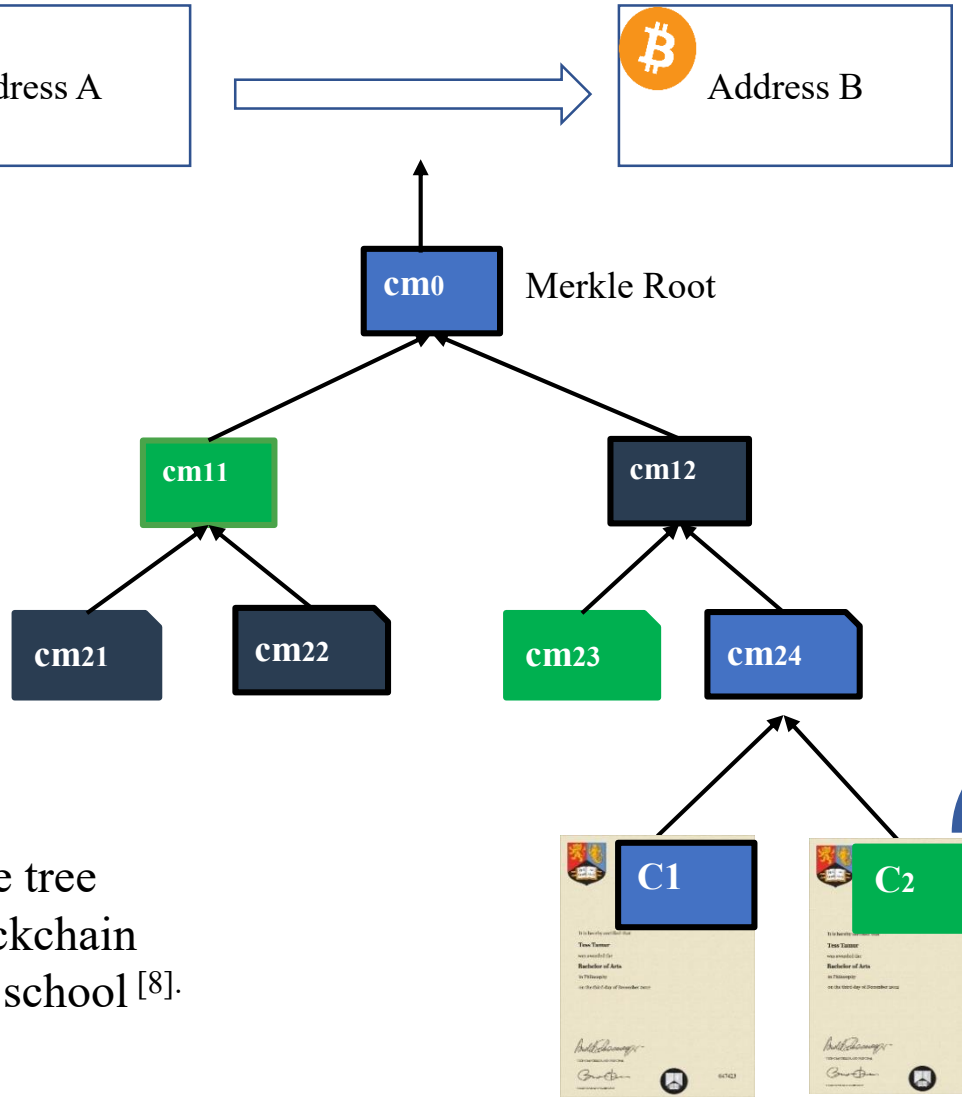
Smart contracts

- An intellectual-property protection model utilized smart contract
  Collaborator: Southern University of Science and Technology .
- An automatic and distributed system for tracing original news
  Collaborator: DMTLab, Birmingham city University

Cryptographic key management

- Ledger-based end-to-end secure messaging system
  Collaborator: Dr. JiangshanYu, University of Luxembourg.
- EthIKS: Using Ethereum to audit a CONIKS key transparency log
- Collaborator: CONIKS Team, Princeton university

Blockchain based academic certificate



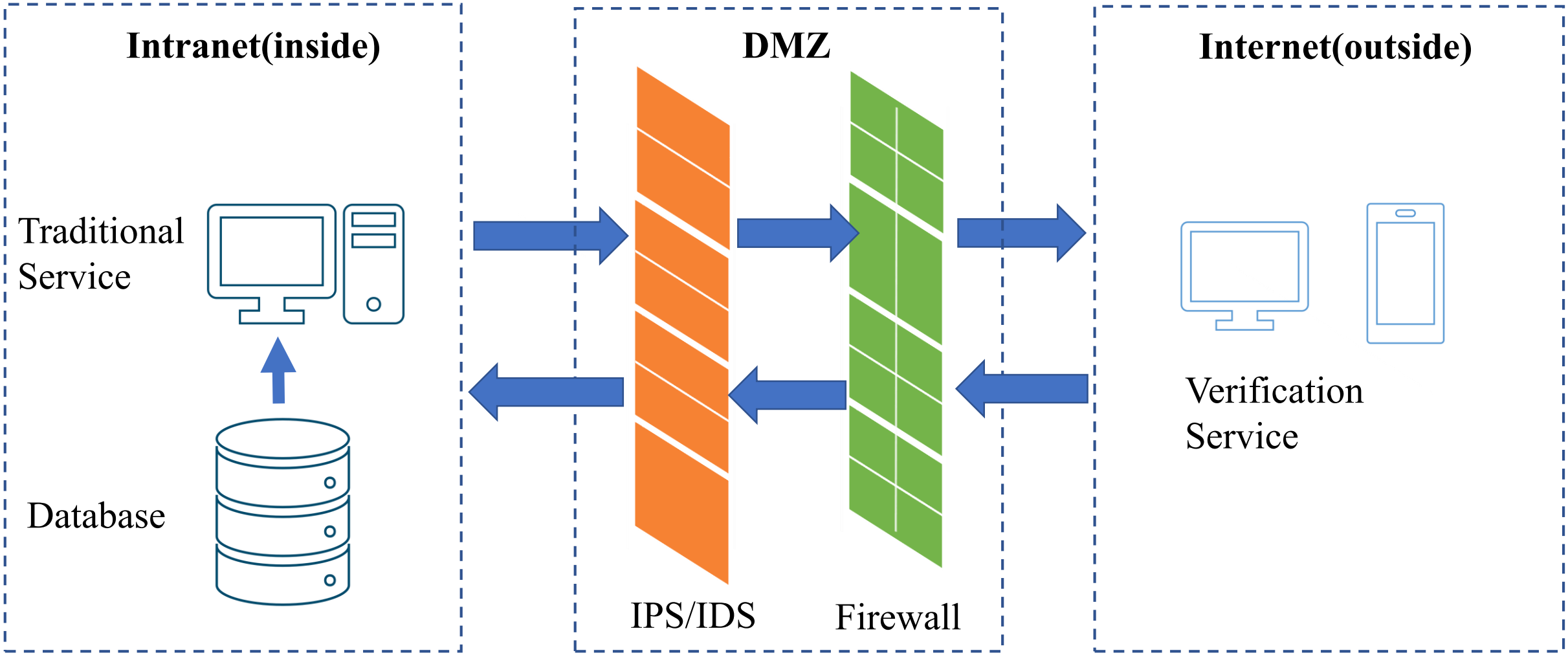
Security Federated Identity
Multi-signature

$cm_0 = Hash(cm_{11}, cm_{12})$
$cm_{11} = Hash(cm_{21}, cm_{22})$
$cm_{21} = Hash(C_1, C_2)$

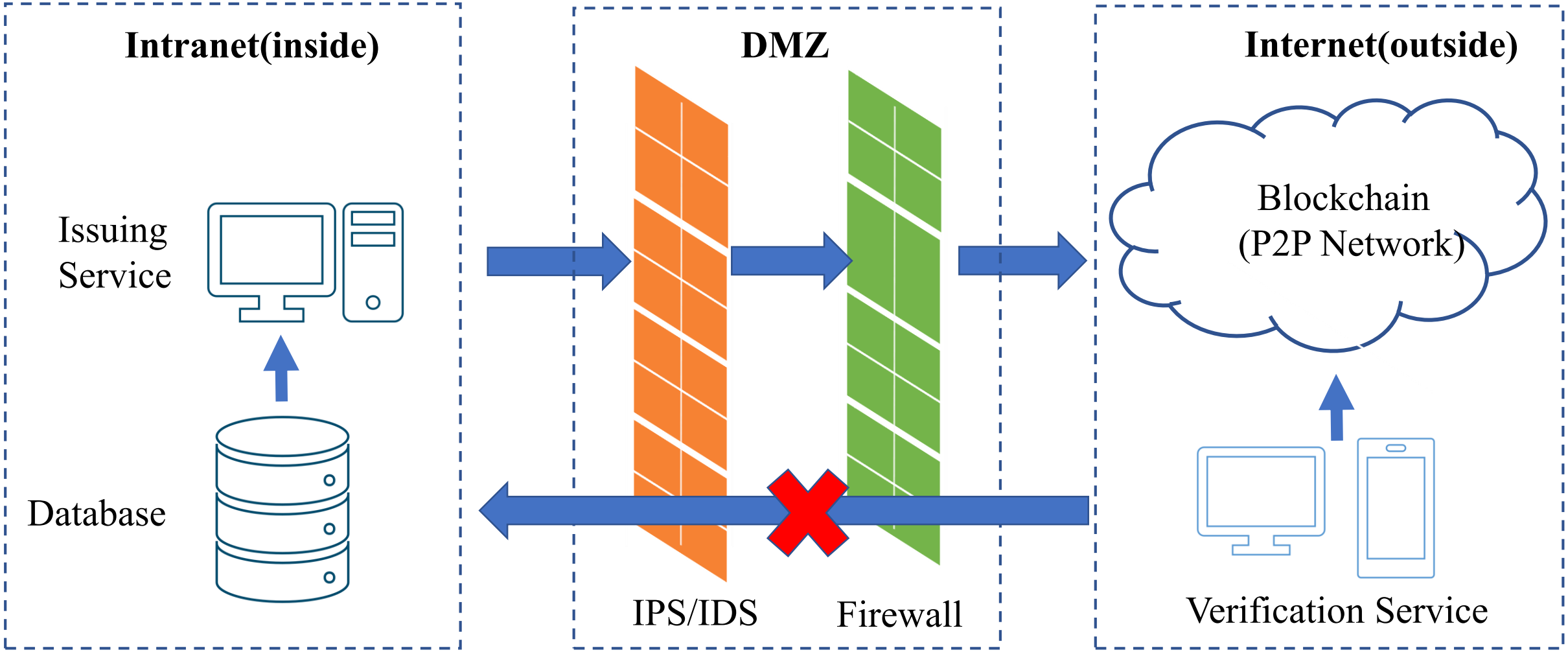
$Prove\_presence(cm_0, C_1) = (C_2, cm_{23}, cm_{11})$.

1. Ensure the certificate is in the Merkle tree
2. Ensure the Merkle Root is in the blockchain
3. Prove the address is belonged to this school [8].

Blockchain based academic certificate



Blockchain based academic certificate



Blockchain based e-voting system

BLOCK VOTES

E-voting

A real e-voting system for Registration Authority, Election Authority, Voters, Candidates [9].

Blockchain

The public ledger to store the information of signatures and candidate id. It protect the privacy of voters

Ring Signature

A signature algorithm to sign the candidate id to ensure the verifiability of individual and universal

BlockVotes

An e-voting system based on blockchain and ring signatures.

The network of blockchain can choose the bitcoin and the testnet

04

Conclusion

Value of Blockchain technology
Blockchain development
Future of Blockchain

Value of blockchain technology

Decentralised

Digital currency

Smart Contracts

Decentral applications

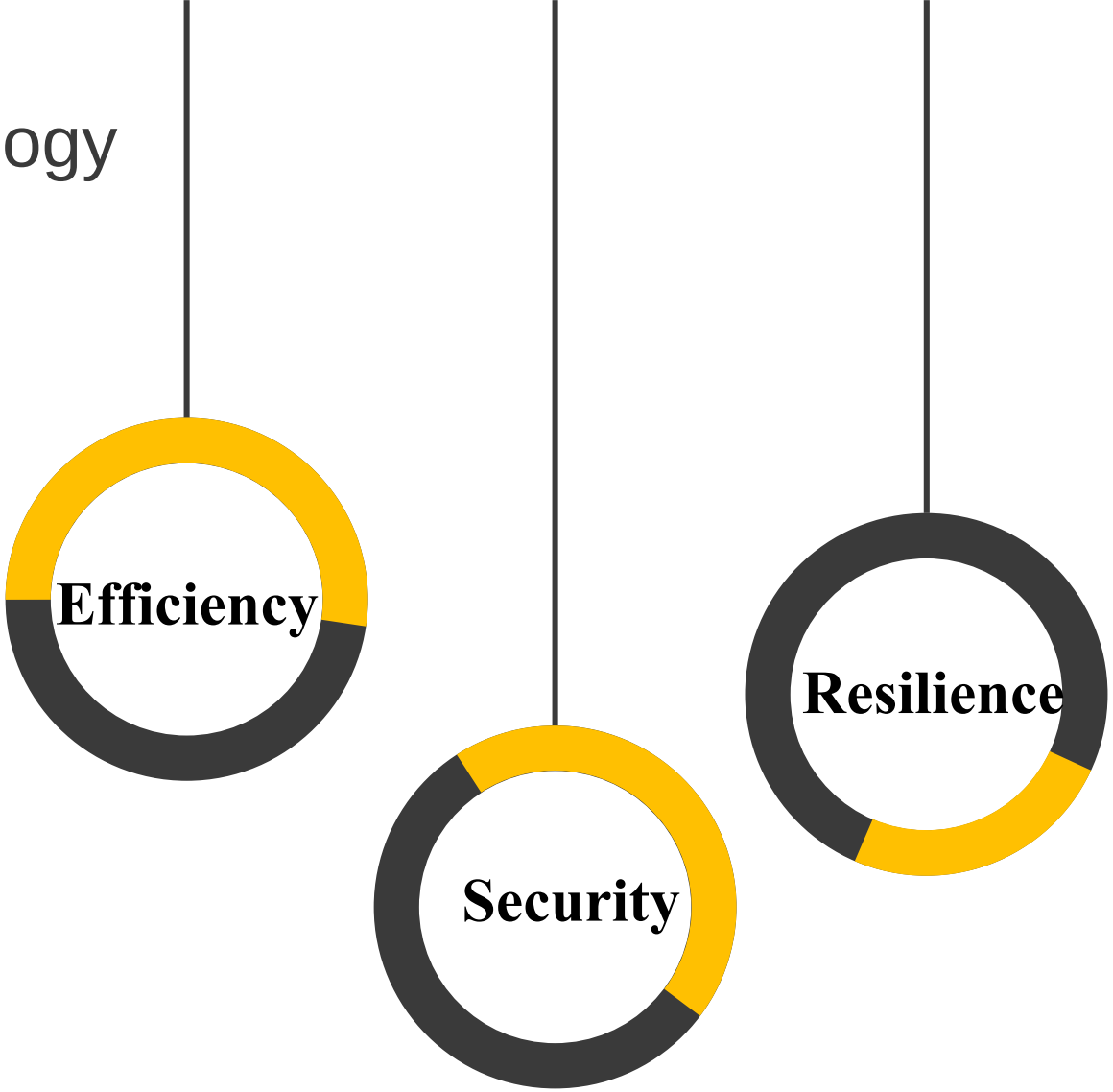
Disintermediation

Reduction of costs and complexity

Shared trusted transactions

Reduction of errors

Resilience, Secure, Auditability



Blockchain development

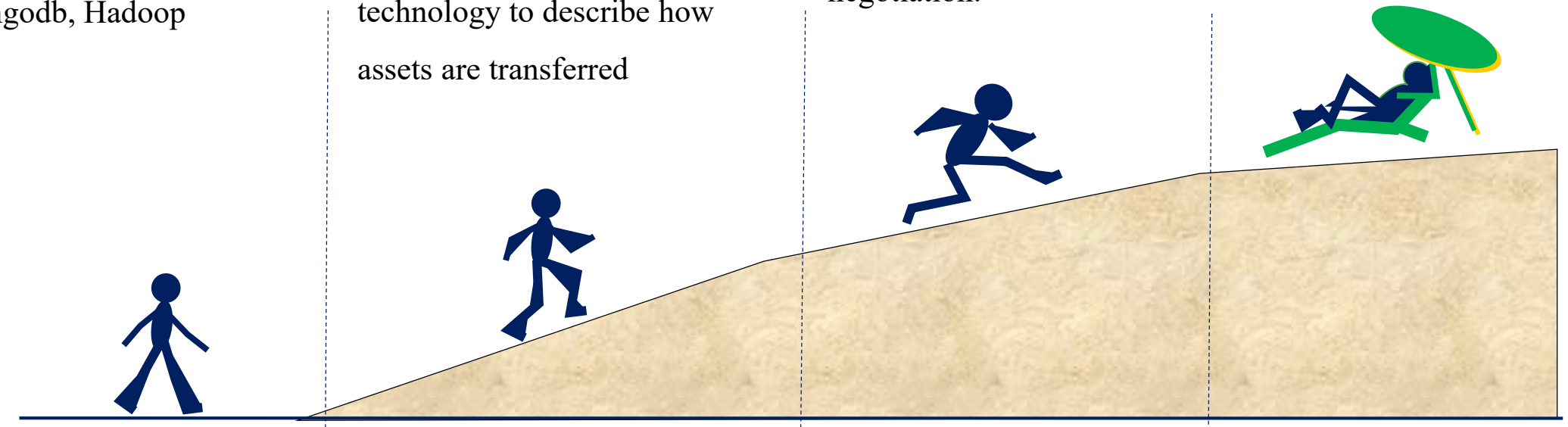
Decentralized systems: there have been many decentralized systems such as Mongodb, Hadoop

Currency: Bitcoin is used to mean the protocol that runs over the underlying blockchain technology to describe how assets are transferred

Smart Contracts: Smart contract are computer protocols that facilitate, verify, or enforce the negotiation.

Decentral applications: Smart Contracts ++

Filecoin IPFS



Pre-Blockchain | Blockchain 1.0 | Blockchain 2.0 | Blockchain 3.0

Future of Blockchain

Is blockchain going to be the next big disruptor for:

… information technology…

… the economy …

… the society …

… our lifestyle ?

Blockchain

THANK YOU !

Reference

1. En.wikipedia.org. (2017). Blockchain. [online] Available at: https://en.wikipedia.org/wiki/Blockchain [Accessed 11 Nov. 2017].
2. Yevgeniy Brikman. (2017). Bitcoin by analogy. [online] Available at: https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/ [Accessed 11 Nov. 2017].
3. Alex Biryukov, Dmitry Khovratovich and Ivan Pustogarov. 2014. "Deanonymisation Of Clients In Bitcoin P2P Network". 2014 ACM SIGSAC Conference On Computer And Communications Security, 15-29.
4. Androulaki, E., Cachin, C., Caro, A., Kind, A., Osborne, M. and Schubert, S. (2017). Cryptography and Protocols in Hyperledger Fabric. Real-World Cryptography Conference.
5. Seibold, S. and Samman, G. (2017). Cite a Website - Cite This For Me. [online] Bravenewcoin.com. Available at: https://bravenewcoin.com/assets/Industry-Reports-2016/kpmg-blockchain-consensus-mechanism.pdf [Accessed 11 Nov. 2017].
6. Chamberlin, B. and Juros, I. (2017). Blockchain Trend Report, 2017. Vertical Industries, MD&I bluemine.
7. Matsuo, S. (2017). Role of Academic Research (MIT). Fintech Summit.
8. Li, R. (2017). An academic certificate authentication using blockchain technology. Master. University of Birmingham.
9. Wu, Y. (2017). An e-voting system based on blockchain and ring signature. Master. University of Birmingham.
10. Chimera.labs.oreilly.com. (2017). Mastering Bitcoin. [online] Available at: http://chimera.labs.oreilly.com/books/1234000001802/ch07.html [Accessed 12 Nov. 2017].
11. En.wikipedia.org. (2017). Algorithm. [online] Available at: https://en.wikipedia.org/wiki/Algorithm [Accessed 15 Nov. 2017].
12. fintechblue. (2017). What is the difference between an algorithm and a protocol?. [online] Available at: http://www.fintechblue.com/2016/08/difference-algorithm-protocol-matter/ [Accessed 15 Nov. 2017].

Distributed Ledger Technologies – Landscape

Various DLTs and other providers are working together to meet market demand for a diverse set of applications and use cases across industries.

Industry consortiums

- Hyperledger
- Chinaledger
- R3CEV
- PTDL Group

Applications and use cases

- Trade finance
- Commercial paper trading
- Asset/security tracking (Provenance)
- Accounting & assurance
- Swaps reporting
- Record keeping
- Cross-border payments
- Digital identifies
- Document digitization
- Cryptocurrencies and tokenization
- Smart contracts
- Trade settlement

Consensus mechanisms

- Leader-based
- Proprietary distributed ledger consensus
- Federated consensus
- N2N
- Proof-of-work
- Proof-of-stake
- Delegated proof of stake
- Round robin
- PBFT and derivatives

Platform technologies/providers

Private/proprietary

- Digital asset
- Tendermint
- Casper
- NASDAQ (Linq)
- SETL
- Ripple
- Chain
- Intel (Sawtooth)
- Wave
- Juno

Private Consortium

- Corda (R3 CEV)
- Sentinel (Kynetix)

Open-source

- MultiChain
- Hyperledger

Open

- Ethereum
- Stellar
- PBFT
- Bitcoin
- Consensys
- Paxos
- Coinprism
- Symbiont

Infrastructure technologies/providers

Non-DLT/Traditional Infrastructure

- Public/private cloud – AWS, Azure, etc.
- *In-house systems/data centers*

DLT-specific Infrastructure

- IBM Bluemint
- Amazon Web Services
- MS Azure
- ETH BAAS

Sample implementations and tests we are seeing in the market