# Ring Signatures and Other Cryptographic Research Challenges in Blockchain

CUHK · 2018.8.31

Yuen Tsz Hon, John

# About Me

Yuen Tsz Hon (John)
阮子瀚

- Assistant Professor (2018 – present)
  - Department of Computer Science + Faculty of Economics
  - Research area: Fintech, cryptography

HUAWEI
(Singapore)

- Senior Researcher (2013 – 2018)

  Research area: blockchain, big data privacy, searchable encryption for database, identity-based authentication for 5G, etc. Published 14 papers including IEEE TC, ESORICS, and filed 6 patents.

- Post-doctoral Fellow (2010 – 2013)
  - Research on cryptography and security. Published 16 papers including Eurocrypt, ESORICS.

CityU
Senior Research Associate (2010)

UNIVERSITY OF WOLLONGONG
(Australia)
Ph.D. (2007-2010)

M.Phil. (2004-2006)
B.Eng. (2001-2004)

# Content

# Blockchain: The Trust Machine

- Blockchain: underlying technology of Bitcoin

"The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a **machine for creating trust**."

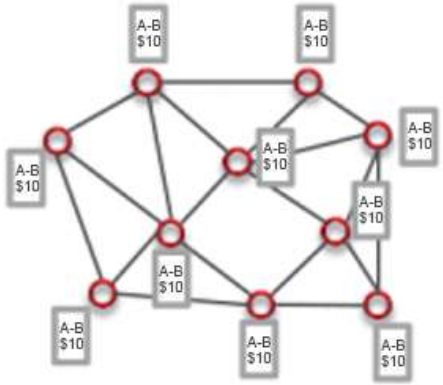
Economist, October 2015

# Why do we need Blockchain?

## Goal: Transfer value digitally without trusted third party

Problem:
Resolve conflicts

Distributed Ledger




- Single version of history
- Transparent
- Immutable
- Unforgeable (signature)

Blockchain

- Order transactions

Consensus

- Determine who can record

: Hash function

# Content

# Challenges of Using Blockchain in FinTech

## Business obstacles

**Cryptocurrency Bubble**

- Promising applications are overwhelmed by unrealistic projects due to speculative investments

**Auditing**

- Difficult to find out the real user identity under pseudonym

**Regulation**

- Lack of law for cryptocurrency, smart contract and Fintech use cases (e.g. ICO, P2P lending, etc.)

## Technical obstacles

**Efficiency**

- Bitcoin:7 transactions per second (tps)
- Most blockchain system: <10,000 tps
  - Cf. Visa with peak capacity 56,000 tps, Alibaba with max. 256,000 tps on 2017.11.11

**Privacy**

- Public transaction history → no privacy of transaction amount/address
- Use cryptography → Tradeoff between privacy and efficiency

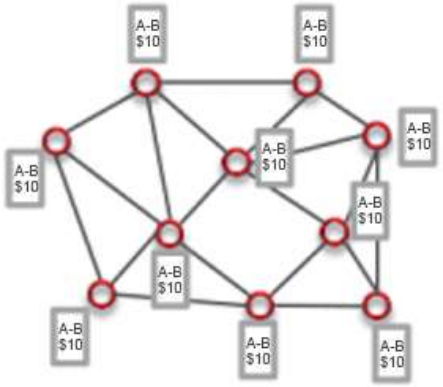
**Security**

- Software security of user's wallet and exchange
  - Major exchange Mt. Gox was bankrupted after USD$450M bitcoin was stolen

# Technical Challenge 1: Consensus

Problem:
Resolve conflicts

Distributed Ledger



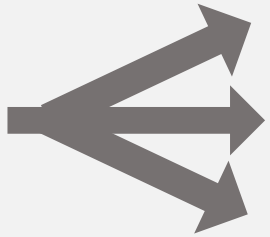

Blockchain

Consensus

- Determine who can record

Problem of Bitcoin's Consensus (Proof of Work):

- Low throughput (7 tps)
- High latency (10 minutes/block, 6 blocks for finality)
- Waste electricity



Theoretical breakthrough

Semi-trusted consensus nodes

Trusted hardware

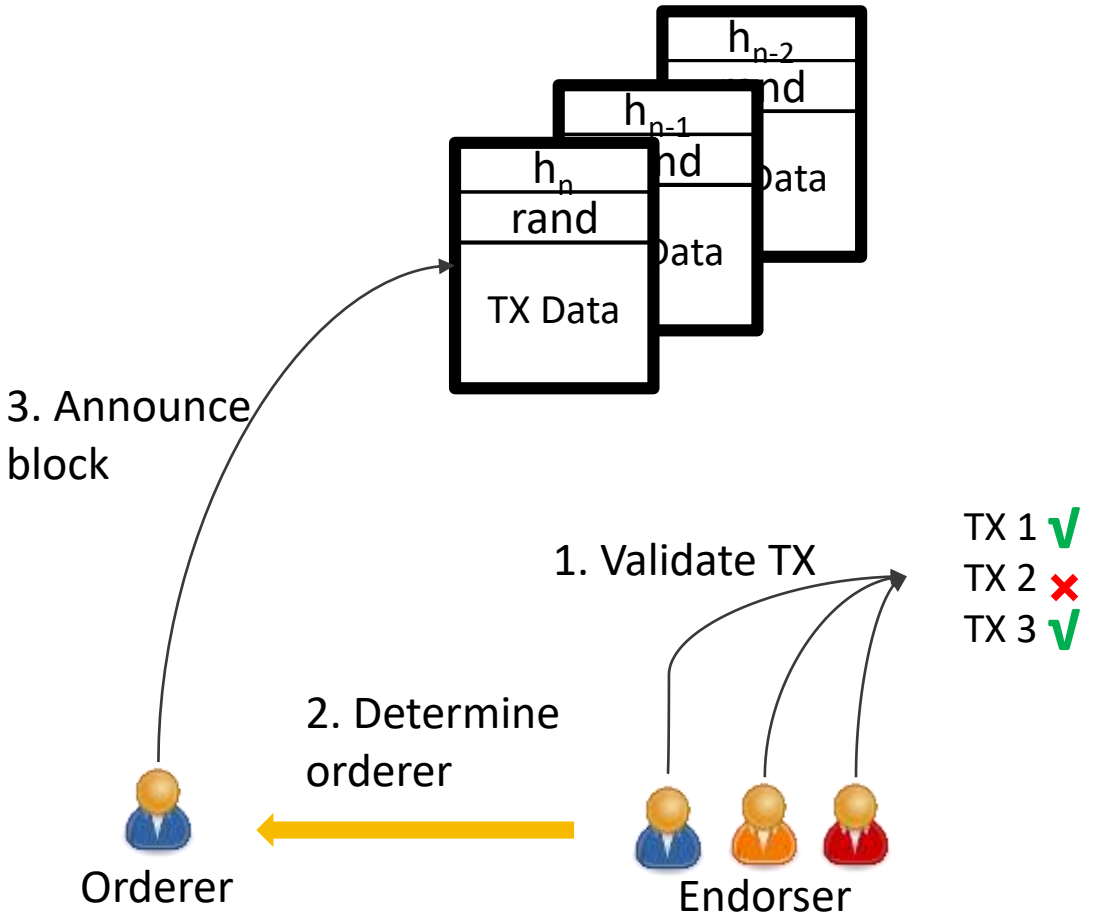
# Technical Challenge 1: Consensus (1)

**Theoretical breakthrough**: New consensus algorithms using cryptographic primitives, such as threshold signature, secret sharing, etc.

- Proof of Stake (PoS)
  - Creator of the next block is chosen via combinations of random selection and wealth (stake)
  - Used in various cryptocurrencies such as Ethereum

Active research area:

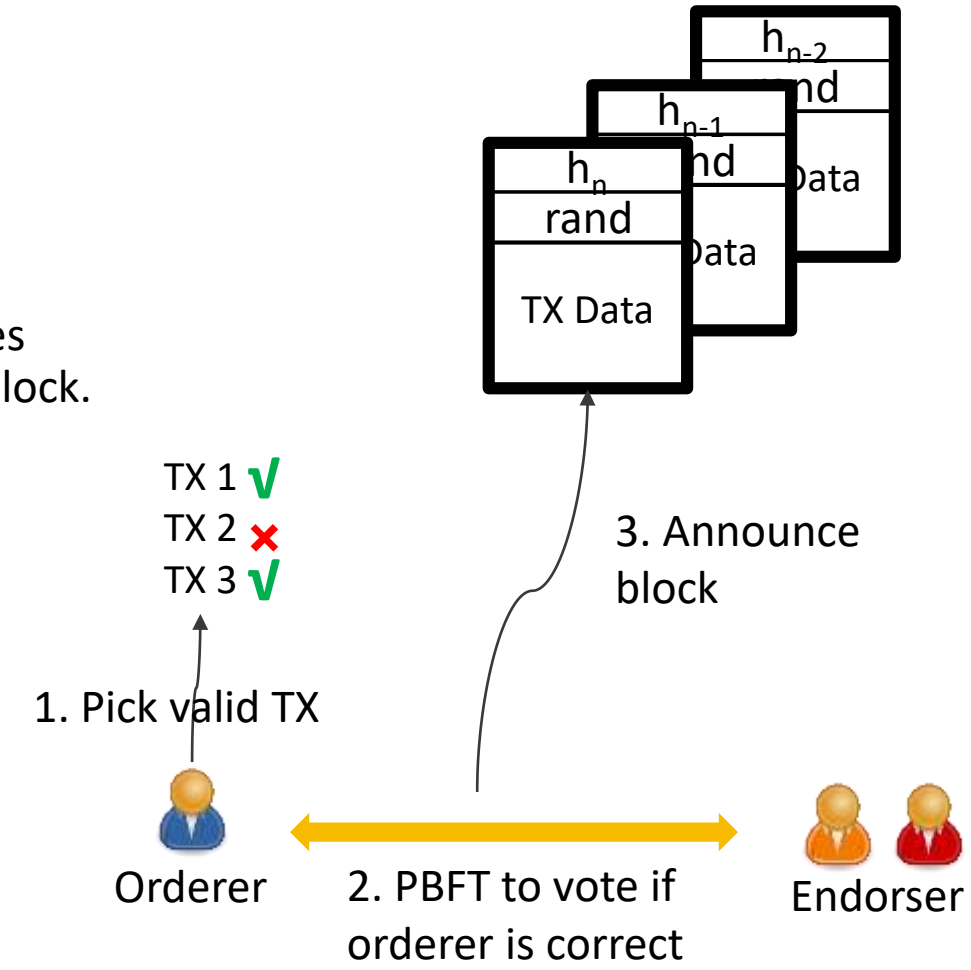
- Honey Badger (Miller et al. CCS 2016)
- Ouroboros (Kiayias et al. CRYPTO 2017)
  - used in Cardano (#5 cryptocurrency, USD$16 billion)
  - Ouroboros praos (Eurocrypt 2018), Ouroboro genesis
- Algorand (Micali et al. SOSP 2017), Algorand agreement
- Snow White (Pass, Shi. Asiacrypt 2017), Thunderella (Eurocrypt 2018)



# Technical Challenge 1: Consensus (2)

**Semi-trusted consensus nodes**: Assume consensus nodes are known and majority are honest, it can be reduced to Byzantine fault tolerance algorithm.

- Practical Byzantine Fault Tolerance (PBFT)
  - What is PBFT:
    - Achieve consensus if >2/3 nodes are not faulty
  - How to use PBFT in blockchain:
    - Nodes become orderer in round-robin. All nodes "vote" if they agree with the orderer's written block.
  - Advantages:
    - Efficient: Theoretically 10000+ tps
    - Well-studied algorithm
  - Disadvantages:
    - Unscalable: Only allows < 20 nodes
    - Nodes must be known to each other



# Technical Challenge 1: Consensus (2)

**Semi-trusted consensus nodes**: More suitable to Fintech applications

Consortium Blockchain:

- Blockchain with multi-authorities
- More realistic for Fintech applications
  - E.g. Clearing and settlement between banks
- Industrial alliances (e.g. R3, Hyperledger, Enterprise Ethereum Alliance) are formed

- PBFT-type consensus is suitable
  - Good for low-medium frequency trading (10,000 tps)
  - Daily transaction??
    - Visa with peak capacity 56,000 tps
    - Alibaba with 325,000 tps at peak on 2017.11.11

HYPERLEDGER

- Open source blockchain alliance to advance cross-industry collaboration

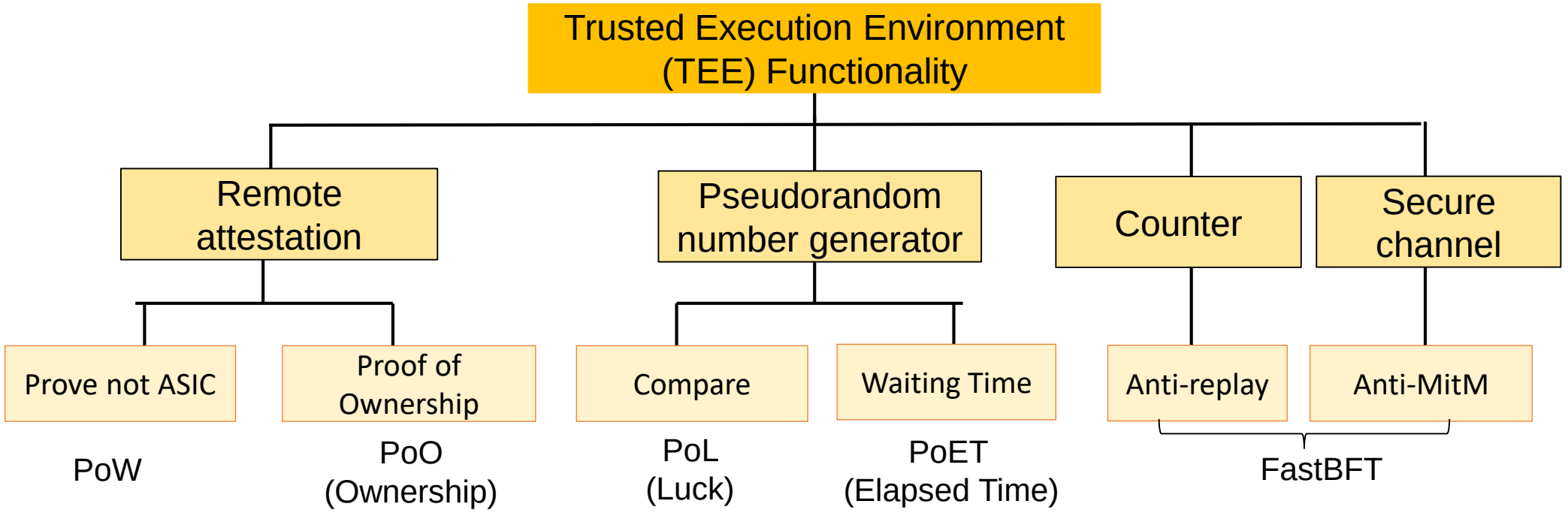
J.P.Morgan DTCC AMERICAN EXPRESS

SWIFT BANK OF ENGLAND

IBM intel Baidu 百度 HUAWEI

# Technical Challenge 1: Consensus (3)

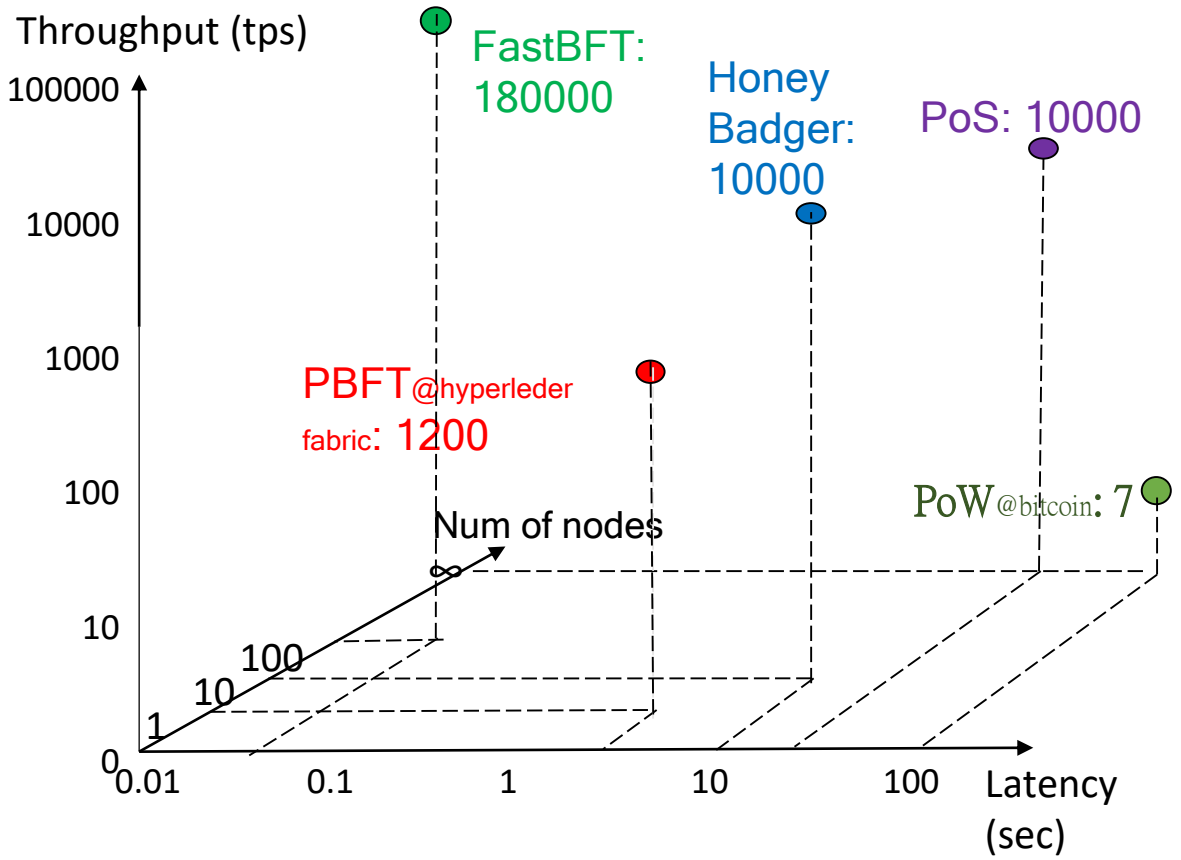
**Trusted hardware**: Most efficient solution based on strong security requirement

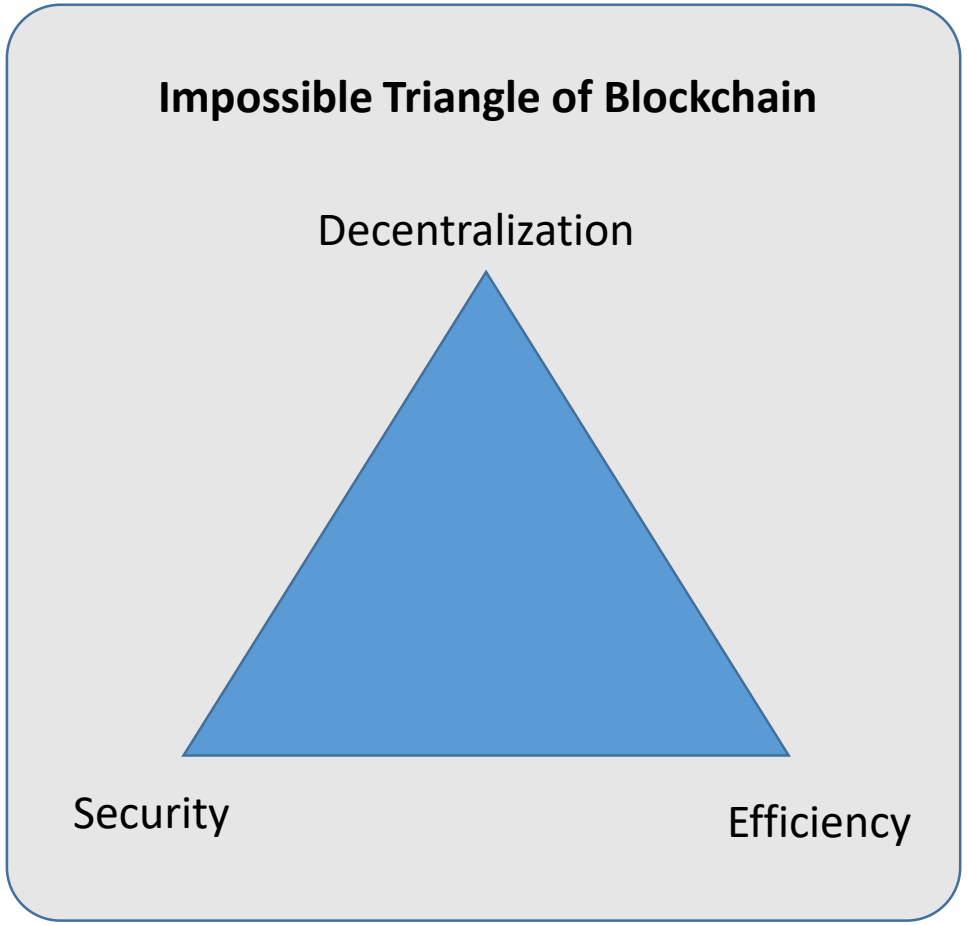



Hardware-based consensus algorithm is more concerned by the industry (e.g. Intel's PoET, NEC's FastBFT).

# Technical Challenge 1: Consensus Summary

➢Tradeoff:

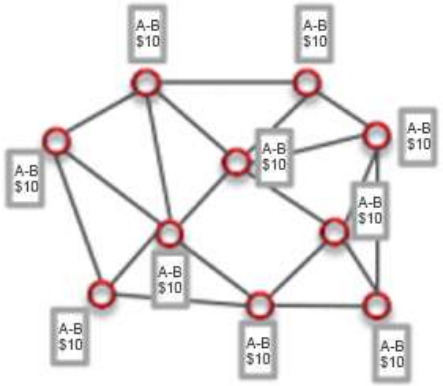


# Technical Challenge 2: Data Structure

Problem:
Resolve conflicts

Distributed Ledger




Blockchain

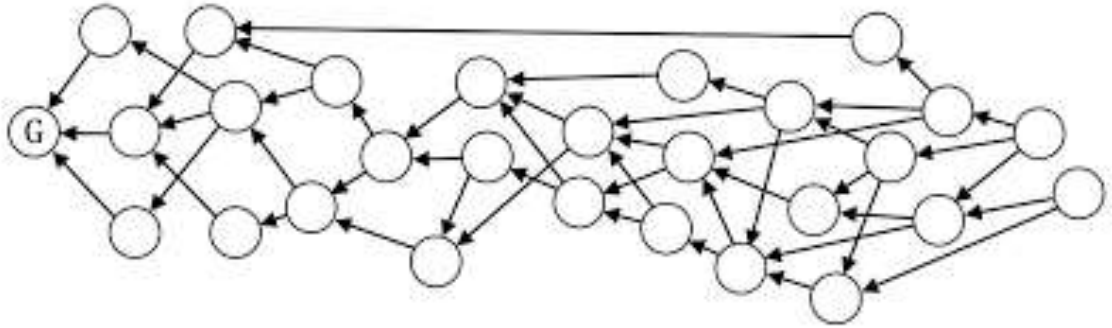
- Order transactions

Consensus

- Why do we need a chain of blocks? → In case of conflict, discard the second transaction
- Problem of “blockchain” data structure: no parallel computation → limited throughput

# Technical Challenge 2: Data Structure

**Directed acyclic graph (DAG)**




- DAG: Each transaction references two or more previous transactions → parallel transactions are possible
- Question: How to solve conflicts?

IOTA

IOTA:

- Support currency transaction only
- All nodes are weighted. Heavier branches are more likely to survive
- Markov Chain Monte Carlo is used to choose which branch to extend

Byteball

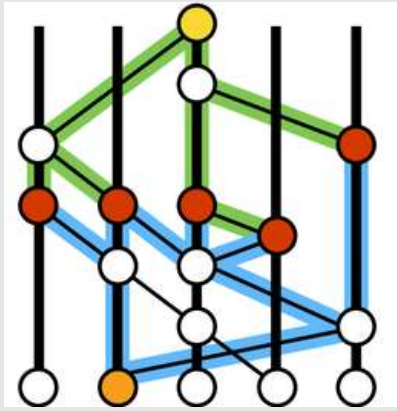
Byteball:

- Support smart contract
- Trusted *witness* is responsible to finalize certain blocks (chain-then-block)

Hedera Hashgraph

Hashgraph:

- DAG for permissioned blockchain

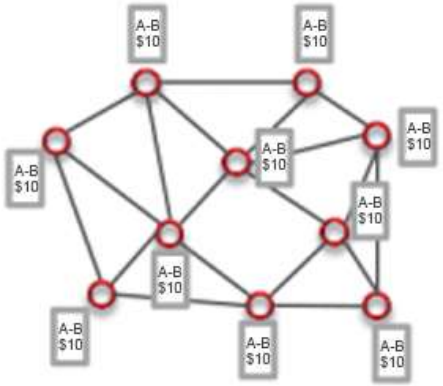


- Also Graphchain by boyen et. al. in BCC@AsiaCCS 2018

# Technical Challenge 3: Privacy

Problem:
Resolve conflicts

Distributed Ledger




- Single version of history
- Immutable
- Transparent
- Unforgeable (signature)

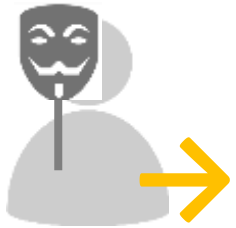
Blockchain

Consensus

- Transparency is good for some use cases, e.g. supply chain management
- Transparency is not desirable for sensitive information, e.g. transaction details between two banks should not be known to other banks

# Technical Challenge 3: Privacy

3 Types of Privacy:



Sender anonymity


Confidential transaction

Recipient anonymity

Zcash (#26)

- Use zero knowledge proof of circuit “zk-SNARK” to achieve all 3 types of privacy
- Based on IEEE SP 2014 paper

√ Can be extended to zk-smart contract (IEEE SP 2016)

× 1. Prove time = 30 sec.
2. Require trusted setup

Monero (#13)

- Sender anonymity: linkable ring signature
- Recipient anonymity: Diffie-Hellman key exchange
- Confidential transaction: Pederson commitment

√ Quite Practical

× Not scalable for sender anonymity

Dash (#12)

- Mixing a few transactions’ input and output together, using homomorphic encryption

√ Practical

× Limited anonymity

# Technical Challenge 3: Privacy

**Privacy**: Popular among both researchers and practitioners

Zero-knowledge proof approach:

- zk-SNARK is implemented on top of Ethereum (#2) and JP Morgan's Quorum platform
- Very active research area, 10+ papers in top conferences since 2014

Coin-shuffling approach:

- Improved in applications, such as SharedCoins, Dark Wallet.
- CoinShuffle paper in ESORICS 2014, works for bitcoin

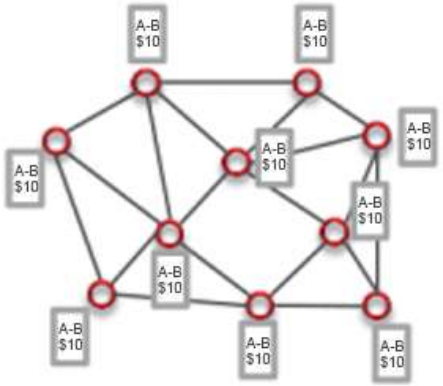
Linkable Ring Signature + Confidential Transaction approach:

- Confidential transaction is used by top startups such as Blockstream and Chain.com
- RuffCT is proposed by Monero developers to improve the scalability of linkable ring signature

# Technical Challenge 4: Sharding

Problem:
Resolve conflicts

Distributed Ledger




- Single version of history
- Immutable
- Transparent
- Unforgeable (signature)

Blockchain

Consensus

- Sharding is a common technique in database. It improves the throughput of blockchain system
  - Network and Transaction Sharding: Each subgroup of nodes reach consensus on a subset of transactions in parallel, but every node will need to store all the data. (e.g., Zilliqa, CCS 2016)
  - State sharding: State data is split and stored on different shards separately. Before the sharding group is re-organized, data exchanges must be done in advance. (e.g. Ethereum 2.0)

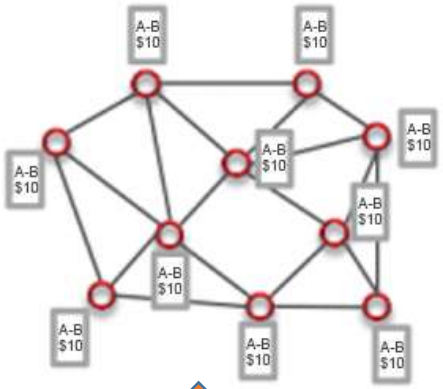
# Technical Challenge 5: Layer 2-solution

Problem:
Resolve conflicts

Distributed Ledger

Blockchain

Consensus

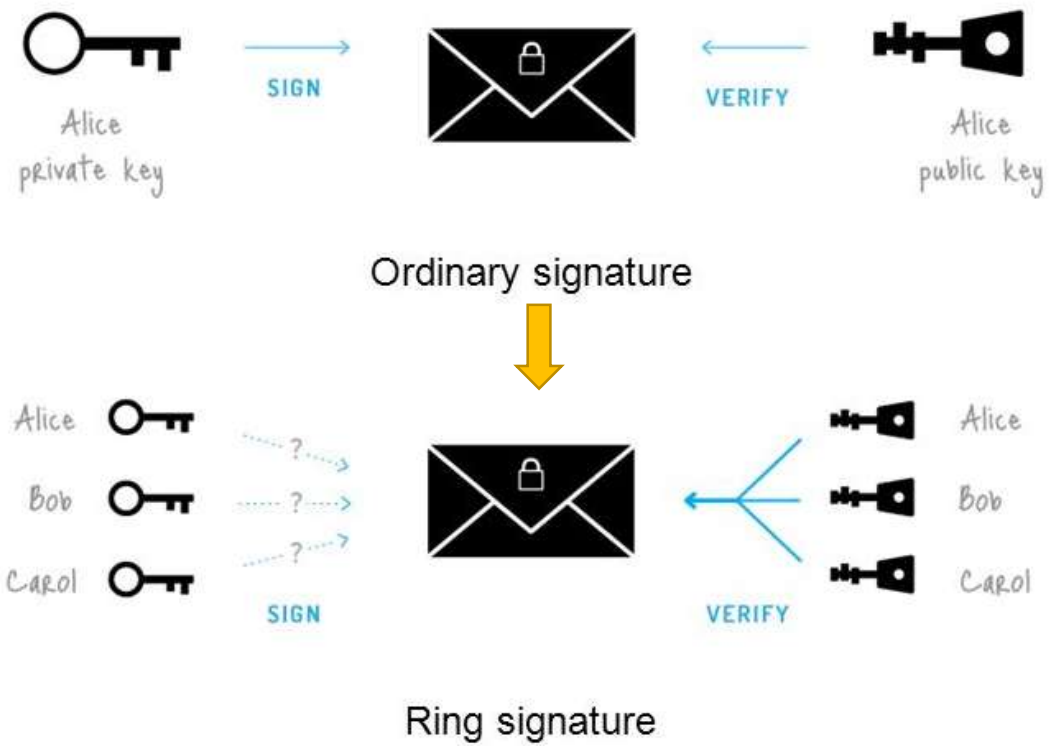



Layer 2-solution: Handling transaction off main chain

- Lightning network: increasing transaction throughput and confirmation speed of bitcoin network. Submit a fraud proof against the malicious side to the main chain so as to confiscate his deposit as a penalty.
- State channel: a more general 2 party off-chain channel which manages the states of smart contract
- Plasma: multiple parties can participate and the confirmation time of a transaction depends on when the plasma block header is submitted to the plasma contract on the parent blockchain.
- Truebit, Plasma cash, etc…

# Content

# Ring Signatures for Blockchain Privacy

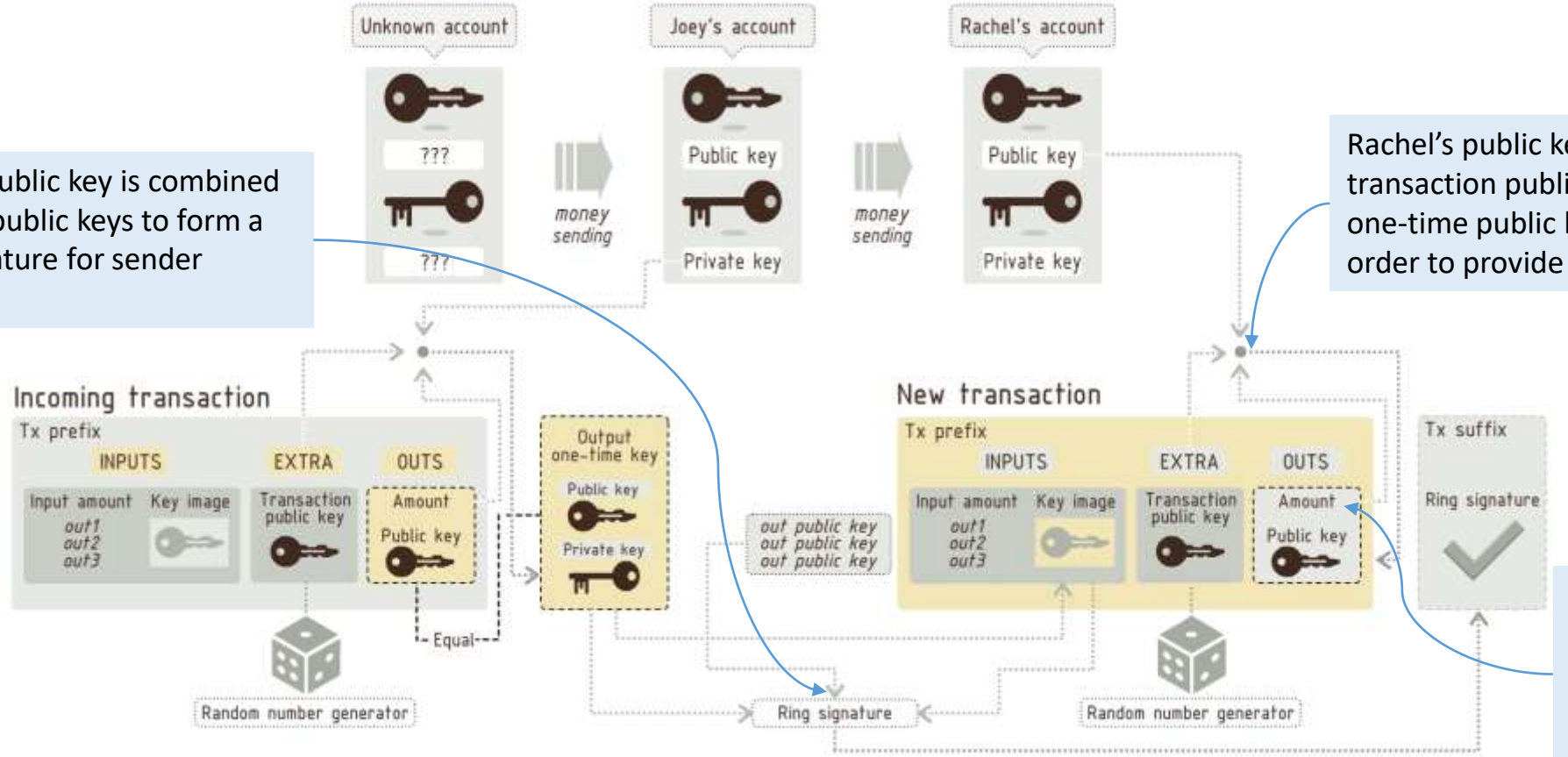



Linkable Ring Signature:

- Detect signer that sign twice → used to detect double spending in blockchain

# Ring Signatures for Blockchain Privacy

Confidential Transactions in Monero: Joey receives money from some unknown account (left hand side) and sends it to Rachel (right hand side).




Joey's one-time public key is combined with 3 other out public keys to form a linkable ring signature for sender anonymity.

Rachel's public key is combined with transaction public key to form the output one-time public key (stealth address), in order to provide recipient privacy.

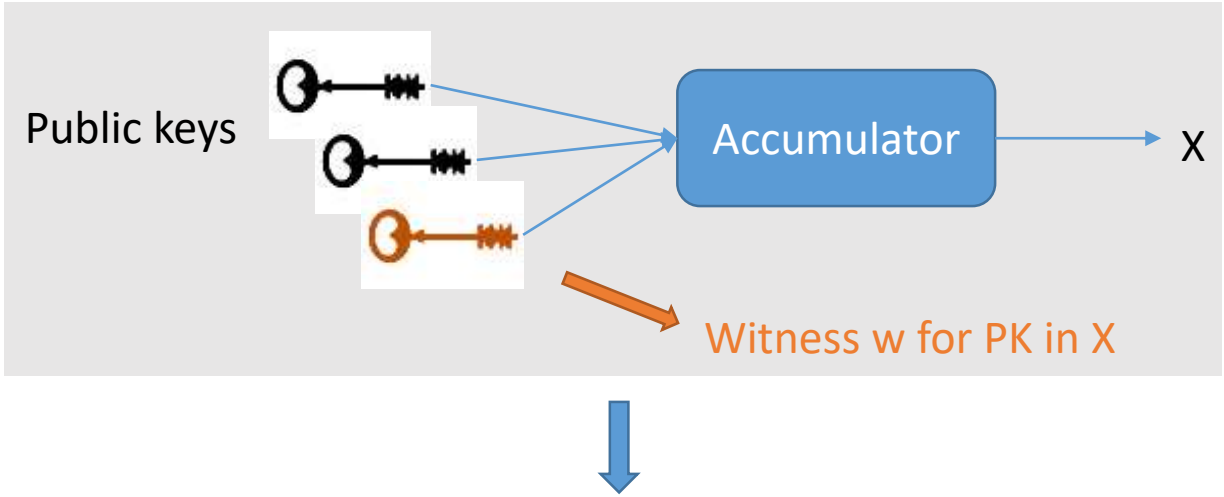
Transaction privacy can be achieved by computing additive homomorphic commitment on the input and output amount.

Monero's limitation:

- Signature size is O(n), where n = number of public keys (PKs) to "hide" the signer → not scalable

# RingCT 2.0

- RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero. Shi-Feng Sun, Man Ho Au, Joseph K. Liu, Tsz Hon Yuen. ESORICS 2017.




Linkable Ring Signatures:

PoK{ (SK, PK, w) : SK is the secret key of PK
and w is a witness for PK in X
and Key-Image = F(SK) }

Challenge:

- RingCT protocol is essentially a multi-ring signature scheme
  - If the transaction has 3 inputs, it has a ring signature for each input
  - Hence it requires the same user index for these 3 inputs simultaneously to ensure correctness
- Accumulator does not consider order of the value stored in it
  - Classical ring signature has user' order

Our solution:

- Add user index to the public keys before accumulating it

Advantage: constant proof size due to the use of accumulator
Disadvantage: trusted setup in accumulator

# News about our ESORICS 2017 publication:

kryptomoney August 22, 2017 Crypto Currency, Latest Posts 0

## Monero: Cryptocurrency for True Anonymity

Monero was recently in top gainers in the cryptocurrency world, almost doubling from $50 to $100 within the last couple of hours and then settling at around $80. The current surge can be attributed to two major developments in the last month. First, Monero is rumoured to be listed on Bithumb, South Korea's largest bitcoin exchange starting August 23. Second, contributions from the Monero development team in the technical whitepaper, titled **"RingCT 2.0: A Compact Linkable Ring Signature Based Protocol for Blockchain Cryptocurrency Monero"** by Sun et al which is set to be presented at ESORICS 2017.

# BulletRingCT

- Current work: RingCT from the Bulletproof framework

BulletRingCT idea:

- Vector commitment $C = h^r y_1^{b_1} y_2^{b_2} \dots y_n^{b_1}$
- If $(y_1, y_2,\dots, y_n)$ are public keys and $\overrightarrow{b_L} = (b_1, b_2,\dots, b_n)$ is a binary vector of Hamming weight 1, then the commitment C is a commitment to one public key

Bulletproof framework:

- ZK proof for inner product relation
  $\langle \vec{a}, \vec{b} \rangle$ = x
- Proof size is log $|\vec{a}|$
- No trusted setup

- Define $\overrightarrow{b_R} = \vec{1}$ - $\overrightarrow{b_L}$
- $\overrightarrow{b_L} = (b_1, b_2,\dots, b_n)$ is a binary vector of Hamming weight 1 can be shown as:
  $\overrightarrow{b_L} \circ \overrightarrow{b_R} = \vec{0}$, $\overrightarrow{b_R} = \vec{1}$ - $\overrightarrow{b_L}$, $\langle \overrightarrow{b_L}, \vec{1} \rangle = 1$
- We can use Bulletproof for showing inner product with log-size proof!
  - Caution: Bulletproof requires that the DL of $y_1, y_2,\dots, y_n$ are unknown in the security proof.
    - No problem for ring signature
    - Cannot go through the security model of linkable ring signatures! So we have to hash function to formulate the public key set as well.

# BulletRingCT

## Signature Size

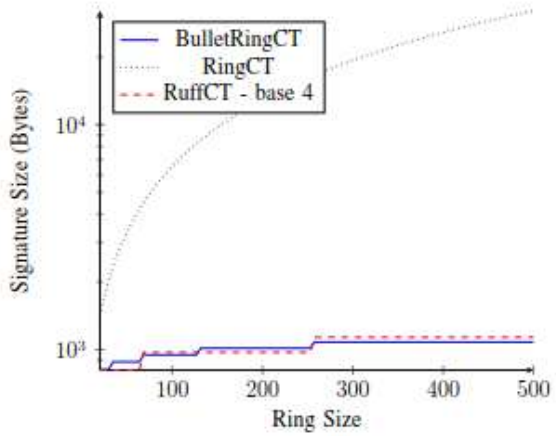



Fig. 2. Comparison of BulletRingCT, RuffCT and RingCT for a transaction with 2 inputs, with small ring size.

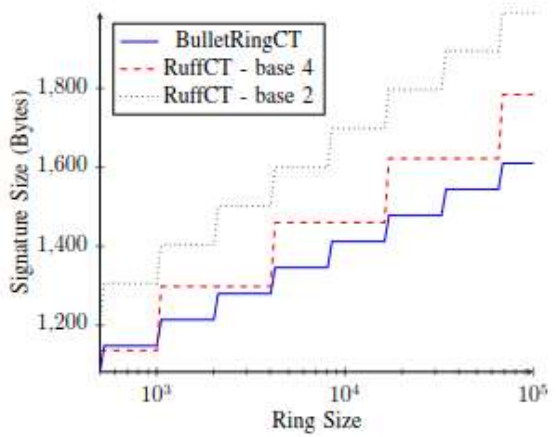



Fig. 3. Comparison of BulletRingCT and RuffCT for a transaction with 2 inputs, with large ring size.

## Running Time

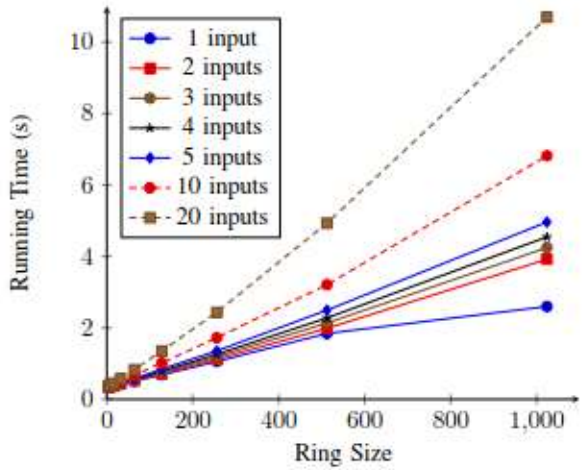



Fig. 4. Running Time of Spend in BulletRingCT.

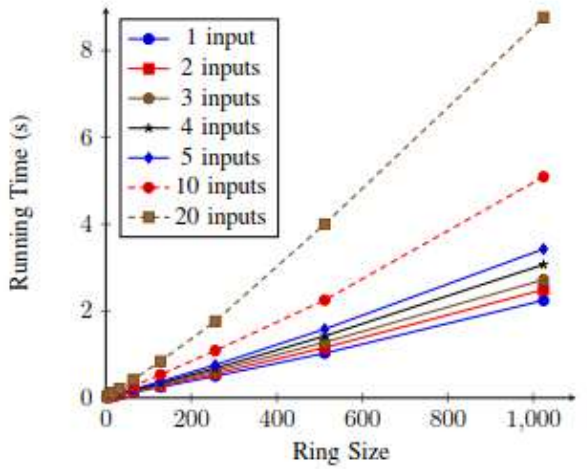



Fig. 5. Running Time of Verify in BulletRingCT.

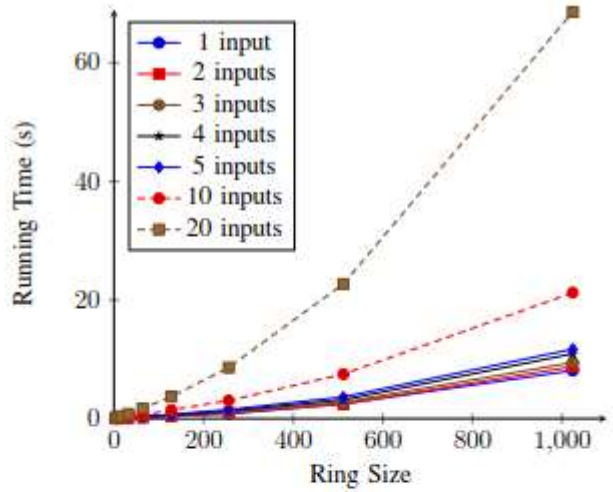



Fig. 6. Running Time of Spend in RuffCT.

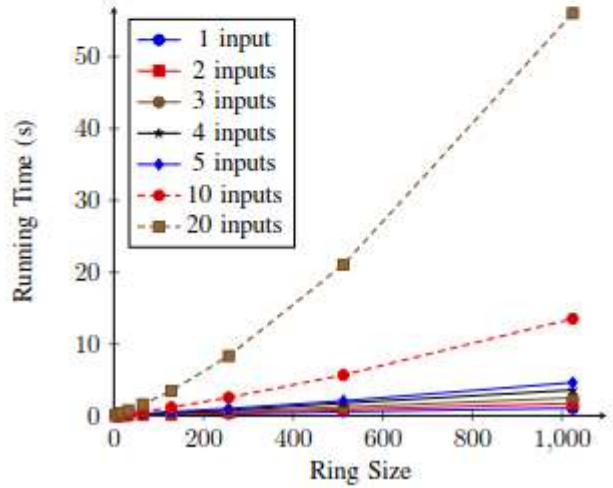
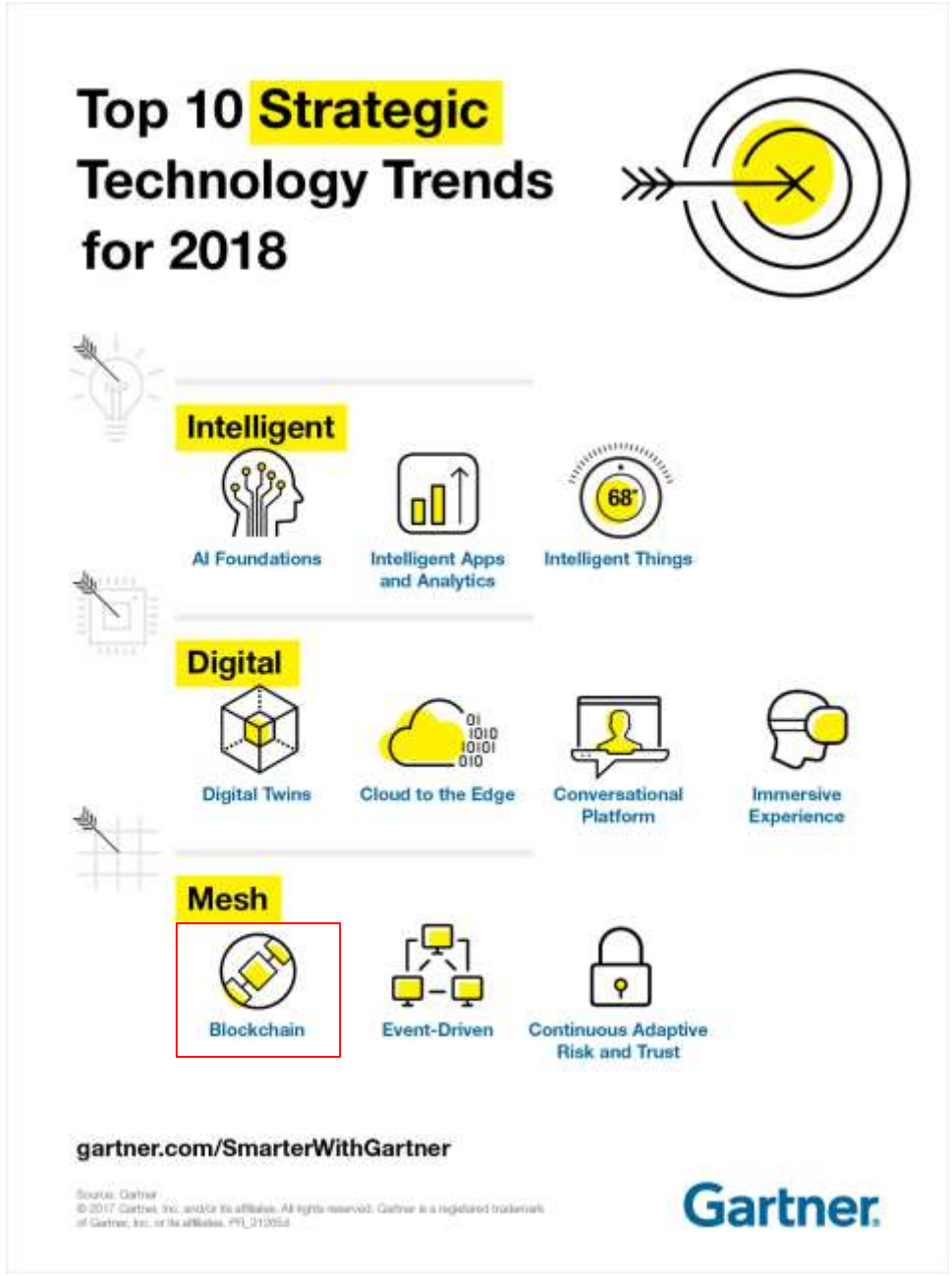



Fig. 7. Running Time of Verify in RuffCT.

# Conclusion

- Blockchain is a promising technology, especially for the finance industry.
  - Other killer applications to be determined
- Many active research areas:
  - Short term: Consensus, privacy
  - Medium-Long term: DAG data structure, inter-chain transactions, smart contract security, sharding, layer 2, cryptoeconomics…
- Ring signature is one important tools for privacy in blockchain applications.


Top 10 Strategic Technology Trends for 2018
Intelligent
AI Foundations
Intelligent Apps and Analytics
68°
Intelligent Things
Digital
Digital Twins
Cloud to the Edge
Conversational Platform
Immersive Experience
Mesh
Blockchain
Event-Driven
Continuous Adaptive Risk and Trust
gartner.com/SmarterWithGartner
Gartner

# THANK YOU