Fun with Blockchain Research

Kotaro Kataoka
Associate Professor
Indian Institute of Technology Hyderabad

Blockchain as Tamper-Resistant Distributed Ledger

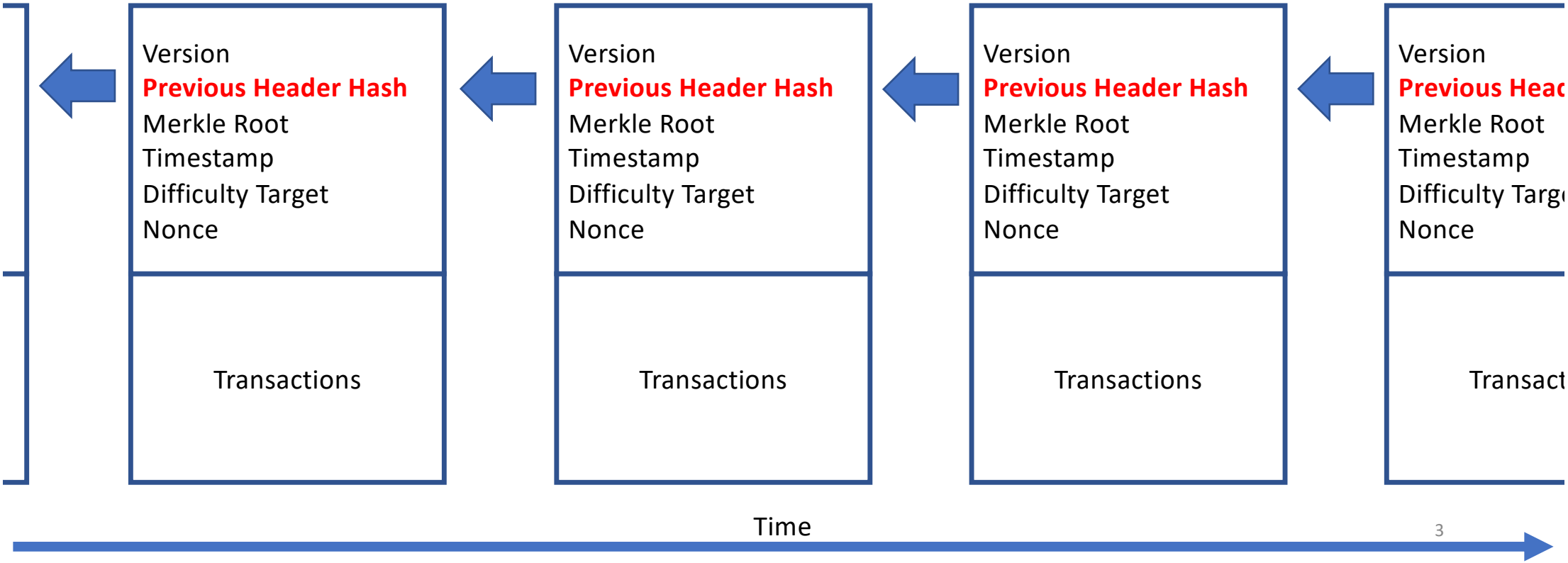
- Cryptocurrency: Bitcoin, Ethereum, etc.
- SmartContract: Sending/receiving/recording statements rather than coin

- Bitcoin Components
  - A decentralized peer-to-peer network (the bitcoin protocol)
  - A public transaction ledger (the blockchain)
  - A set of rules for independent transaction validation and currency issuance (consensus rules)
  - A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)

Source: Bitcoinbook http://bitcoinbook.info

How does Blockchain look like?

- A linked list using ”Previous Block Hash” as a pointer

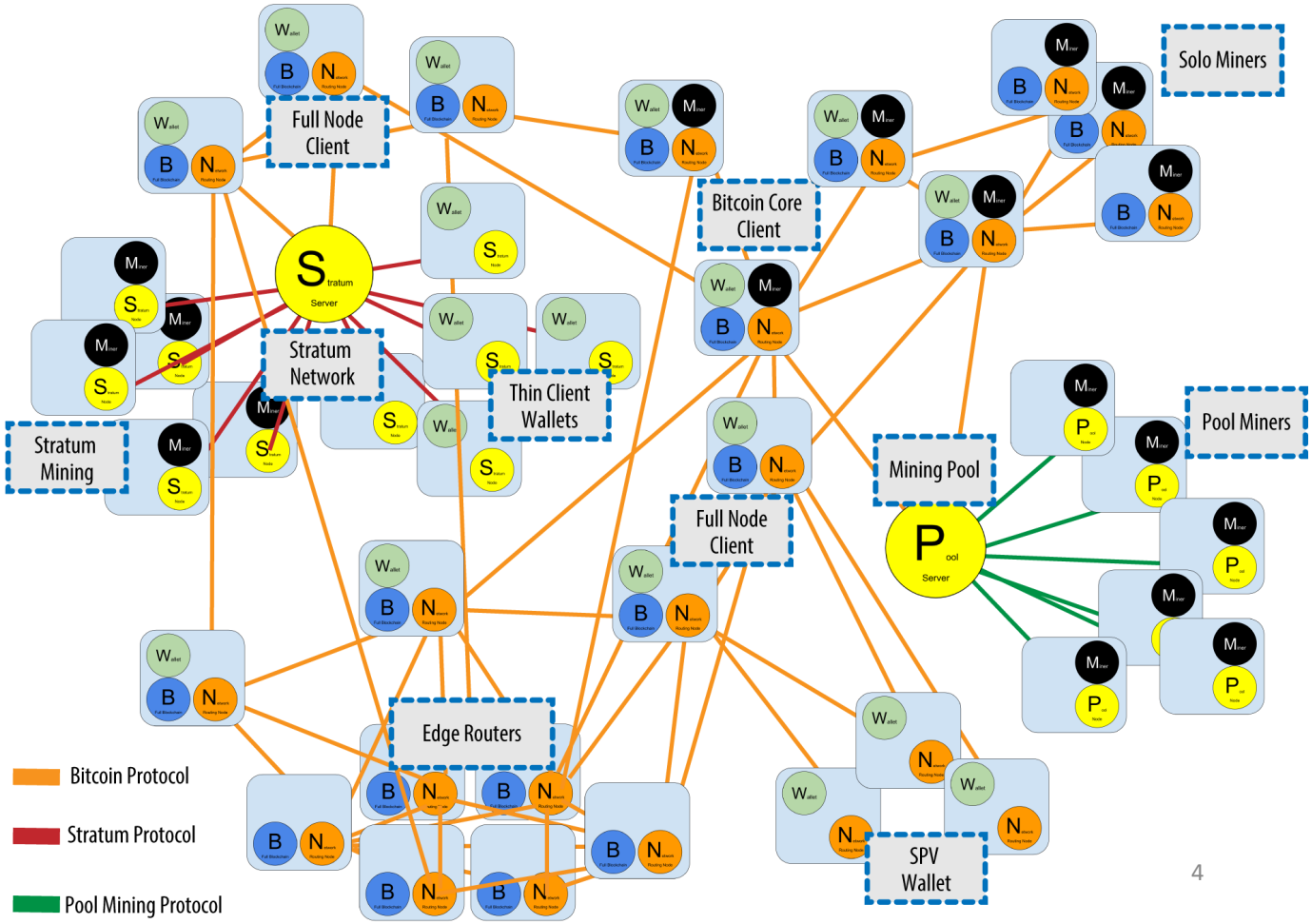


Stakeholders in Bitcoin Blockchain

- Bitcoin Core Clients
- Full Node Clients
- Edge Routers

- Solo Miners
- Pool/Stratum Miners

- SPV Wallets
- Thin Client Wallets



Source: Bitcoinbook http://bitcoinbook.info

Blockchain as a Distributed Ledger

- Extremely-Difficult-To-Tamper
  - Full Nodes in Blockchain maintain the replica of the entire Blockchain
  - To tamper (alter) the ledger, the attacker needs to successfully alter the blockchain on more than 50% (reportedly even less) of nodes
- Root of Trust
  - No central trusted root
  - Genesis Block and Blockchain itself built using “Strong” Consensus Algorithm
- Takes long time to form a history
  - Approx. 10 mins (in the case of Bitcoin) till a new block is added to the blockchain
  - 3 (95%) to 6 (99.7%) blocks to be added to confirm the block in the blockchain

Source: Bitcoinbook http://bitcoinbook.info

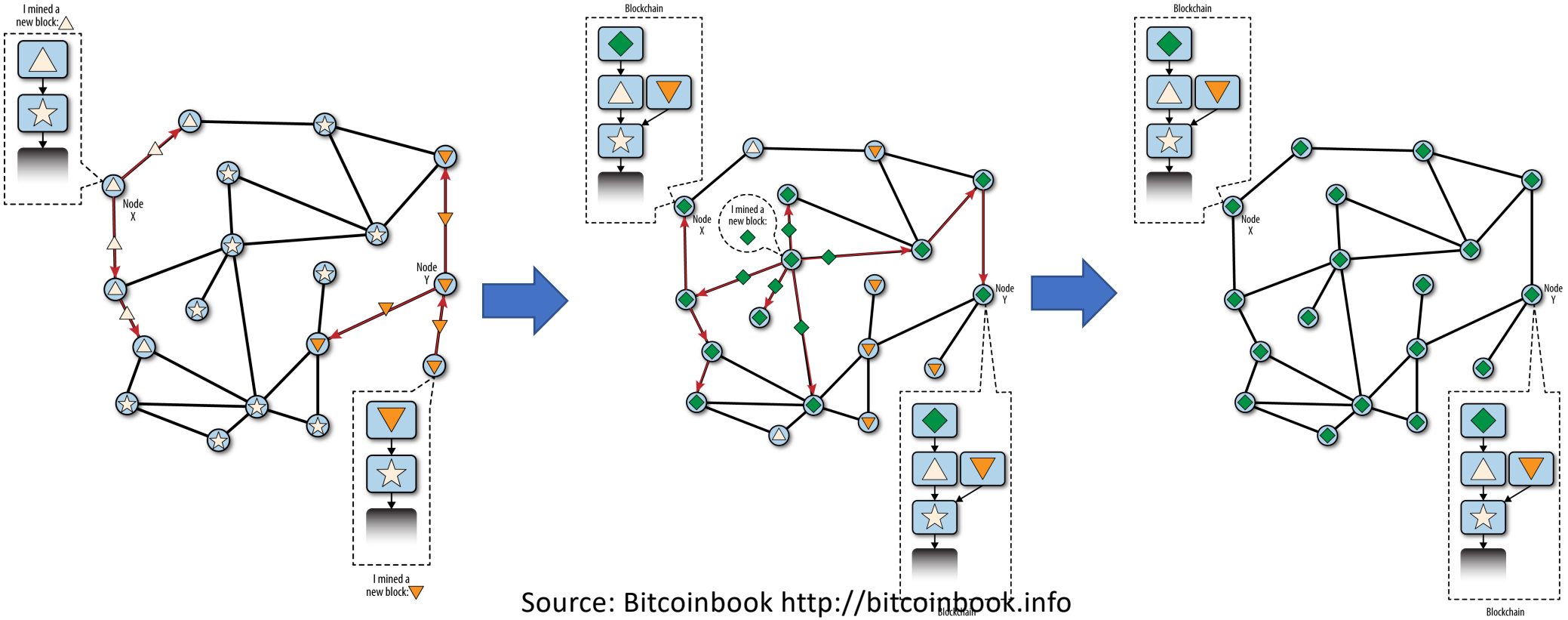
One-to-all-the-others Data Delivery in Bitcoin

- Unspent Transaction Output (UTXO) and block information should reach the stakeholder of minors, full nodes, etc.

- Bitcoin Peer Selection is random using “DNS Seed” providing the IP addresses of bitcoin nodes

Fork and Longest Chain in Blockchain

- Multiple miners may create a block at the same time



Source: Bitcoinbook http://bitcoinbook.info

Longest chain survives

- Soft Fork
  - Not Hard Fork, Software Fork

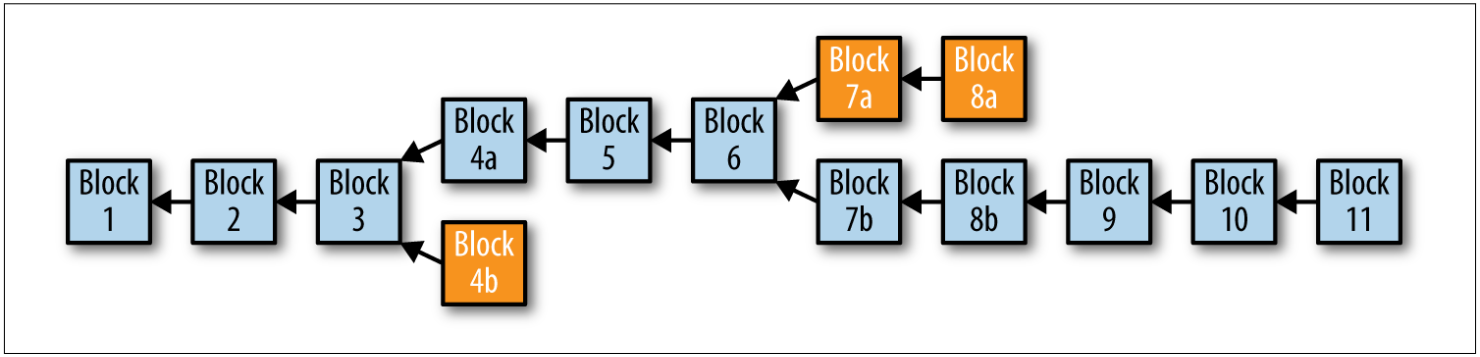


Figure 10-9. A blockchain with forks

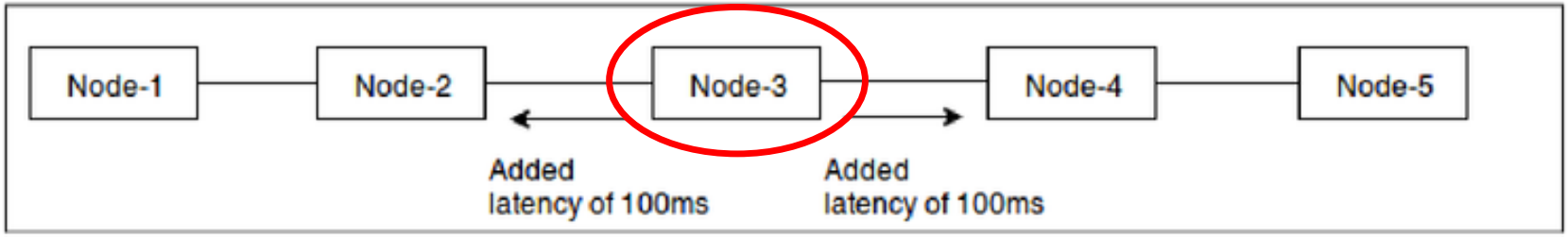
- Even through multiple blocks are successfully mined at the same tome, only one is taken. The others will be wasted.

What are the matters from the networking point of view?

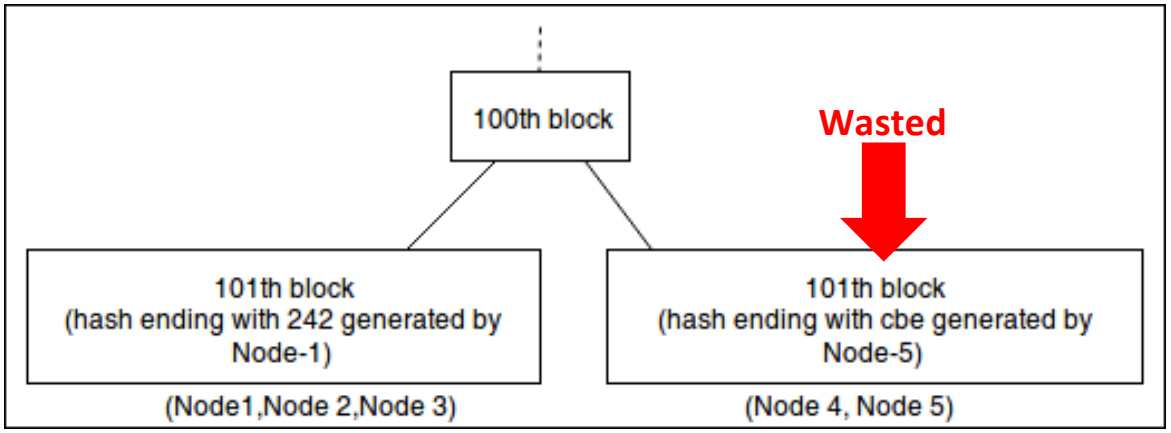
- Transaction throughput
  - The number of transactions per second that are appended to the blockchain in the form of valid blocks
- Stale Block Rate
  - The percentage of the blocks that are wasted in the forking over the total blocks generated in the network
- Mean Propagation Delay
  - The average time taken for a block to propagate in the whole network reaching every node

Impact of Peer Selection causing “Fork” (1/2)

- One “slow” node in the middle of P2P network

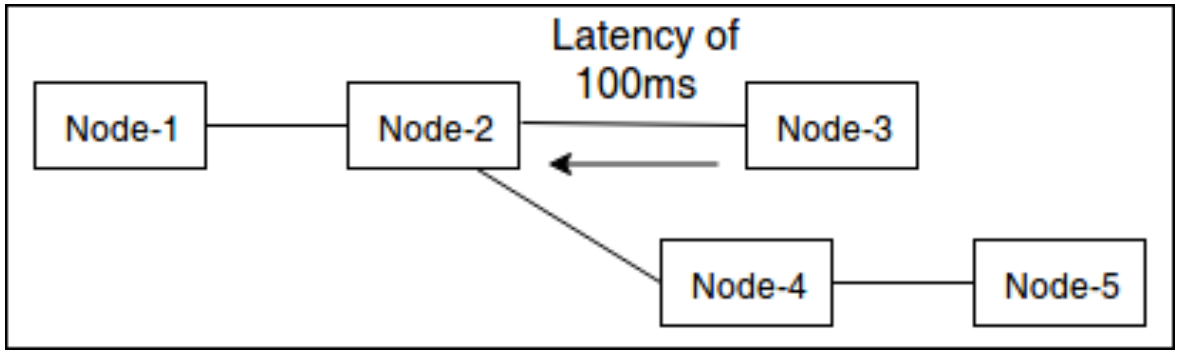


- Increases probability of Fork
- Block and B/W are wasted



Impact of Peer Selection causing “Fork” (2/2)

- One slow node at the edge of P2P network



- Slow node in the middle: 45 Blocks wasted
- Slow node at the edge: 5 Blocks wasted

Question and Challenges

- What's the potential betterment for P2P networking for one-to-all-the-others data delivery?

- Existing P2P networking techniques don't help
  - "Cache Hit Ratio" doesn't help
  - Randomness of Bitcoin's peer selection approach

The techniques explored till now

- Considering Latency and Bandwidth among Peers
- Use Greedy algorithm to select best peers
- Sounds it works

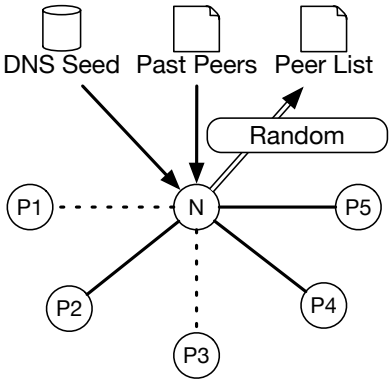


Fig. 1: Random Peer Selection

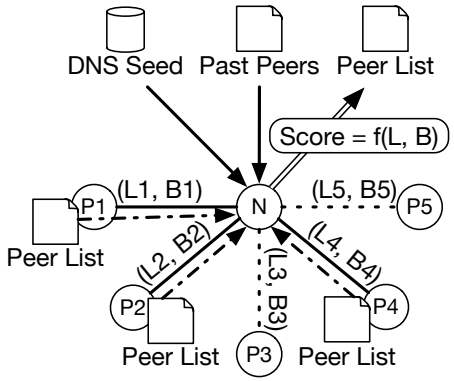


Fig. 2: Proposed Peer Selection

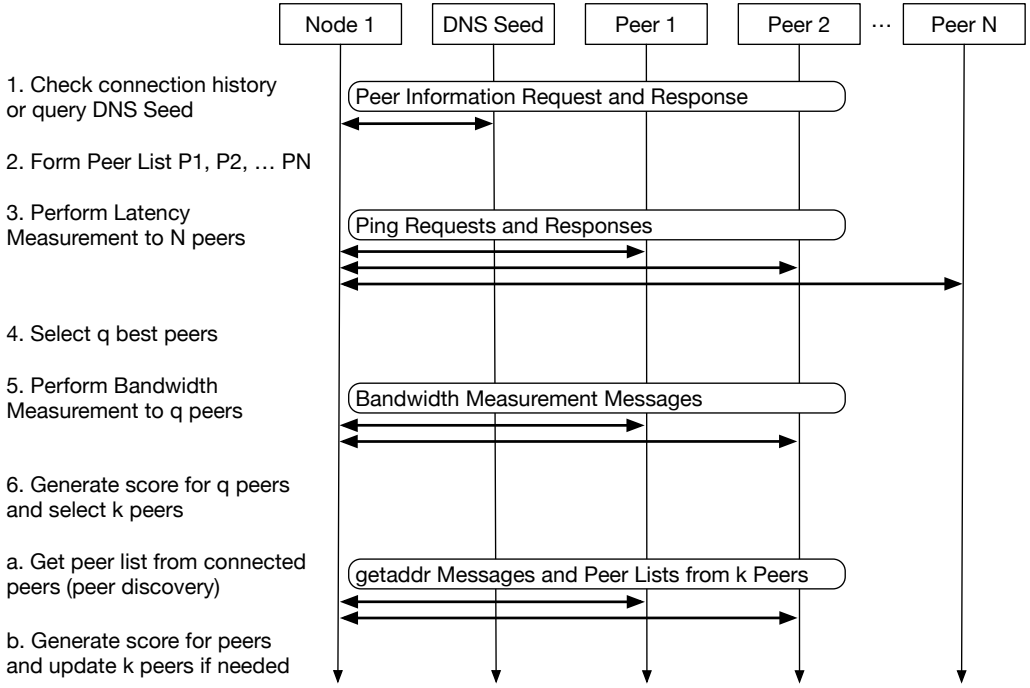


Fig. 2: Working of Proposed Approach in Bitcoin Network

Discussions and Intermediate Conclusion

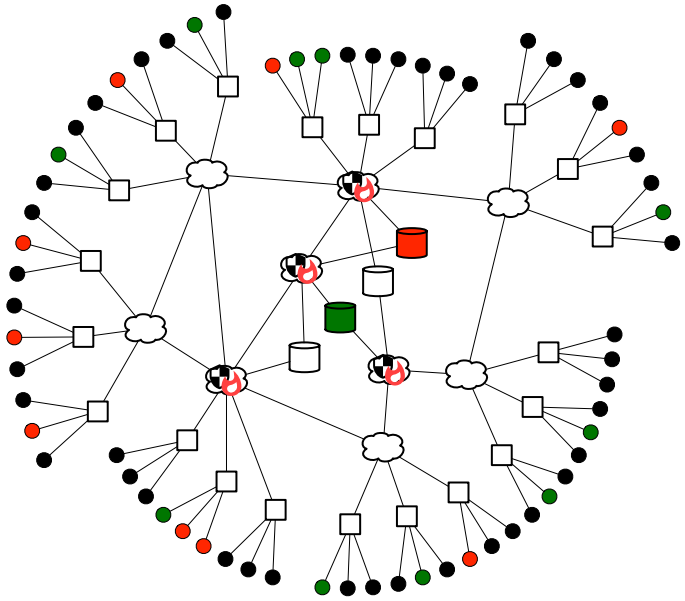
- Adjustment of DNS Seed will decrease “nature of randomness” of peer selection. What are potential side-effects?
- Achieving shorter propagation delay introduces significant benefit
  - Less network resource consumption
  - Less chances of fork in blockchain
  - Higher throughput
- Designing a protocol and figure out the convergence time
- Applicable to other blockchains that uses one-to-all-the-others data delivery

Other Blockchain Topics

Exposing some experiences of working abroad

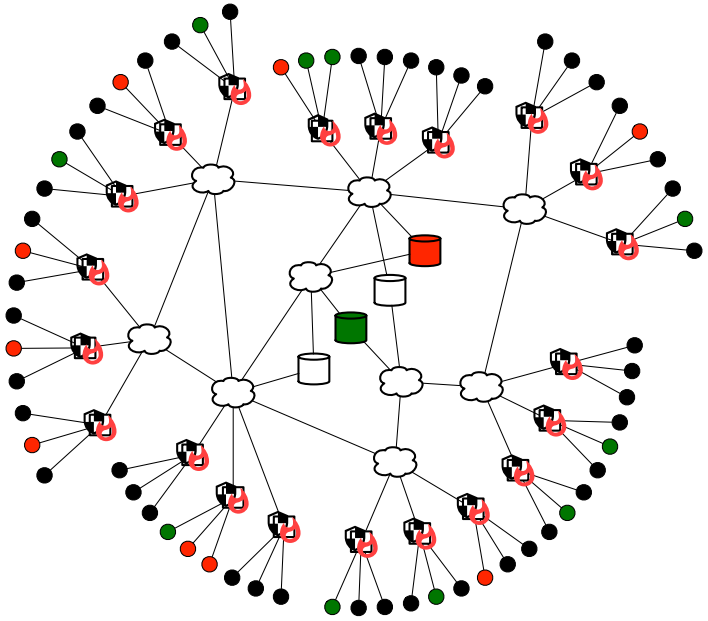
Trust List: Internet-wide and Distributed IoT Traffic Management using Blockchain and SDN (1/3)

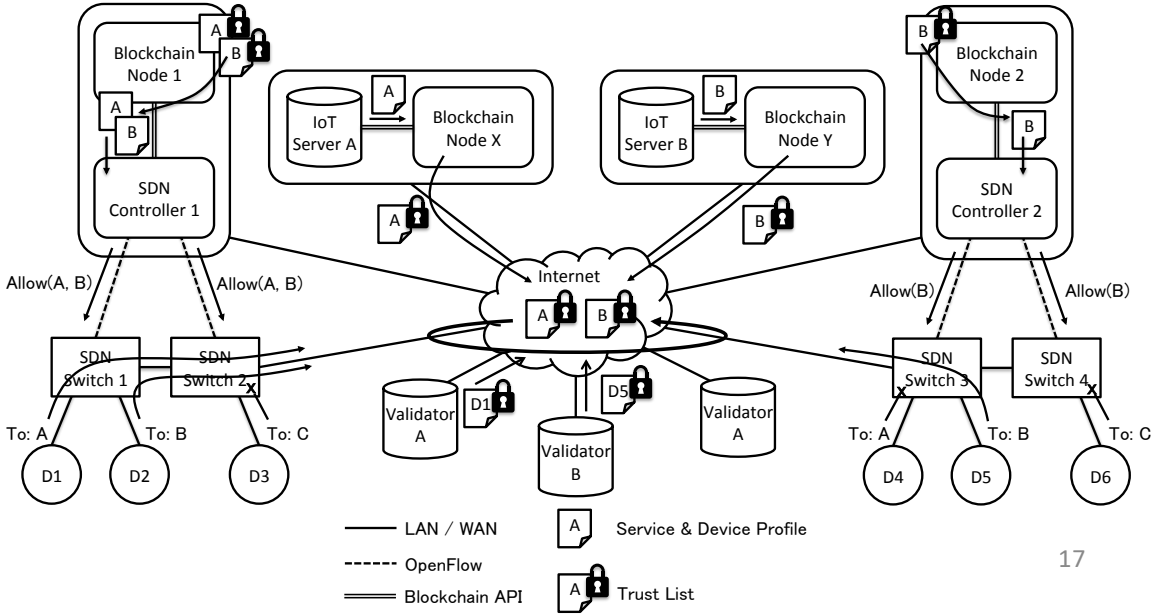
- Problem about IoT
  - Devices can be left unattended easily become a part of powerful botnet
  - Isolation among IoT stakeholders: services, devices and networks to properly identify good traffic
  - The lack of scalability trustability of traffic management policies to implement at the edge network
- Failure by trying protect important things



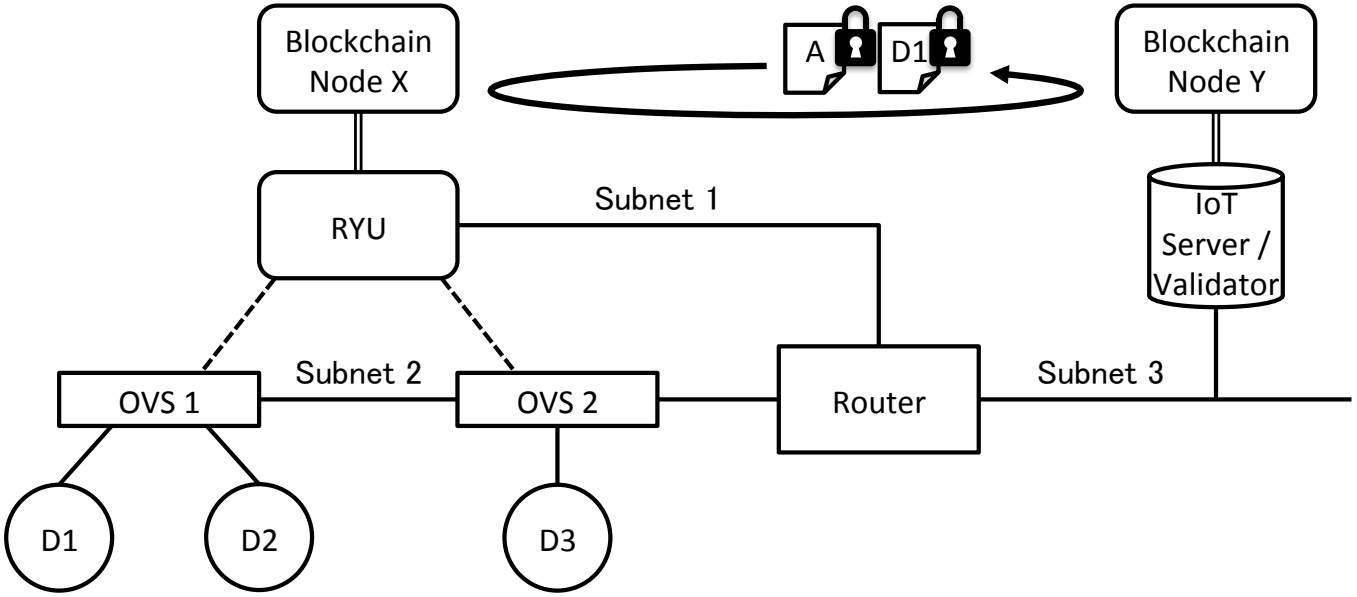
Trust List: Internet-wide and Distributed IoT Traffic Management using Blockchain and SDN (2/3)

- Solution: Trust List for Filtering at the edge
  - Allowing the interaction among IoT stakeholders using Blockchain and SDN
  - Introduces a stakeholder “validator”
  - Enabling the automated traffic management at edge SDN networks





Trust List: Internet-wide and Distributed IoT Traffic Management using Blockchain and SDN (3/3)



Blockchain	Ethereum 1.6.6-stable
Smart Contract	Solidity Compiler 0.4.12
SDN Controller	Ryu 4.15 using OpenFlow 1.3
SDN Switch	Open vSwtich 2.6.1

- Tips
  - Separate Segment / Subnet should be for IoT devices
  - Set the service-specific flow rule and avoid from blindly allowing all communication
  - Such configuration will scale because enforcement happens in the edge network

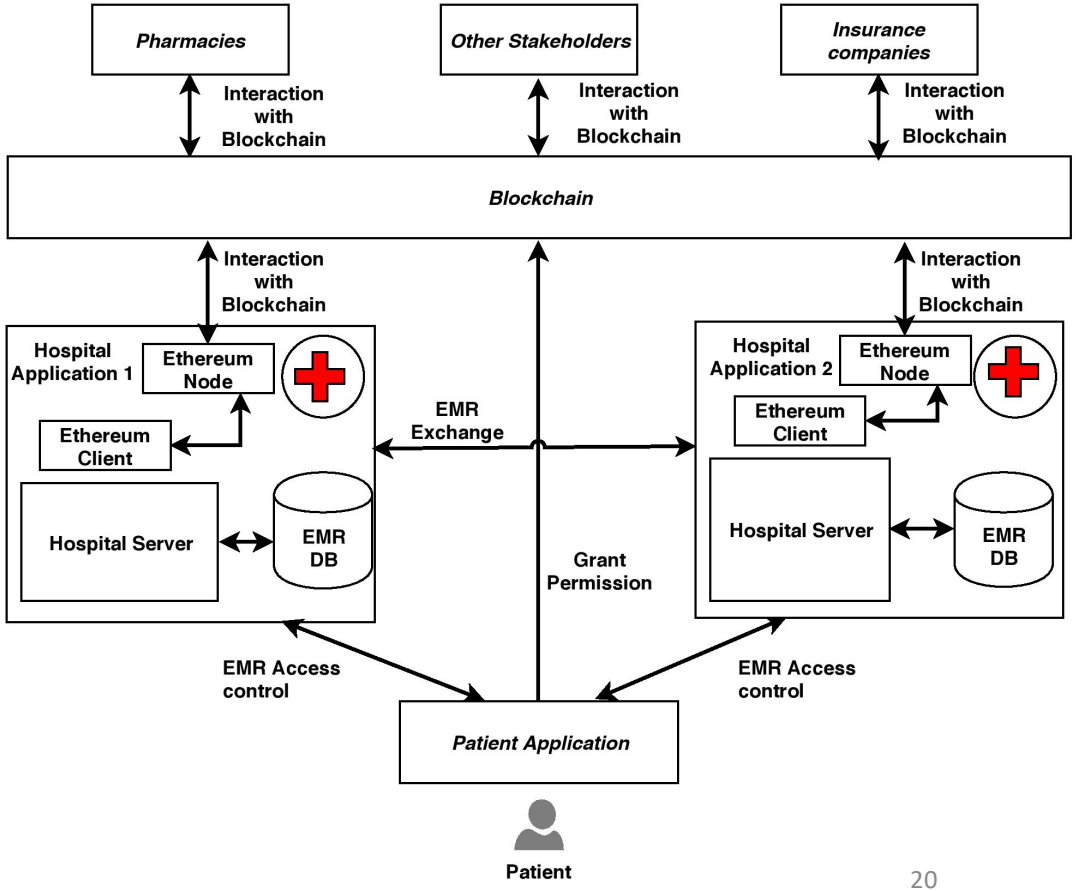
PACEX: Patient-Centric EMR eXchange in Healthcare Systems using Blockchain (1/4)

- Indian Scenario
  - Hardcopy (Paper) of Medical Record is maintained by a Patient
  - Medical Accidents (Malpractice) can be hidden by altering MR that a patient carries

- Questions
  - How can a patient maintain the ownership of Medical Record after digitization?
  - How can a patient 1) maintain proper access control to EMR, and 2) prevent EMR to be tampered?

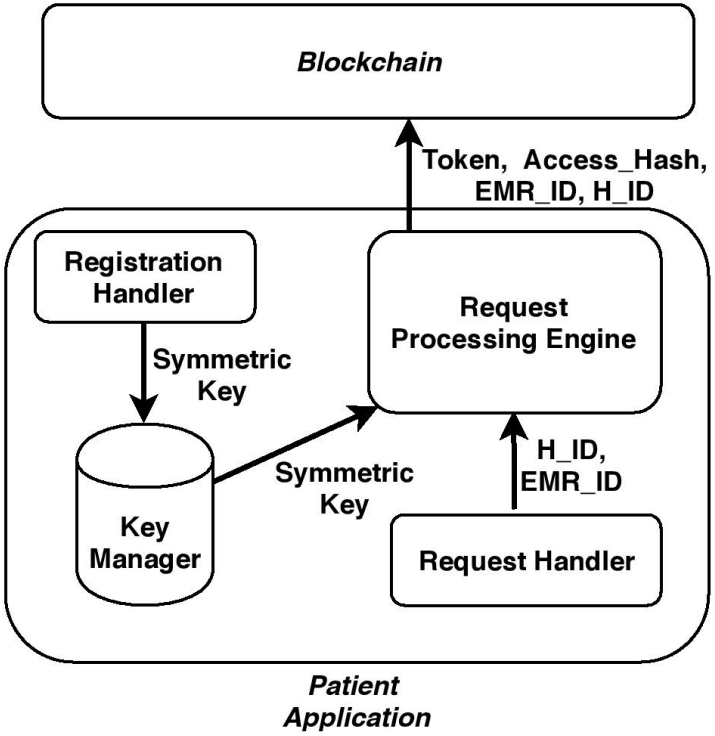
PACEX: Patient-Centric EMR eXchange in Healthcare Systems using Blockchain (2/4)

- Patient-Centric Access Control among Healthcare Stakeholders
  - Can have full authority over EMR
  - Can easily track the history of EMR movements and use
- Characteristics
  - Anomaly detection on EMRs
  - Blockchain-based interplay
  - Affordably small change to the existing healthcare systems
  - No need of technical knowledge of patients

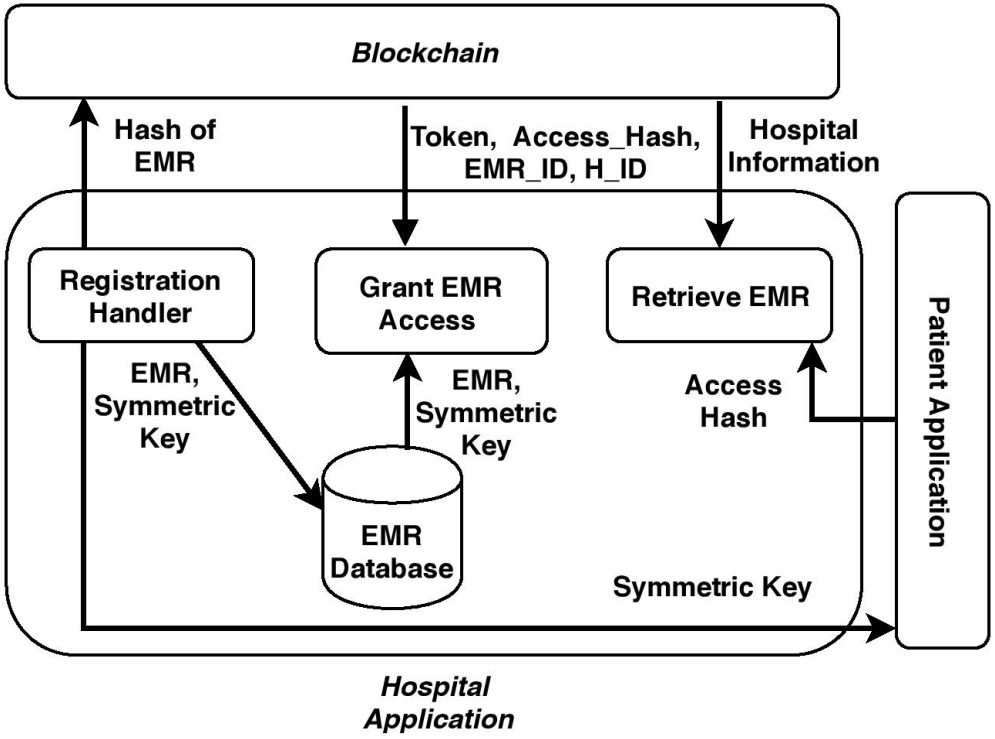


PACEX: Patient-Centric EMR eXchange in Healthcare Systems using Blockchain (3/4)

Patient Application



Hospital Application



PACEX: Patient-Centric EMR eXchange in Healthcare Systems using Blockchain (4/4)

Smart Contract	Use
Patient Smart contract (PSC)	Specific to patient, a new PSC is deployed for each new patient.
Hospital Information Smart contract (HISC)	Maps the basic details of hospital, such as Hospital ID to Hospital server's IP address.
Logger Smart Contract (LSC)	Logs all access requests made, result of processing the access request.
EMR Hash Smart Contract (EHSC)	Stores the hash of EMR record.

Particulars	Module/Language	Version
Blockchain	Ethereum	1.0
Ethereum CLI	Geth	1.9.1
Web Application	Python (Flask)	3.6.7
Smart Contract	Solidity	0.4.25
Database	MongoDB	3.6.3

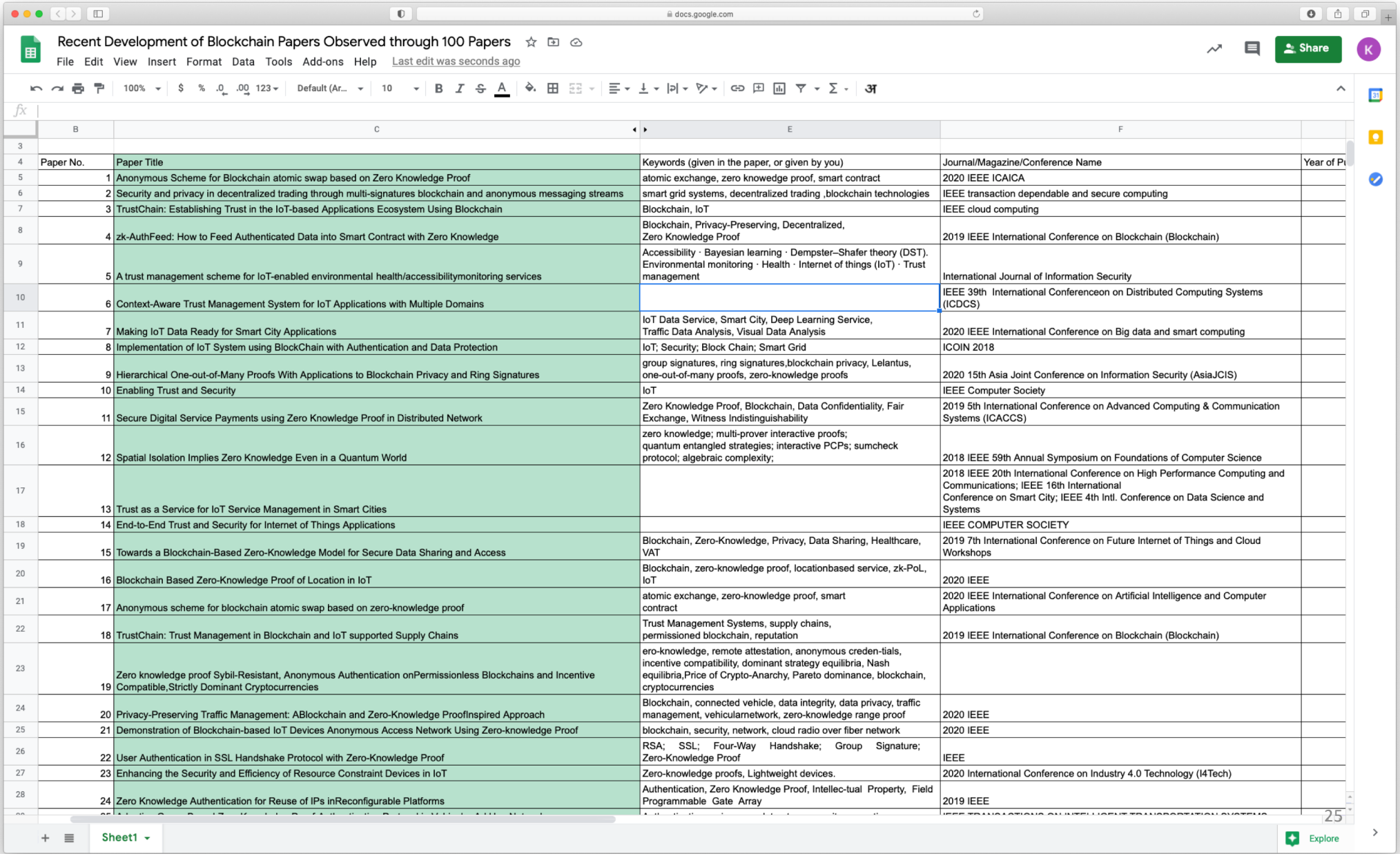
Way of thinking

- What information should be dumped in the blockchain?
- What do you need to think apart from the blockchain?
- Do you want to make your own blockchain?
- What kind of standardization need to be done so that people can take the advantage of blockchain more easily?

Conclusion: Think and Enjoy!!

- Internet performance and protocol design really matter for Blockchain performance

- Using the blockchain should not be an objective!!
  - How to use the blockchain just as a tool is matter.
  - Blockchain related part in a blockchain application is tiny!



Recent Development of Blockchain Papers Observed through 100 Papers

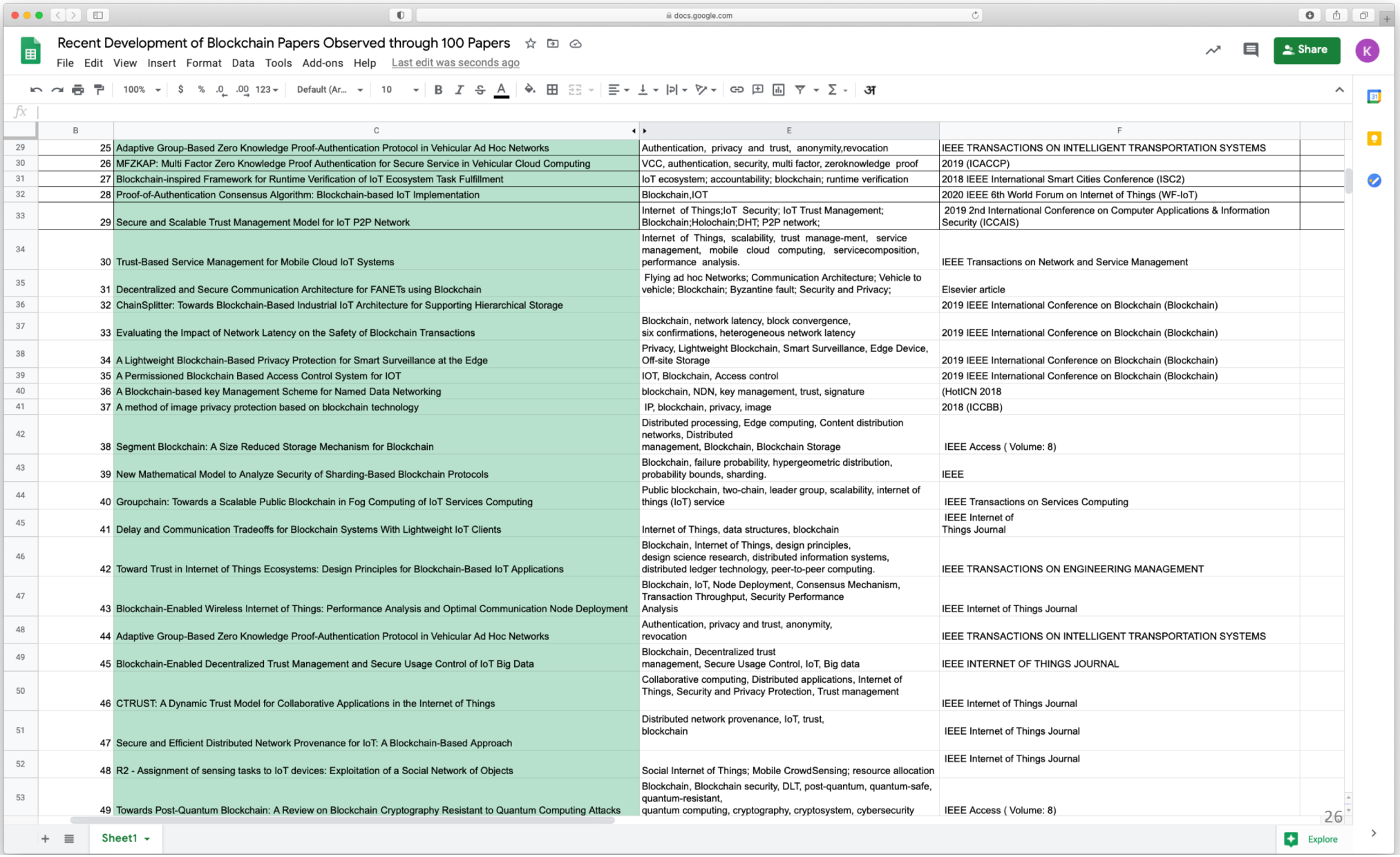
File Edit View Insert Format Data Tools Add-ons Help Last edit was seconds ago

Share

	B	C	E	F	
3					
4	Paper No.	Paper Title	Keywords (given in the paper, or given by you)	Journal/Magazine/Conference Name	Year of Pu
5	1	Anonymous Scheme for Blockchain atomic swap based on Zero Knowledge Proof	atomic exchange, zero knowedge proof, smart contract	2020 IEEE ICAICA	
6	2	Security and privacy in decentralized trading through multi-signatures blockchain and anonymous messaging streams	smart grid systems, decentralized trading ,blockchain technologies	IEEE transaction dependable and secure computing	
7	3	TrustChain: Establishing Trust in the IoT-based Applications Ecosystem Using Blockchain	Blockchain, IoT	IEEE cloud computing	
8	4	zk-AuthFeed: How to Feed Authenticated Data into Smart Contract with Zero Knowledge	Blockchain, Privacy-Preserving, Decentralized, Zero Knowledge Proof	2019 IEEE International Conference on Blockchain (Blockchain)	
9	5	A trust management scheme for IoT-enabled environmental health/accessibilitymonitoring services	Accessibility · Bayesian learning · Dempster–Shafer theory (DST). Environmental monitoring · Health · Internet of things (IoT) · Trust management	International Journal of Information Security	
10	6	Context-Aware Trust Management System for IoT Applications with Multiple Domains		IEEE 39th International Conferenceon on Distributed Computing Systems (ICDCS)	
11	7	Making IoT Data Ready for Smart City Applications	IoT Data Service, Smart City, Deep Learning Service, Traffic Data Analysis, Visual Data Analysis	2020 IEEE International Conference on Big data and smart computing	
12	8	Implementation of IoT System using BlockChain with Authentication and Data Protection	IoT; Security; Block Chain; Smart Grid	ICOIN 2018	
13	9	Hierarchical One-out-of-Many Proofs With Applications to Blockchain Privacy and Ring Signatures	group signatures, ring signatures,blockchain privacy, Lelantus, one-out-of-many proofs, zero-knowledge proofs	2020 15th Asia Joint Conference on Information Security (AsiaJCIS)	
14	10	Enabling Trust and Security	IoT	IEEE Computer Society	
15	11	Secure Digital Service Payments using Zero Knowledge Proof in Distributed Network	Zero Knowledge Proof, Blockchain, Data Confidentiality, Fair Exchange, Witness Indistinguishability	2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)	
16	12	Spatial Isolation Implies Zero Knowledge Even in a Quantum World	zero knowledge; multi-prover interactive proofs; quantum entangled strategies; interactive PCPs; sumcheck protocol; algebraic complexity;	2018 IEEE 59th Annual Symposium on Foundations of Computer Science	
17	13	Trust as a Service for IoT Service Management in Smart Cities		2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th Intl. Conference on Data Science and Systems	
18	14	End-to-End Trust and Security for Internet of Things Applications		IEEE COMPUTER SOCIETY	
19	15	Towards a Blockchain-Based Zero-Knowledge Model for Secure Data Sharing and Access	Blockchain, Zero-Knowledge, Privacy, Data Sharing, Healthcare, VAT	2019 7th International Conference on Future Internet of Things and Cloud Workshops	
20	16	Blockchain Based Zero-Knowledge Proof of Location in IoT	Blockchain, zero-knowledge proof, locationbased service, zk-PoL, IoT	2020 IEEE	
21	17	Anonymous scheme for blockchain atomic swap based on zero-knowledge proof	atomic exchange, zero-knowledge proof, smart contract	2020 IEEE International Conference on Artificial Intelligence and Computer Applications	
22	18	TrustChain: Trust Management in Blockchain and IoT supported Supply Chains	Trust Management Systems, supply chains, permissioned blockchain, reputation	2019 IEEE International Conference on Blockchain (Blockchain)	
23	19	Zero knowledge proof Sybil-Resistant, Anonymous Authentication onPermissionless Blockchains and Incentive Compatible,Strictly Dominant Cryptocurrencies	ero-knowledge, remote attestation, anonymous creden-tials, incentive compatibility, dominant strategy equilibria, Nash equilibria,Price of Crypto-Anarchy, Pareto dominance, blockchain, cryptocurrencies		
24	20	Privacy-Preserving Traffic Management: ABlockchain and Zero-Knowledge ProofInspired Approach	Blockchain, connected vehicle, data integrity, data privacy, traffic management, vehicularnetwork, zero-knowledge range proof	2020 IEEE	
25	21	Demonstration of Blockchain-based IoT Devices Anonymous Access Network Using Zero-knowledge Proof	blockchain, security, network, cloud radio over fiber network	2020 IEEE	
26	22	User Authentication in SSL Handshake Protocol with Zero-Knowledge Proof	RSA; SSL; Four-Way Handshake; Group Signature; Zero-Knowledge Proof	IEEE	
27	23	Enhancing the Security and Efficiency of Resource Constraint Devices in IoT	Zero-knowledge proofs, Lightweight devices.	2020 International Conference on Industry 4.0 Technology (I4Tech)	
28	24	Zero Knowledge Authentication for Reuse of IPs inReconfigurable Platforms	Authentication, Zero Knowledge Proof, Intellec-tual Property, Field Programmable Gate Array	2019 IEEE	

Sheet1

Explore



Recent Development of Blockchain Papers Observed through 100 Papers

File Edit View Insert Format Data Tools Add-ons Help Last edit was seconds ago

Share

	B	C	E	F
29	25	Adaptive Group-Based Zero Knowledge Proof-Authentication Protocol in Vehicular Ad Hoc Networks	Authentication, privacy and trust, anonymity,revocation	IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS
30	26	MFZKAP: Multi Factor Zero Knowledge Proof Authentication for Secure Service in Vehicular Cloud Computing	VCC, authentication, security, multi factor, zeroknowledge proof	2019 (ICACCP)
31	27	Blockchain-inspired Framework for Runtime Verification of IoT Ecosystem Task Fulfillment	IoT ecosystem; accountability; blockchain; runtime verification	2018 IEEE International Smart Cities Conference (ISC2)
32	28	Proof-of-Authentication Consensus Algorithm: Blockchain-based IoT Implementation	Blockchain,IOT	2020 IEEE 6th World Forum on Internet of Things (WF-IoT)
33	29	Secure and Scalable Trust Management Model for IoT P2P Network	Internet of Things;IoT Security; IoT Trust Management; Blockchain;Holochain;DHT; P2P network;	2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)
34	30	Trust-Based Service Management for Mobile Cloud IoT Systems	Internet of Things, scalability, trust manage-ment, service management, mobile cloud computing, servicecomposition, performance analysis.	IEEE Transactions on Network and Service Management
35	31	Decentralized and Secure Communication Architecture for FANETs using Blockchain	Flying ad hoc Networks; Communication Architecture; Vehicle to vehicle; Blockchain; Byzantine fault; Security and Privacy;	Elsevier article
36	32	ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage		2019 IEEE International Conference on Blockchain (Blockchain)
37	33	Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions	Blockchain, network latency, block convergence, six confirmations, heterogeneous network latency	2019 IEEE International Conference on Blockchain (Blockchain)
38	34	A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge	Privacy, Lightweight Blockchain, Smart Surveillance, Edge Device, Off-site Storage	2019 IEEE International Conference on Blockchain (Blockchain)
39	35	A Permissioned Blockchain Based Access Control System for IOT	IOT, Blockchain, Access control	2019 IEEE International Conference on Blockchain (Blockchain)
40	36	A Blockchain-based key Management Scheme for Named Data Networking	blockchain, NDN, key management, trust, signature	(HotICN 2018
41	37	A method of image privacy protection based on blockchain technology	IP, blockchain, privacy, image	2018 (ICCBB)
42	38	Segment Blockchain: A Size Reduced Storage Mechanism for Blockchain	Distributed processing, Edge computing, Content distribution networks, Distributed management, Blockchain, Blockchain Storage	IEEE Access (Volume: 8)
43	39	New Mathematical Model to Analyze Security of Sharding-Based Blockchain Protocols	Blockchain, failure probability, hypergeometric distribution, probability bounds, sharding.	IEEE
44	40	Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing	Public blockchain, two-chain, leader group, scalability, internet of things (IoT) service	IEEE Transactions on Services Computing
45	41	Delay and Communication Tradeoffs for Blockchain Systems With Lightweight IoT Clients	Internet of Things, data structures, blockchain	IEEE Internet of Things Journal
46	42	Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications	Blockchain, Internet of Things, design principles, design science research, distributed information systems, distributed ledger technology, peer-to-peer computing.	IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT
47	43	Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment	Blockchain, IoT, Node Deployment, Consensus Mechanism, Transaction Throughput, Security Performance Analysis	IEEE Internet of Things Journal
48	44	Adaptive Group-Based Zero Knowledge Proof-Authentication Protocol in Vehicular Ad Hoc Networks	Authentication, privacy and trust, anonymity, revocation	IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS
49	45	Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data	Blockchain, Decentralized trust management, Secure Usage Control, IoT, Big data	IEEE INTERNET OF THINGS JOURNAL
50	46	CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things	Collaborative computing, Distributed applications, Internet of Things, Security and Privacy Protection, Trust management	IEEE Internet of Things Journal
51	47	Secure and Efficient Distributed Network Provenance for IoT: A Blockchain-Based Approach	Distributed network provenance, IoT, trust, blockchain	IEEE Internet of Things Journal
52	48	R2 - Assignment of sensing tasks to IoT devices: Exploitation of a Social Network of Objects	Social Internet of Things; Mobile CrowdSensing; resource allocation	IEEE Internet of Things Journal
53	49	Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks	Blockchain, Blockchain security, DLT, post-quantum, quantum-safe, quantum-resistant, quantum computing, cryptography, cryptosystem, cybersecurity	IEEE Access (Volume: 8)

Sheet1

Explore

Done!!