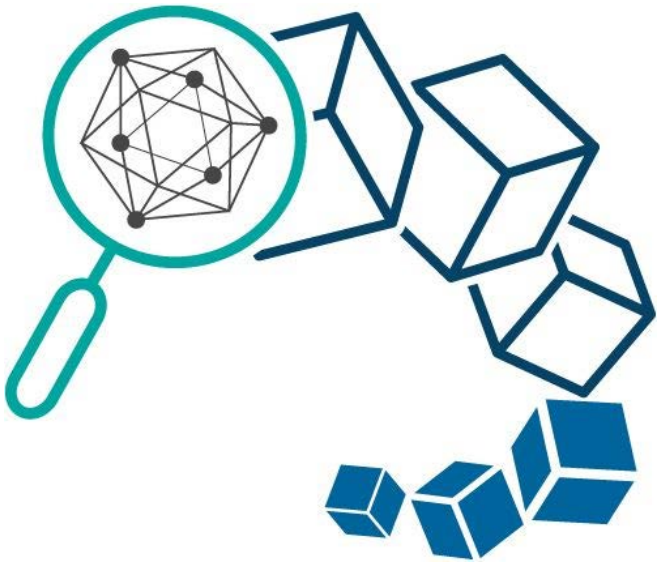
G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications



Laphou Lao*, Xiaohai Dai*†, Bin Xiao* and Songtao Guo‡
*The Hong Kong Polytechnic University, Hong Kong,
†Huazhong University of Science and Technology, China,
‡Chongqing University, China

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學
Opening Minds • Shaping the Future • 啟迪思維 • 成就未來

Contents

- Introduction
- Problem Statement
- Protocol Design
- Performance Analysis
- Conclusion

Introduction

- Blockchain
  - Cryptocurrencies
  - Online Payment
  - Data Tracking
- IoT
  - Smart Home Appliances
  - Indoor and Outdoor Sensors
- IoT Blockchain
  - Record Transaction Data
  - Optimize System Performance
  - Additional Security
  - Automatic Transaction Management

IoT Blockchain

- Background of IoT Blockchain
  - Become Increasingly Popular
  - Wide Range of Applications
  - Advantages in massive devices management, security and data credibility
- Challenge of IoT Blockchain
  - Resource Constraints
  - Consensus Protocol
  - Scalability

Challenges to IoT Blockchains

- Resource Constraints
  - Computational Power, Storage, Bandwidth
- Consensus Protocol with Security Design
  - Vulnerable to Sybil Node Attacks
  - High Computational Cost
  - Low Scalability
- Scalability
  - Manage Enormous Number of IoT Devices
  - Frequent Change of Network Size

Problem definition

- How to design a practical and scalable consensus mechanism for IoT blockchains with high-consensus efficiency and low-consensus latency?

Related work

- Few consensus mechanism designed for IoT-Blockchain
- Some research works on utilizing location information in the blockchain, such as [6]–[9].
- Focus on
  - Location Accuracy
  - Security
  - Privacy Preserving
- Not include
  - Consensus Efficiency
  - Network Overhead
  - Network Scalability

Application comparisons

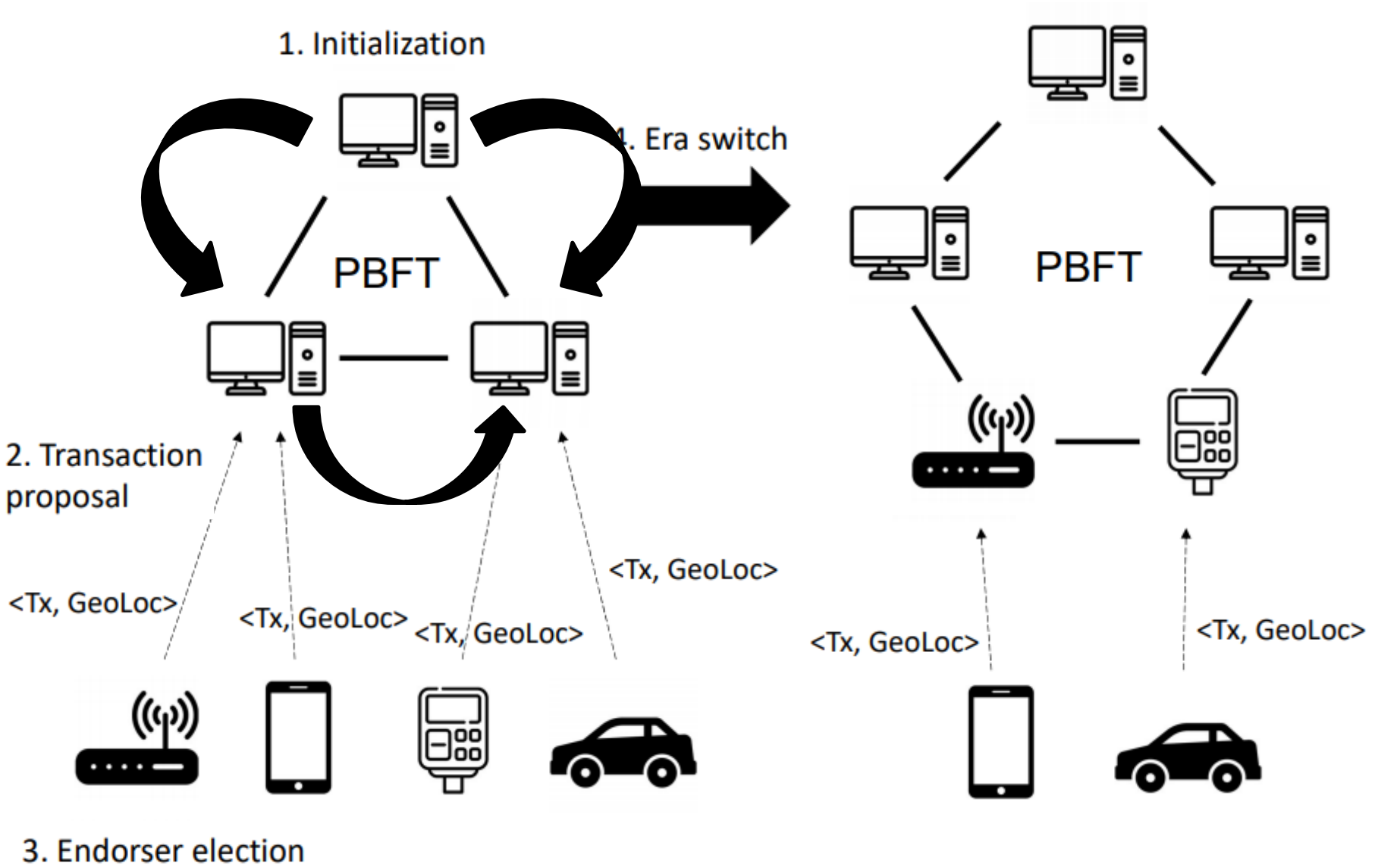
Comparison Between IoT-Blockchain Applications

IoT-Blockchain	Blockchain	Consensus	Service	IoT devices	Company size
Atonomi [5]	Atonomi	Atonomi	IoT-blockchain solutions	Smart devices, Smart home	Leading provider of IoT data security
ElectriCChain [13]	SolarCoin	PoS	Process data of solar panel	Solar panel	Open source project
Filament [3]	Hardware-based Consortium Blockchain	PoW	Transaction service to embedded IoT	Blocklet USB Enclave, Blocklet Chip	40 milions market cap
JD.com [14]	BFT blockchain	BFT	Blockchain platform	IoT devices	1.7 trillions market cap
LeewayHertz [15]	Public blockchain	PoW	IoT-blockchain solutions	Robots, Audio devices	More than 10 years in operations
LO3 Energy [16]	Public blockchain solution	PoW	Solar energy marketplace	Grid Edge, Solar plane	1 million in revenue annually
Slock.it [17]	Ethereum	PoW	Commission shop	Electronic lock	1.5 millions in revenue annually
UniquID [18]	Litecoin	PoW	Integrated service to IoT and blockchain	Sensors, Actuators, Appliances	Open source project
Xage [4]	Fabric	PBFT	Security service	Broker, Enforcement Point	300 milions market cap

Our Novel Method: G-PBFT

- Resource-Constraint Architecture Design
  - Endorser Election
  - Fixed IoT devices have more computational power
- Novel Consensus Protocol
  - Location-Based, More Secure
- Scalable Design
  - Low Delay
  - High Consensus Efficiency
  - High Scalability

G-PBFT Overview



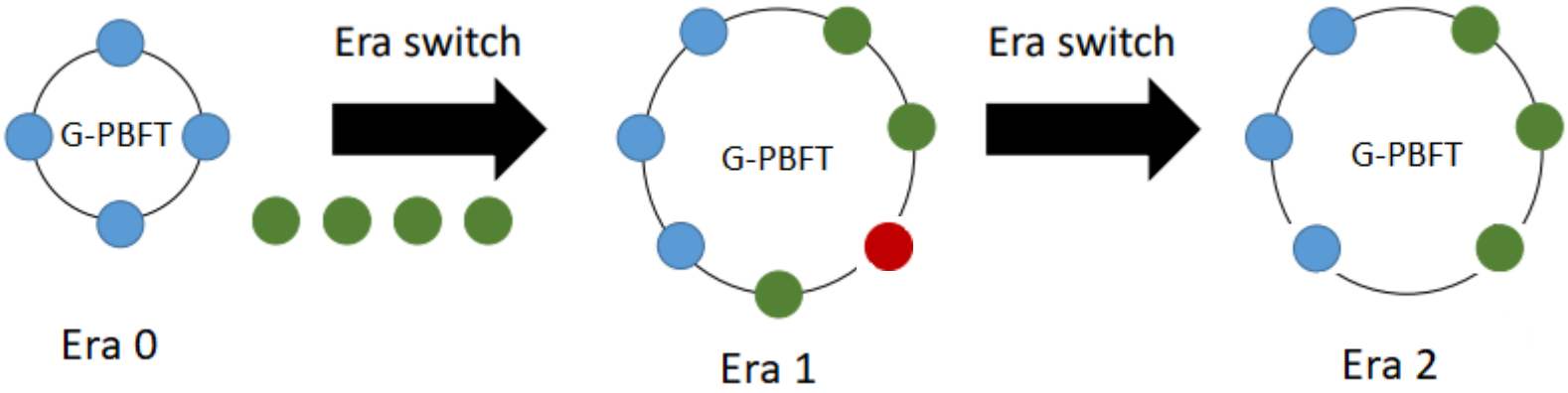
3. Endorser Election

- IoT devices generate data and upload to blockchain
  - Essential Data
  - Temperature of Sensors
  - Business Data of Mobile Payments
- Requires IoT devices to upload location and timestamp periodically
  - Crypto-Spatial Coordinates (CSC)
    - location Information
    - Smart Contract Address
  - IoT device with longer geographic time become endorser
  - Authenticated node becomes endorser makes the system more secure

	CSC	Timestamp	Geographic Timer
1	5AH71r9wTRp9eHsqR	5/8/2019 18:00:00	0
2	5AH71r9wTRp9eHsqR	5/8/2019 18:56:04	56:04
3	5AH71r9wTRp9eHsqR	6/8/2019 00:00:00	06:56:04
4	5AH71r9wTRp9eHsqR	6/8/2019 06:00:00	12:56:04
5	5AH71r9wTRp9eHsqR	6/8/2019 12:00:00	18:56:04

4. Era Switches Mechanism

- Scalable by Era Switches
  - Allows frequent arrival and departure of IoT devices
  - Happen every T seconds in our system
  - Minimize the impact on performance when network change
  - Achieve high network scalability

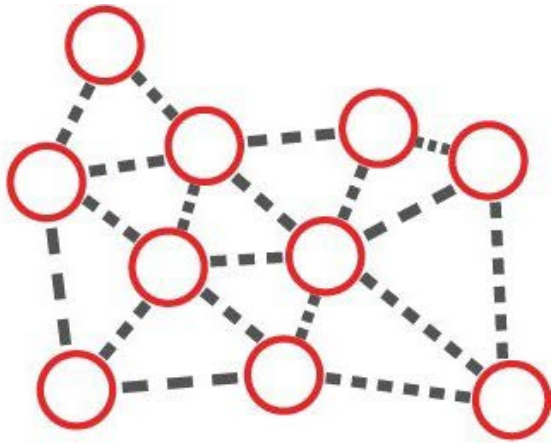


Incentive Design in GPBFT

- Incentive mechanism
  - Geographic timer is used for block generation
  - A longer time in the geographic timer will have a higher chance of generating a new block
  - An endorser generates a new block can get 70% of the transaction fee
  - Endorsers endorse others block can share 30% of the transaction fee

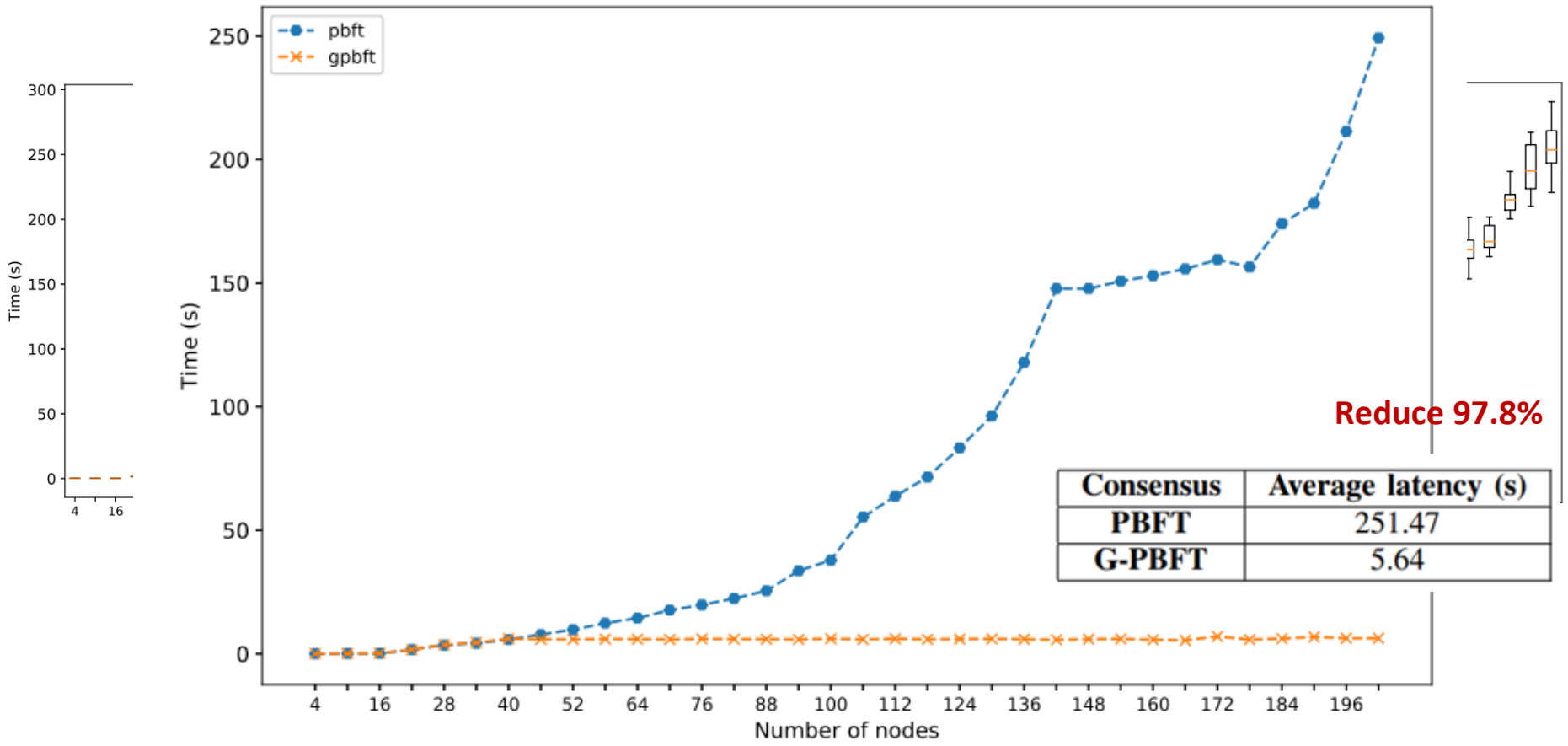
Experiment Setup

- We construct an IoT system by Ubuntu machines
- Numerous IoT nodes in an IoT system
- Small size of endorser committee
- Reasonable amount of 202 nodes to facilitate the running of a large IoT network
- Initial consensus committee 4 and gradually increase to 202 by election



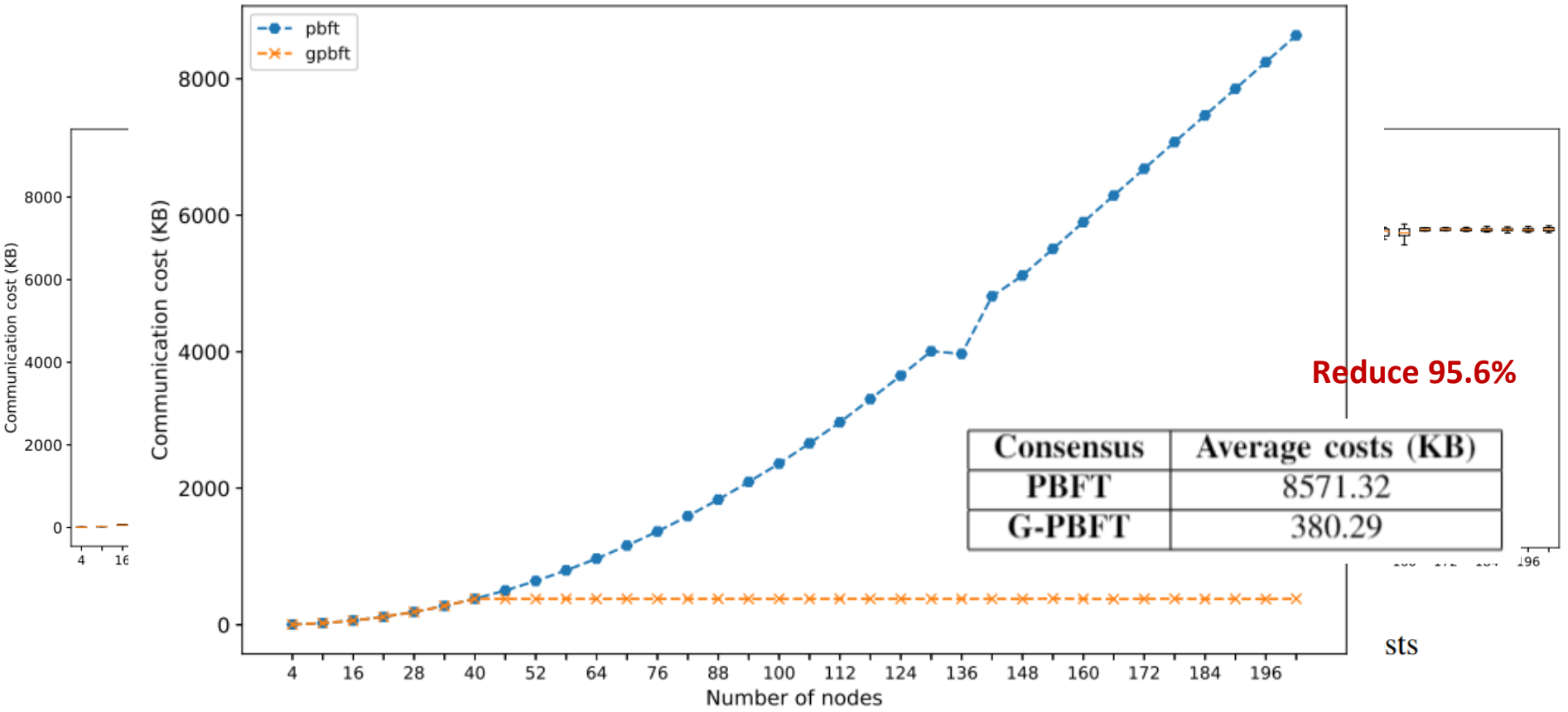
Consensus Latency Analysis

- Comparison of consensus latency between PBFT and G-PBFT



Communication Cost Analysis

- Comparison of communication cost between PBFT and G-PBFT



Consensus	Average costs (KB)
PBFT	8571.32
G-PBFT	380.29

Reduce 95.6%

Comparison between Consensus

Compare G-PBFT with other consensuses in different aspects

Consensus	Blockchain type	Speed	Scalability	Network Overhead	Computing Overhead	Adversary Tolerance	Example of use
BFT	Permissioned	High	Low	High	Low	<33.3% Replicas	Tendermint
PBFT	Permissioned	High	Low	High	Low	<33.3% Faulty Replicas	Hyperledger
dBFT	Permissioned	Low	High	High	Low	<33.3% Faulty Replicas	NEO
PoW	Permissionless	Low	Low	High	High	<25% Computing Power	Bitcoin
PoS	Permissionless	Low	Low	High	Low	<50% Stake	Peercoin
DPoS	Permissionless	High	Low	Low	Low	<50% Validators	BitShares
PoA	Permissionless	Low	High	Low	Low	<50% of Online Stake	Decred
PoSpace	Permissionless	Low	Low	High	Low	<50% Space	SpaceMint
PoI	Permissionless	Low	Low	High	Low	<50% Stake	NEM
PoB	Permissionless	Low	Low	High	Low	<50% Coins	XCP
G-PBFT	Permissionless	High	High	Low	Low	<33.3% Endorsers	

Contribution

1. We propose a novel location-based blockchain consensus protocol G-PBFT
   - Ensure the Loyalty of Endorser
   - Enhance Security of Blockchain

2. G-PBFT solve high computational overhead and low scalability problem
3. G-PBFT reduce 97.8% consensus latency and 95.6% communication cost of traditional consensus protocol

Conclusion

- Novel location-based blockchain consensus for IoT-blockchain applications.
  - Geographic and Timestamp Information
  - Automated Endorser Elections
- High consensus efficiency and low network overhead
  - reducing the number of endorsers
  - security guaranteed
- High scalability
  - Join and leave freely
  - Keep the performance
- Comprehensive experiments

Thank You!!!