QuarkChain - A High-Capacity Peer-to-Peer Transactional System

Qi Zhou
qizhou@quarkchain.org

Blockchain Scalability Problem

- Low transaction per second of Blockchain compared to its centralized counterpart

- Bitcoin ~ 3 TPS, Ethereum ~ 10 TPS

- VISA 56,000 TPS (Aug. 2014)

- Alipay 120,000 TPS (Nov. 2016)

Solution 1: Multiple Blockchains

- Multiple blockchains run independently (Bitcoin, Litecoin, BCH, Ethereum)

- Limited cross-chain transactions

- Unbalanced hash power among chains

- Maintain multiple accounts/addresses on different blockchains

Solution 2: Lightning Network

- Offload on-chain transactions to off-chain

- Number of off-chain transactions per second could be infinite in theory

- Generally require two transactions to create/destroy a channel

- Doesn't improve on-chain capacity

Solution 3: Sharding

- Ethereum adopts sharding to address scalability problem

- Cross-shard transactions are not supported in 1.0

- Need to manage multiple accounts in different shards

QuarkChain - Design for Scalability from Beginning

- Support 1,000,000+ on-chain transactions per second

- Trustless

- Smart contract

Two-Layered Blockchains

- QuarkChain consists of two layers of blockchains

- First layer contains elastic sharding blockchains

- Second layer is a root blockchain that confirms the blocks from sharded blockchains

- Support adding more shards in active network

Collaborative Mining (or Minting)

- Design incentives from game-theoretic perspective

- Hash powers are incentivized to distribute evenly among shards

- Prevent double spending: Requires 25%-40+% percentage of overall hash power regardless the number of shards

Verification of Collaborative Mining

Node 1 mined minor block height 1694 on minor chain 4, used t...
=====================================
Node 1, rewards 1262800
Node 2, rewards 1238900
Node 3, rewards 15000
Node 4, rewards 17100
Node 5, rewards 12000
Node 6, rewards 4000
Node 7, rewards 19200
Node 8, rewards 4100
Node 9, rewards 13700
Node 10, rewards 6800
Node 11, rewards 3800
Node 12, rewards 4100
Node 13, rewards 13000
Node 14, rewards 20400
Node 15, rewards 20500
Node 16, rewards 13300
Node 17, rewards 20200
Node 18, rewards 5100
Powerful/weak rewards ratio: 13.01

Major chain height 234, reward 8400, work 78307.24, blocks interval 7.73
Minor chain 0, height 1693, work 1010.22, block interval 1.07
Minor chain 1, height 1678, work 999.83, block interval 1.08
Minor chain 2, height 1690, work 1003.83, block interval 1.07
Minor chain 3, height 1690, work 1005.94, block interval 1.07
Minor chain 4, height 1694, work 997.31, block interval 1.07
Minor chain 5, height 1697, work 999.02, block interval 1.07
Minor chain 6, height 1686, work 999.34, block interval 1.07
Minor chain 7, height 1678, work 999.61, block interval 1.08
=====================================
Node 1 mined minor block height 1695 on minor chain 4, used time 0.11
Node 1 mined minor block height 1696 on minor chain 4, used time 0.03
Node 1 mined minor block height 1697 on minor chain 4, used time 0.38
Node 1 mined minor block height 1698 on minor chain 5, used time 0.01
Node 1 mined minor block height 1699 on minor chain 5, used time 0.03
Node 1 mined minor block height 1700 on minor chain 5, used time 0.05
Node 1 mined minor block height 1687 on minor chain 6, used time 0.05
Node 15 mined minor block height 1694 on minor chain 0, used time 0.02
Node 1 mined minor block height 1679 on minor chain 1, used time 0.01
Node 1 mined minor block height 1691 on minor chain 2, used time 0.04
Node 16 mined minor block height 1691 on minor chain 3, used time 0.13
Node 1 mined minor block height 1679 on minor chain 7, used time 0.05

Cross-Shard Transactions as First-Class Citizen

- Cross-shard transactions can be issued at any time

- Cross-shard transactions can be confirmed in minutes

- Scalable: the TPS of cross-shard transactions increases linearly as the number of shards increases

Simple Account Management

- One account for all shards

- Smart wallet - a user doesn't need to aware of sharding

Scale Horizontally

- A super-full node can be extremely expensive when TPS goes high

- Enable running a cluster of honest nodes as a super-full node

Competitor Comparison

|	Ethereum Sharding	EOS	LightChain	QuarkChain
Target TPS	1,000	100,000	100,000	1,000,000
Consensus	PoS	DPOS	PoW + PoM	PoW (+ PoS)
Cross-shard transaction	Not supported in Sharding 1.0	N/A	No	Yes
Other		21 selected nodes to generate blocks	Raised 50,000 ETH (50% token) in Jan. 2018	

Competitor Comparison

	Zilliqa	IOST	Ardor	QuarkChain
Target TPS	10,000	100,000	100	1,000,000
Consensus	PoW + Leader	Byzantine consensus	PoS	PoW (+ PoS)
Cross-shard transaction	Supported	Atomix (Multiple stage commitment)	Each child chain owns its coin	Yes
Other		Leader election in distributed sharding	Child chain may submit conflicting transactions	

Dev Team Members

Qi Zhou/CEO/CTO

Software Engineer at Facebook
Expert in high-performance systems
Former Googler and have 15+ years
development experience
PhD from Georgia Institute of Technology
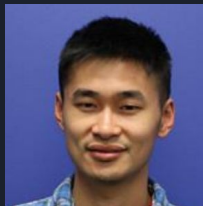
Xifan Yan

Software Engineer at Facebook
Expert in large-scale systems and help
Facebook process 100+M videos/day
MSc from Carnegie Mellon University

(Clearing conflict of interest with Facebook)

Software Engineer at Facebook
Expert in distributed system, computer
communication, and network protocol
MSc from University of Southern California

(Clearing conflict of interest with Facebook)

Software Engineer at Facebook
5 years work experience at Google
Expert in large distributed storage and massive
fanout systems
Investor of blockchain since 2013
MSc from University of Michigan

Team Members

Ting Du / CMO for Chinese Market

Geek in Product Management
Founder of incubator Demo++, Incubator of Ink
Committee of Liuhe Capital Startup
Dedicated on Blockchain productization and
business application

Yaodong Yang / Researcher

PhD Advisor at Xi'an Jiao Tong Univ.
Partner of Demo++
PhD from Virginia Tech
Dedicated on Blockchain development
and research
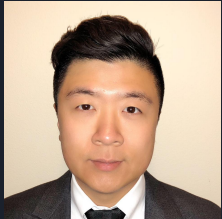
Kyle Wang / COO

Founder and CEO of H&W, LLC (Swizerland),
Harvest Water Cooper, Inc. (US) , and Bespoke Tech
Consulting (Cayman island),Keen understanding of
distributed ledger technology (DLT) regulatory
framework by the government of Gibraltar
12 years experience in international trading and
supply chain finance

Wencen Wu / Fund Manager

Assistant Professor at RPI
Expert in model simulation and verification
in distributed autonomous systems
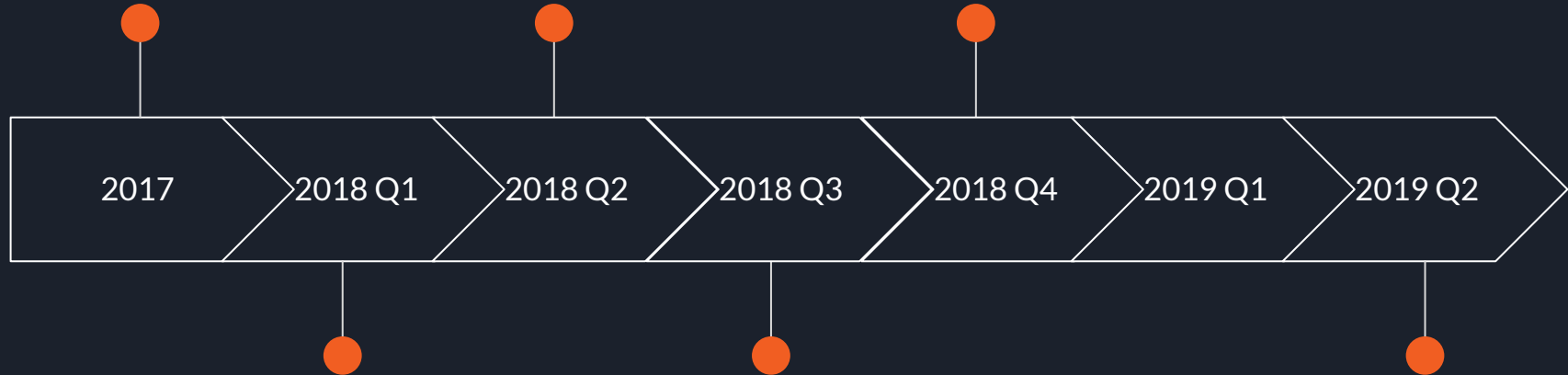PhD from Georgia Institute of Technology

Timeline

Blockchain Scalability
Problem Research

Verification Code 0.2
Testnet 0.1

QuarkChain Core 1.0
Mainnet 1.0
Smart Wallet 1.0

2017　2018 Q1　2018 Q2　2018 Q3　2018 Q4　2019 Q1　2019 Q2

Verification Code 0.1
White Paper

Testnet 0.2

QuarkChain Core 2.0
Smart Wallet 2.0