Scale-Out Blockchains
Off-Chain Scaling

Fangyu Gai, Ph.D. student, supervised by Dr. Chen Feng
University of British Columbia – Okanagan Campus
April 23, 2019

https://medium.com/coinmonks/blockchain-101-4acc9902b3a4
Fangyu Gai

https://fangyugai.me
fangyu.gai@ubc.ca

Ph.D. student, UBC – Okanagan Campus, supervised by Dr. Chen Feng

- **Education**
  - *B.Sc in Software Engineering, Beijing Institute of Technology, China, since 2011*
  - *M.Sc in Computer Science, National University of Defense Technology, China, since 2015*
  - *Ph.D. in Electrical Engineering, University of British Columbia, Canada, since 2018*

- **Research in Blockchain**
  - *Off-chain scaling*
  - *Consensus algorithms*
Overview

• Why does the blockchain need scaling?
• What is off-chain scaling?
• How do off-chain protocols work?
Why does the blockchain need scaling?
Why does the blockchain need scaling?

• Scaling? Scalable? Scalability?

• In a scalable system, as we move from small to large, things should not get incrementally worse.
Why does the blockchain need scaling?

Cryptocurrencies Transaction Speeds Compared to Visa & Paypal

- Visa: 24,000 transactions per second
- Ripple: 1,500 transactions per second
- PayPal: 60 transactions per second
- Bitcoin Cash: 48 transactions per second
- Dash: 20 transactions per second
- Ethereum: 7 transactions per second
- Litecoin: 60 transactions per second
- Visa: 1,500 transactions per second

Article & Sources:
https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared
Why does the blockchain need scaling?
Why does the blockchain need scaling?
Why does the blockchain need scaling?

Because the current blockchains (e.g. Bitcoin, Ethereum) are not scalable.
Why does the blockchain need scaling?

Why are the current blockchains not scalable?
Why does the blockchain need scaling?

Scalability Trilemma

Security

Decentralization

Scalability

https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df
Why does the blockchain need scaling?

Conceptually, there are three main directions we might go about breaking the trilemma

• Alternative blockchain consensus architectures
  • PoS
  • New BFT
  • DAG (Directed Acyclic Graph)
• On-chain solutions (Layer 1)
  • Sharding
  • Parallel Chain
• Off-chain solutions (Layer 2)
  • Payment Channels
  • Sidechain
What is off-chain scaling?
What is off-chain scaling?

- Off-chain protocols use public blockchains as the *settle layer*, aka the “mainchain”.

- Every parties have some *deposits* frozen on the mainchain.

- Parties can do *unlimited transactions* off-chain and only touch the mainchain when it’s *necessary*.

- The mainchain has no idea what happens off-chain, but it can tell who is right or wrong when *conflicts happen*, and the result is *trusted*.

- When someone wants to *withdraw/exit*, he or she needs to provide the *proof of possession*. 
What is off-chain scaling?

A high-level example

Smart Contract

Deposit

Challenge

Withdraw/exit

Transactions

Alice

Bob
What is off-chain scaling?

- Application in need of scalable, fast and reliable blockchain infrastructure
- Traditional database techniques can be used
- The implementation of off-chain protocols depend on the use case
- Expose an API to the upper layer, so that public nodes can verify the integrity inside the network
- Provides trustless services to the upper layer
What is off-chain scaling?

Benefits of off-chain solutions:
- Privacy
- Interoperability
- Instant Transactions
- Low Fees
- Scalability
- Backward Compatibility
How do off-chain protocols work?

— — Take Payment Channels & Sidechain for example
Payment Channels: Open

Blockchain

Multisig Contract
Can be spent only with the signatures of both Alice and Bob
Payment Channels: Transactions

Guarantee for Bob to receive 1 BTC (when published before ⏰)

Blockchain
Payment Channels: Transactions

Alice

Bob

5 (Alice, Bob) → 3 (Alice) → 2 (Bob)

Guarantee for Bob to receive 2 BTC (when polished before)

BlockChain

5 (Alice) → 5 (Alice, Bob) → 5 (Alice)

Alice

?? Bob
Payment Channel Networks

- Alice
- Bob
- Carol

Send 1 BTC to Carol
Payment Channel Networks

1. Send 1 BTC

Send 1 BTC to Carol
Payment Channel Networks

1. Send 1 BTC
2. Forward 1 BTC to Carol

Alice

Bob

Carol
Payment Channel Networks

Alice (Send 1 BTC to Carol)

1. Send 1 BTC

2. Forward 1 BTC to Carol

Should happen atomically
Payment Channel Networks

Send 1 BTC to Carol

1. Send 1 BTC + fee to Bob

Fee acts as an incentive for Bob to participate in the payment

2. Forward 1 BTC to Carol

Should happen atomically
Sidechain

- Decentralized Exchange
- Retailers
- Social Network
- Micropayments

Mainchain (e.g. Ethereum)
Sidechain

MC → CP1 → CP2 → CP3

Commit

Challenge

Smart Contract

Withdrawal/Exit

TX1 → TX2 → TX3 → TX4 → TX5

Propose

V1 → V2 → V3 → V4

P1 P2 P3 P4 P5

Header

TX 1
TX 2
TX 3
TX 4
TX 5

SC Block

Verify
Summary

Open challenges for off-chain protocols

• Online Watchdog Requirements
• Long withdrawal/exit time
• Withholding attack
• Locked and Fragmented Collateral
• Introduce new attack plane
Thanks!

Scale-Out Blockchains
Off-Chain Scaling
Q&A

Fangyu Gai, Ph.D. student, supervised by Dr. Chen Feng
University of British Columbia – Okanagan Campus
April 23, 2019

https://medium.com/coinmonks/blockchain-101-4acc9902b3a4