Scale or Perish?

Payment Channel, State Channel & Plasma

For discussion purposes

DBSystem, SoC, NUS
Pending ethereum transactions after CryptoKitties' release
Agenda

1. Overview
2. Payment channels
3. State channel
4. Plasma
5. Discussion
Overview

Blockchain

On-chain scaling

Sharding, trusted hardware, etc.

Off-chain scaling

Sidechains, Payment channels, State channels, TrueBit, Plasma
Overview

- **On-chain scaling**
  - More blocks per second
  - Scale consensus
- **Off-chain scaling**
  - *Avoid* transactions on blockchain as much as possible
  - Why?
    - Better latency
    - Finality
    - More transaction volumes
Overview

- Off-chain scaling: recurring theme
  - Off-chain communications
  - Blockchain as a fair judge
- History
Agenda

1. Overview
2. **Payment channel**
3. State channel
4. Plasma
5. Discussion
Payment channel - Problem

- Alice wants to pay Bob 0.0001 ETH
- Problems:
  - Fees (0.2-5 USD)
  - Wait for many confirmation blocks (~hours)
  - Cryptokitties
Payment channel - Solution

- Ethereum version of Lightnight network
- Setup

Ethereum

Smart contract

Alice: 10
Bob: 10

Can only withdraw with BOTH signatures

(Deposit 10, Signed Alice)
(Deposit 10, Signed Bob)

Balance: 10
Balance: 10
Payment channel - Solution

- Pay

Smart contract
- Alice: 10
- Bob: 10

Can only withdraw with BOTH signatures

Ethereum

Alice: 9
Bob: 11
SeqNo: 1
Signed Alice
Signed Bob

Balance: 9
Balance: 11
Payment channel - Solution

- Many payments latter

**Smart contract**

*Can only withdraw with BOTH signatures*

**Ethereum**

Alice: 10
Bob: 10

**Balance:**
Alice: 16
Bob: 4

**Signed:**
Alice: 9
Bob: 11
SeqNo: 1
Signed Alice
Signed Bob

Alice: 7
Bob: 13
SeqNo: 2
Signed Alice
Signed Bob

... 

Alice: 16
Bob: 4
SeqNo: 1000
Signed Alice
Signed Bob

**Balance:**
Alice: 16
Bob: 4
Payment channel - Solution

Smart contract

Alice: 10
Bob: 10

This is the latest. Love, Bob

Alice: 9
Bob: 11
SeqNo: 1
Signed Alice
Signed Bob

Alice: 7
Bob: 13
SeqNo: 2
Signed Alice
Signed Bob

Alice: 16
Bob: 4
SeqNo: 1000
Signed Alice
Signed Bob

Balance: 16
Balance: 4
Payment channel - Solution

Alice: 10
Bob: 10

Alice: 9
Bob: 11
SeqNo: 1
Signed Alice
Signed Bob

Alice: 7
Bob: 13
SeqNo: 2
Signed Alice
Signed Bob

Alice: 16
Bob: 4
SeqNo: 1000
Signed Alice
Signed Bob

Bob said SeqNo 2 is the latest. I’ll wait T seconds for Alice
Payment channel - Solution

Ethereum

Smart contract

Alice: 10
Bob: 10

Bob is a liar. Here's the latest. Love, Alice

Alice: 9
Bob: 11
SeqNo: 1
Signed Alice
Signed Bob

Alice: 7
Bob: 13
SeqNo: 2
Signed Alice
Signed Bob

Alice: 16
Bob: 4
SeqNo: 1000
Signed Alice
Signed Bob

Balance: 16
Balance: 4
Payment channel - Solution

Smart contract

Alice: 16
Bob: 4

SeqNo 1000 is latest. Pay out 16 to Alice, 4 to Bob.

Alice: 9
Bob: 11
SeqNo: 1
Signed Alice
Signed Bob

Alice: 7
Bob: 13
SeqNo: 2
Signed Alice
Signed Bob

...
Payment channel

- Instant confirmation: as soon as both parties sign
- 2 blockchain transactions per channel: open & close
  - Virtually unlimited # off-chain transactions
- Security
  - Rebuttal period T is important
  - Parties are rational
- Only does payment
Agenda

1. Overview
2. Payment channel
3. **State channel**
4. Plasma
5. Discussion
State channel - Problem

- Generalize payment channel for any joint computation:
  - Example: Alice and Bob want to play chess on the blockchain!

- Strawman:
  - A contract to encode the rule and current state of the game
  - Player takes turn to send transactions

- Problems:
  - Take too long
    - Longest official chess game takes 286 moves (20h 15m)
  - Expensive
State channel - Solution

- Setup

**Reward:** 20

**State:**

- Etherum (Deposit 10, Signed Alice)
- Etherum (Deposit 10, Signed Bob)

*Can only decide with BOTH signatures*
State channel - Solution

- First move

Can only decide with BOTH signatures

Ethereum

Reward: 20
State:

Signed Alice
Signed Bob

f4
State channel - Solution

- Many moves later

Reward: 20
State: Etherum

Can only decide with BOTH signatures

Reward: 20
SeqNo: 1
State: Signed Alice
Signed Bob

Reward: 20
SeqNo: 2
State: Signed Alice
Signed Bob

Reward: 20
SeqNo: 100
State: Signed Alice
Signed Bob
State channel - Solution

Etherum

Reward: 20
State:

This is the latest. Love, Bob

Reward: 20
SeqNo: 1
State:
Signed Alice
Signed Bob

Reward: 20
SeqNo: 2
State:
Signed Alice
Signed Bob

Reward: 20
SeqNo: 100
State:
Signed Alice
Signed Bob
State channel - Solution

Bob said latest SeqNo=2. I'll wait T seconds for Alice.
State channel - Solution

Bob lied. Here’s the latest state. Love, Alice
State channel - Solution

Alice won at SeqNo=100. Pay out 20ETH to Alice.
State channel

- Ad-hoc state channel: one channel per game
  - Smart contract encoding rule + how to decide on final outcomes
  - Players sign the latest state off-chain

- Generalized state channel:
  - General channel (smart contract) that allow creating ad-hoc channel
    - Using another smart contract as contract registry
  - Counterfactual.com
State channel

- Huge implication to security:
  - Solve the fair secure multi-party computation (MPC) problem, which is impossible without blockchain

- Active research (security):
  - Virtual channels
  - Outsourcing: blockchain watchers

- Assumed:
  - Fixed set of participants
  - Rational players
Agenda

1. Overview
2. Payment channel
3. State channel
4. **Plasma**
5. Discussion
Plasma

- **Problem with State Channels**
  - All players must participate
    - Abort = expensive

- **Building block 1: sidechain**
  - Application-specific blockchain can be a separate blockchain
  - e.g. Cryptokitties and ICOs have their own chains
  - Decision by consensus -> don’t need everyone to participate
Plasma - Sidechain 101

- Early idea, by *Blockstream*: pegged side chain
  - For experimental design
  - Burn coin from one chain to generate coin on another
  - Sidechain is independent of main chain
    - e.g. can run PBFT consensus
Plasma - Sidechain 101

- Federated sidechain:
  - Coins moving both ways
  - A set of validators are members of both chains
  - Still, two chains are independent

![Diagram showing main chain and sidechain connected by validators](image-url)
Plasma

- Plasma = sidechain without federation of validators
- Then how to ensure security in the sidechain?
- Building block 2: TrueBit
Plasma - TrueBit 101

- Setting: outsourced computation on blockchain (!?)
  - e.g. sorting, matrix multiplication
- Problem: minimizing verification cost when given a solution
  - Benefit: same throughput, but for expensive computations
Plasma - TrueBit 101

- TrueBit is a smart contract implementing a verification game

Matrix multiplication

1. Task
2. Verification game
3. Reward

Ethereum

Some deposit

Reward
Plasma - TrueBit 101

- TrueBit is a smart contract implementing a verification game

```
1. Task
2. Verification game
3. Reward
```

Matrix multiplication

Ethereum

Matrix C
Plasma - TrueBit 101

- TrueBit is a smart contract implementing a verification game

Bob said solution is C. I’ll wait for any challenge.

C is wrong. Here’s an example $c_{ij}$
Plasma - TrueBit 101

- TrueBit is a smart contract implementing a verification game

1. Task
2. Verification game
3. Reward

C is wrong. Here’s an example c_ij

Challenge checks out. Penalize Bob! Reward Chris

Etherum
Plasma - TrueBit

● TrueBit-compatible tasks:
  ○ Verification is cheaper than execution
  ○ What tasks satisfy it is not clear!

● Key challenge
  ○ Incentivize Challenger -> intentionally post *wrong solutions*.

● How Plasma uses TrueBit?
  ○ Task = sidechain application logic
  ○ Verification game if any user detects wrong-doing in the sidechain
Agenda

1. Overview
2. Payment channel
3. State channel
4. Plasma
5. Discussion
Discussion

- None of these solutions are deployed on the main-net
  - Security of state channels are well understood
  - Not so for Plasma
- Reasonable assumptions?
  - Rational parties, incentivized by money
  - Synchronous network (bounded delay on any blockchain requests)
- Plasma:
  - Not clear if any sidechain can be supported (what types of computation CAN Truebit support?)
  - Lack too much details to judge
Discussion

- So far, no experimental results
  - Small scale simulations show Lightnight networks few times better
- Cryptocurrencies-based applications only

- Good for us?
  - Yes, for Forkbase
- Possible in permissioned settings?
  - Payment channel? Yes
  - State channel? Yes (auctions)
  - Plasma? Not sure, can just run multiple instances of Hyperledger