Fast and Furious Withdrawals from Optimistic Rollups

Mahsa Moosavi
OffchainLabs - Concordia University
WHOAMI

- Mahsa Moosavi
- PhD Candidate @Concordia University, Montreal, Canada
- Integration Engineer @OffchainLabs

mahsamoosavi.com
Why is Ethereum slow and expensive?
Scalability

Method(x)
Method(x) → Return z

Scalability
Method(x)

Scalability
Method(x)

Relay to all nodes

Scalability
Scalability
All agree on $z$

Return $z$
Why does every node compute?

- Consensus on the *correct* output
- Computing it for yourself is the most straightforward way to know it is *correct*
- But can you be convinced something is correct without computing it?
Why does every node compute?

- You could be given a mathematical proof it is correct
  - Checking a proof of an output needs to be less work than computing the output
  - ZK-Rollups
Method(x)

Proof p: \( z = \text{method}(x) \)

ZK-Rollup
Proof $p: \{z=\text{method()}x\}$
Why does every node compute?

- You could be given a mathematical proof it is correct
  - Checking a proof of an output needs to be less work than computing the output
  - ZK-Rollups

- Someone can assert an output and stake a large amount of money
  - Anyone can dispute but also needs to stake
  - If no disputes after a week, it is considered **correct**
  - If disputes; parties pinpoint the disagreement, ask all nodes to compute it
  - Optimistic-Rollups
Method(x)

STAKE: \{z=\text{method}(x)\}

Optimistic-Rollup
“I want method(x) executed in ArbOS”
Ethereum (Layer 1)

ArbOS (Layer 2)

“I want method(x) executed in ArbOS”
"I want method(x) executed in ArbOS"
"I want method(x) executed in ArbOS"

WAIT 7 DAYS FOR DISPUTES
"I want to withdraw 100 ETH from L2"
"I want to withdraw 100 ETH from L2"
“I want to withdraw 100 ETH from L2”
“I want to withdraw 100 ETH from L2”
In assertion #20, I withdrew 100 ETH
100 ETH

Escrow: 100 ETH

Ethereum (Layer 1)

ArbOS (Layer 2)

Inbox

Outbox

Bridge

Contents

Assertion Of ArbOS State

Executes

100 ETH
Withdrawal Speed

- Withdrawals have to wait 7 days for finality
- Could be longer: disputes extend the window
  
  ! Note: There have been no dispute ever, but they are not impossible
- 7 days is arbitrary but there needs to be some time window
Withdrawal Speed

- Withdrawals have to wait 7 days for finality
- Could be longer: disputes extend the window

Note: There have been no dispute ever, but they are not impossible

- 7 days is arbitrary but there needs to be some time window

Interesting

Anyone running a validator (checking the inbox transactions do result in the assertion) is 100% sure the ETH will be available
Can Alice withdraw $100 \text{ETH}_{(L2)}$ from Arbitrum in less than 7 days?
Can Alice withdraw 100 ETH\textsubscript{(L2)} from Arbitrum in less than 7 days?

Solution #1

- Alice goes to a centralized exchange and trades 100 ETH\textsubscript{(L2)} for 100 ETH

- It’s centralized
Can Alice withdraw $100 \text{ ETH}_{(L2)}$ from Arbitrum in less than 7 days?

Solution #2

- Alice has $100 \text{ ETH}_{(L2)}$ - Bob has $100 \text{ ETH}$
- Atomic Swap

- It does not finalize
Can Alice withdraw 100 ETH\(_{(L2)}\) from Arbitrum in less than 7 days?

Solution #3

- Alice does the withdrawal and while it is pending, the outbox gives her a “ticket” for the withdrawal on L1
- Bob validates Arbitrum assertion, knows ticket is valid, and buys it from Alice for 99 ETH
- Bob has a dual role: has liquidity (has 100 ETH on L1) and is a validator
- Bob is scarce
A prediction market is setup for the “the 10th assertion will become finalized” on L1.

For 1 ETH, you can buy a share for “YES” and a share for “NO” and resell them.

If it becomes valid, a “YES” share can be redeemed for 1 ETH and a “NO” share is worth nothing.

If it does not become valid, a “YES” share is worth nothing and a “NO” share is worth 1 ETH.

Can Alice withdraw 100 ETH\(_{(L2)}\) from Arbitrum in less than 7 days?
Can Alice withdraw 100 ETH\(_{(L2)}\) from Arbitrum in less than 7 days?

- Alice deposits 100 ETH for 100 “YES” and 100 “NO” shares
- Alice sells to David (who runs a validator): 100 “YES” shares for 0.99 ETH each
- Alice sells to Carol (who has liquidity): 1 ticket for 100 ETH & 100 “NO” shares

If assertion is valid: 100 ETH can be withdrawn and “NO” shares are worth nothing

If assertion is invalid: ETH cannot be withdrawn but “NO” shares are worth 100 ETH
Implementation

- Modified Arbitrum Nitro to support solutions and provide measurements
  - Solution #3:
    - Implemented an L1 market
    - Modified the Outbox
  - Solution #4:
    - Modified the Rollup and Outbox contracts
Implementation

1. Alice withdraws 100 ETH from her Outbox.
2. The transaction is processed through the Bridge.
3. The funds are sent to her Inbox.
4. The funds are then transferred to the Market.
Implementation

1. Alice withdraws 100 ETH from her inbox.
2. She transfers funds to the bridge.
3. The funds are transferred to the outbox.
4. The outbox transfers the funds to the market address.

Diagram:
- Alice
- Inbox
- Bridge
- Outbox
- Market

Function call: `transferSpender(exit #10, Market address)`
Implementation

1. **withdraw 100 ETH**
   - Inbox
   - Bridge

2. **transferSpender(exit #10, Market address)**
   - Outbox

3. **openMarket(exit #10, askPrice: 99)**
   - Market
Our implementation consists of the following steps:

1. Alice withdraws 100 ETH from her wallet.
2. Alice transfers the 100 ETH to the Bridge.
3. Alice opens a market with an ask price of 99.

This process allows for the exchange of assets between Alice and Bob through the Bridge.
Implementation

1. withdraw 100 ETH
2. transferSpender(exit #10, Market address)
3. openMarket(exit #10, askPrice: 99)
4. submitBid(BidPrice: 99.1)
5. transferSpender(exit #10, Bob)

Bob

Alice

99.1 ETH

99.1 ETH

Market

Bridge

Outbox

Inbox
Implementation

**1. withdraw 100 ETH**

**2. transferSpender(exit #10, Market address)**

**3. openMarket(exit #10, askPrice: 99)**

**4. submitBid(BidPrice: 99.1)**

**5. transferSpender(exit #10, Bob)**
**Implementation**

1. **Alice** withdraws 100 ETH.
2. **Alice** transfers 100 ETH to the **Outbox**.
3. **Alice** opens a market with an ask price of 99.
4. **Alice** submits a bid of 99.1 to the **Market**.
5. **Alice** transfers 99.1 ETH to the **Bridge**.
6. **Alice** executes the transaction.
7. **Bob** receives 100 ETH.
8. **Bob** transfers 100 ETH to the **Bridge**.
9. **Bob** transfers 100 ETH to the **Outbox**.
10. **Bob** transfers 100 ETH to the **Inbox**.
11. **Bob** transfers 99.1 ETH to the **Market**.
12. **Bob** transfers 99.1 ETH to the **Outbox**.
1. withdraw 100 ETH
2. transferSpender(exit #10, Market address) - gasUsed: 86,701
3. openMarket(exit #10, askPrice: 99)
4. submitBid(BidPrice: 99.1)
5. transferSpender(exit #10, Bob)
6. executeTransaction(exit #10)

Measurements:
gasUsed: 86,701

Transaction Details:
- Alice withdraws 100 ETH
- Gas used: 86,701
- Bob opens a market with askPrice: 99
- Alice submits a bid of 99.1 ETH
- Gas used: 86,701

Alice receives 99.1 ETH
Bob receives 100 ETH

Total gas used: 86,701
withdraw 100 ETH

openMarket(exit #10, askPrice: 99)

submitBid(BidPrice: 99.1)

transferSpender(exit #10, Market address)

executeTransaction(exit #10)

transferSpender(exit #10, Bob)

gasUsed: 328,029

Alice

Bob

100 ETH

Measurements
Inbox

Market

Outbox

Bridge

Alice

Bob

withdraw 100 ETH

transferSpender(exit #10, Market address)

1

3

openMarket(exit #10, askPrice: 99)

2

4

submitBid(BidPrice: 99.1)

5

executeTransaction(exit #10)

6

100 ETH

100 ETH

99.1 ETH

99.1 ETH

Measurements

gasUsed: 105,287
Inbox

Market

Outbox

Bridge

Bob

Alice

withdraw 100 ETH

1

2

transferspender(exit #10, Market address)

3

openMarket(exit #10, askPrice: 99)

4

executeTransactino(exit #10)

gasUsed: 92,148

5

transferspender(exit #10, Bob)

6

submitBid(BidPrice: 99.1)

100 ETH

99.1 ETH

99.1 ETH

Measurements

gasUsed: 92,148
Thank you!

Mahsa Moosavi
Integration Engineer @OffchainLabs
PhD Candidate @Concordia University

@mvs_mahsa
Enter your slide title here.

Your subtitle here.

Your Name

Your title, your organization
Section 1

Section 1 title here.
Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula
Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Section 1 details with a main point.
Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.
Section 2

Section 2 title here.
Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Section 2 details with a main point.
Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.
Enter your main point / statement here.
Here’s the timeline.

Event 1
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.
Thank you!

Your Name
Your title, your organization
email@emailaddress.com
@twitterhandle