Sealed-Bid Blockchain Auctions using Flash Freezing Flash Boys (F3B)

by Michael Gysel

Thesis Advisor

Professor Bryan Ford

Thesis Supervisor

Haoqian Zhang

Table of Contents

What is a sealed-bid auction?

Photo by MDEXEC1

1. Bidders submit secret bids during bidding period
2. Wait for bidding period to finish
3. Open bids and declare highest bidder winner

Past research on sealed-bid blockchain auctions

BID PERIOD

- Bidders commit to bid transaction
- Bidders make deposit at least as large as bid

REVEAL PERIOD

- Bidders make reveal transaction

END OF AUCTION

- Highest bidder selected winner
- Lower bidders refunded

Drawbacks: Requires two transactions and a deposit

Table of Contents

Desired Sealed-Bid Blockchain Auction Properties

Implement a sealed-bid blockchain auction with the following properties:

1. One transaction latency: Guarantees that each bidder is required to submit only one transaction.
2. No deposit: Guarantees that bidders do not submit a deposit.
3. Sealed-bid: Guarantees each bid is kept secret from all other bidders during the bidding period.
4. Fund binding: This guarantees the winning bidder purchases the asset.

Research Goals

Goal 1 (Traditional Auction)

Implement a traditional sealed-bid blockchain auction

Goal 2 (F3B Auction)

Implement a sealed-bid blockchain auction with:

1. One transaction latency
2. No deposit
3. Sealed-bid
4. Fund binding

Goal 3 (Evaluation)

Qualitative and Quantitative Evaluation of both auctions

Table of Contents

Traditional Sealed-Bid Auction Architecture

Latency

- One bid tx
- One reveal tx

Deposit

- All bidders make deposit

Sealed-Bid

Fund Binding

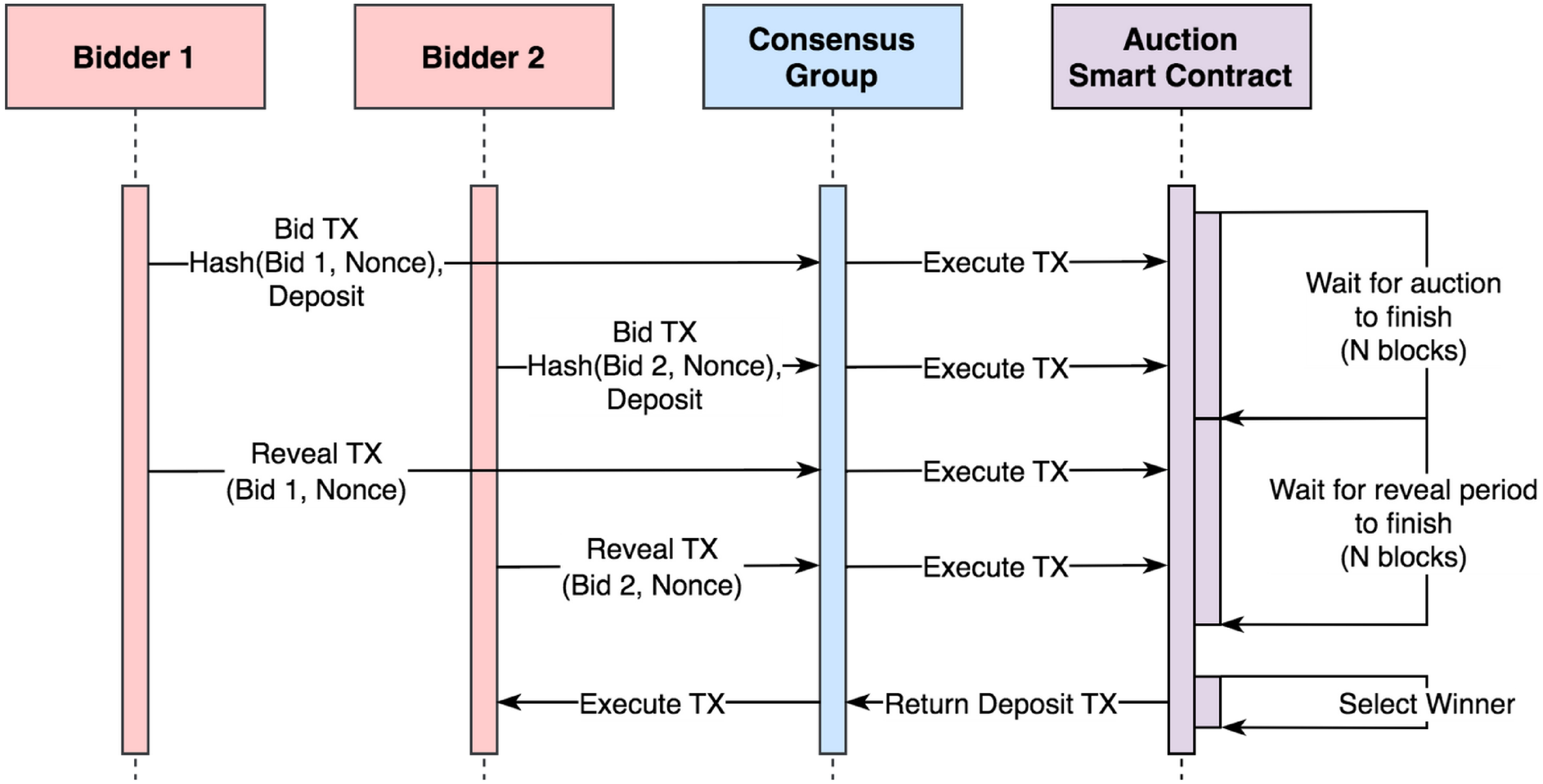


Figure 1: Architecture of Traditional Sealed-Bid Blockchain Auction

Traditional Sealed-Bid Auction Implementation

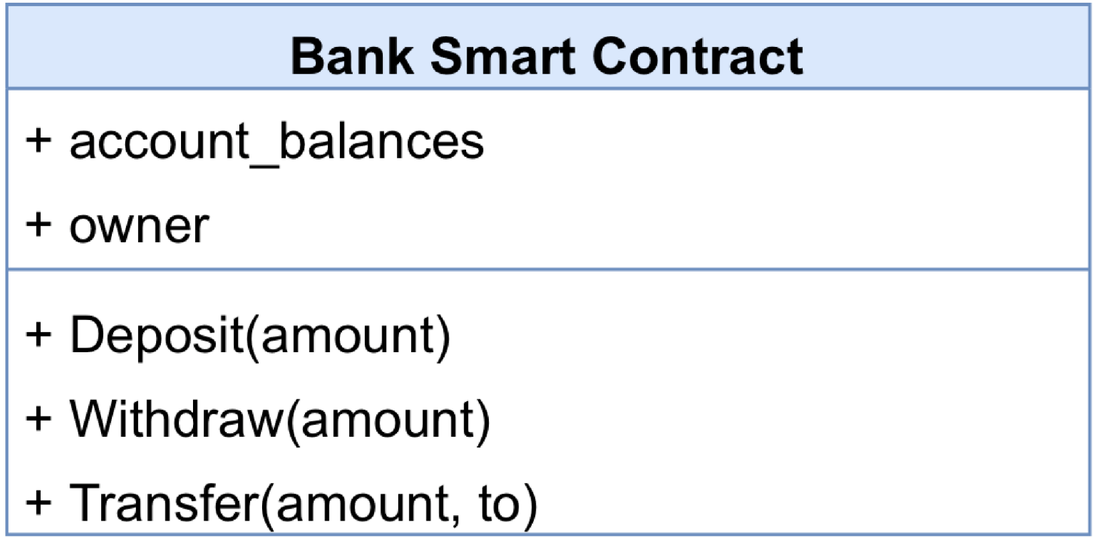


Figure 2: Bank Smart Contract Class Diagram

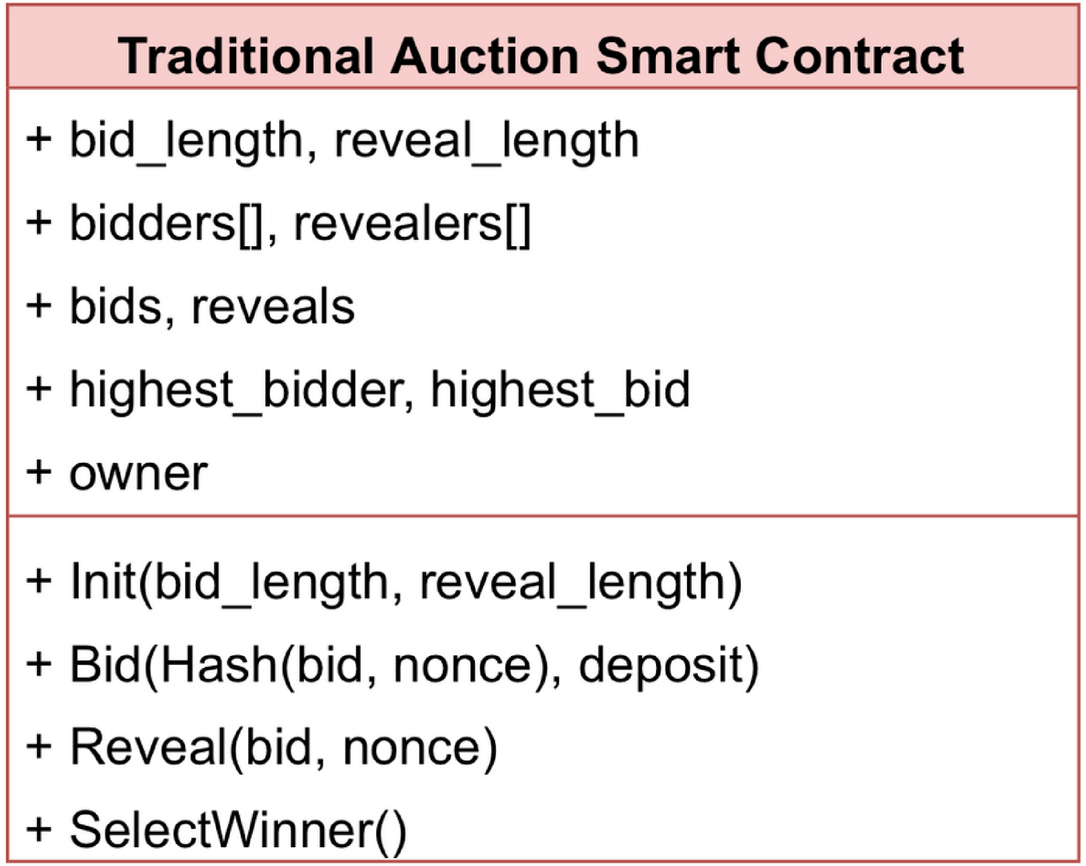


Figure 3: Traditional Auction Smart Contract Class Diagram

Table of Contents

What is Flash Freezing Flash Boys (F3B)?

F3B Allows for

- Encrypted Transactions
- Delayed Execution

Secret Management Committee

- Committee of trustees
- Reveal decryption key shares after a delay

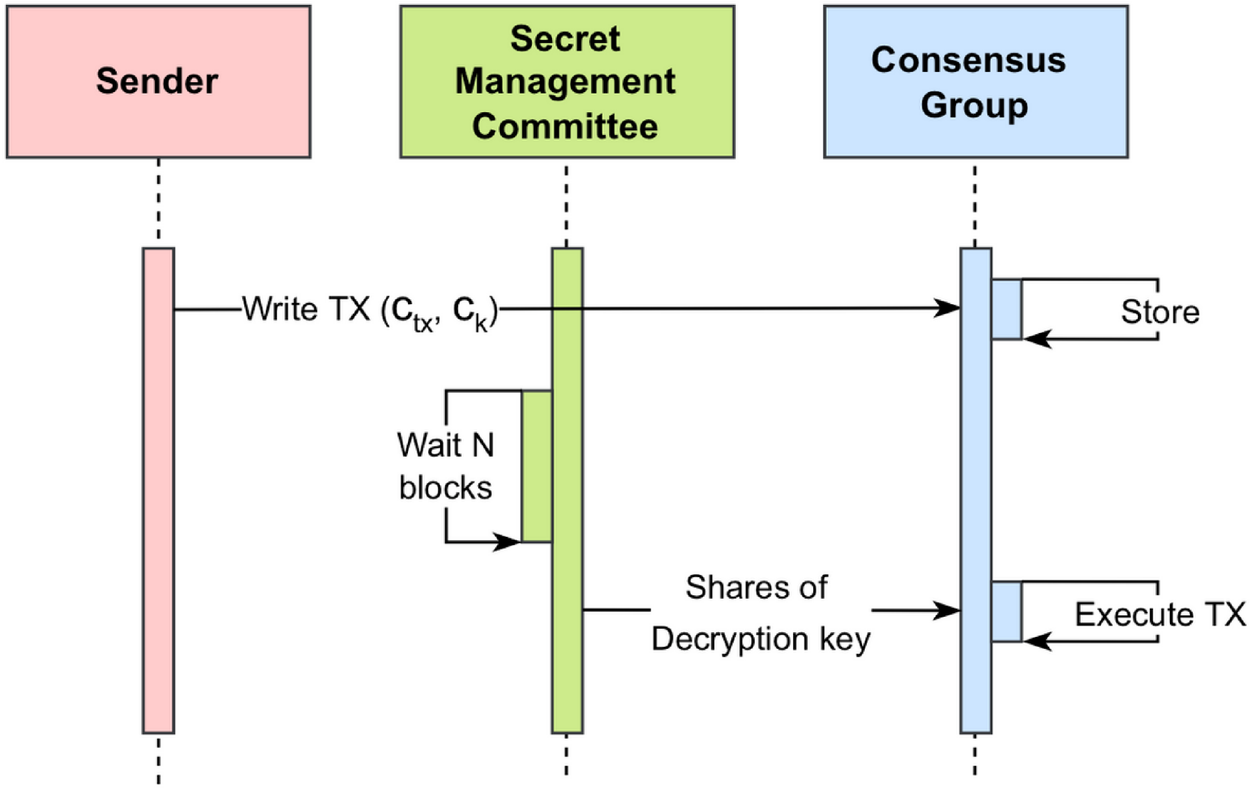


Figure 4: F3B Architecture

F3B Auction Architecture

Latency

- One bid transaction

Deposit

- Low bidders immediately refunded

Sealed-Bid

Fund Binding

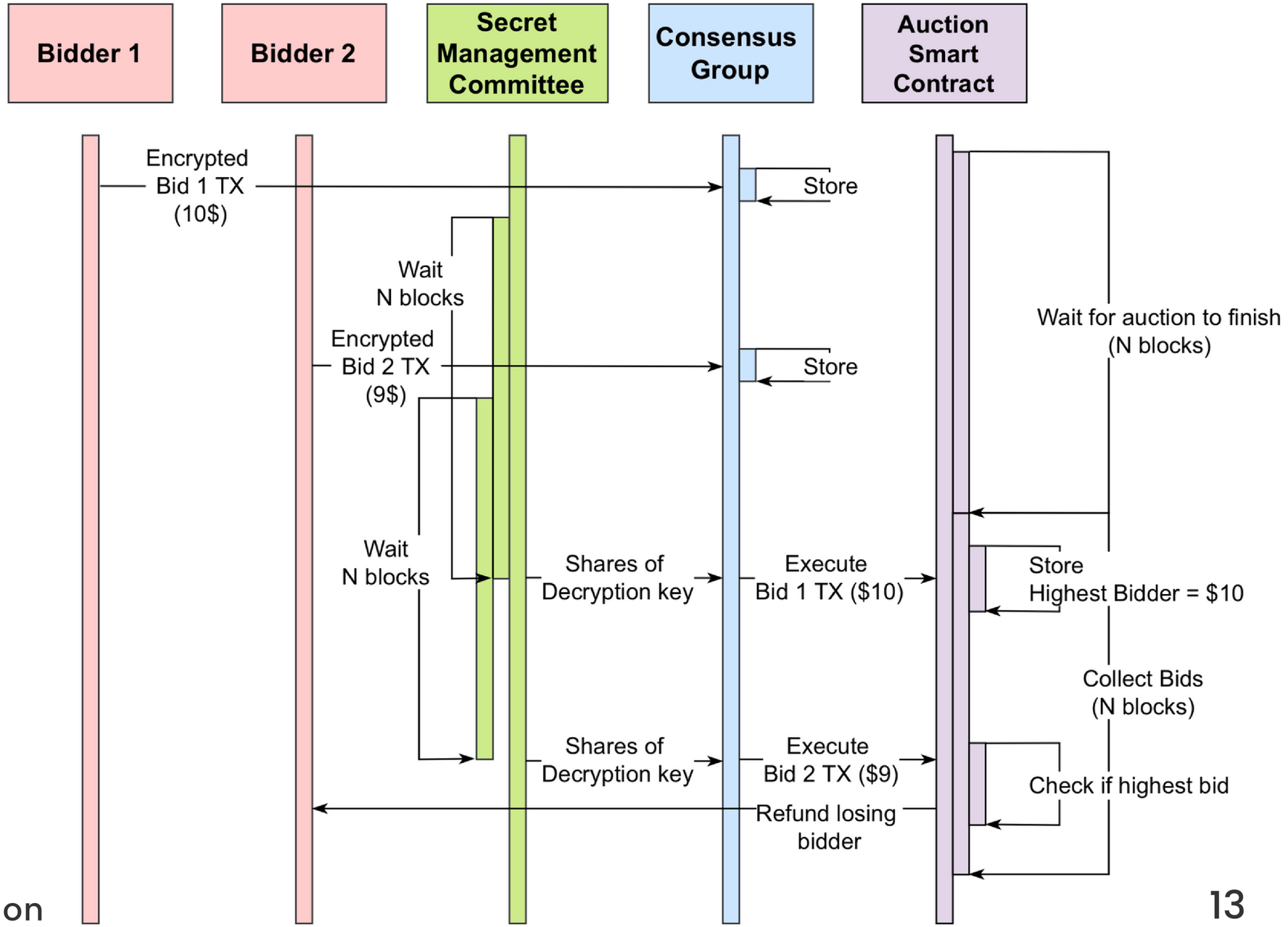


Figure 5: Architecture of F3B Sealed-Bid Blockchain Auction

F3B Sealed-Bid Auction Implementation

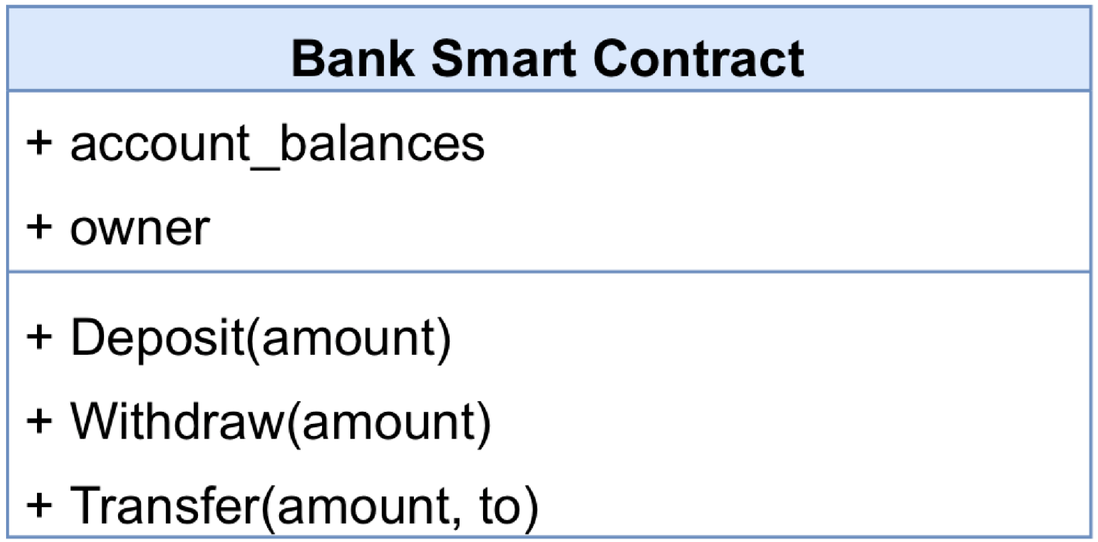


Figure 6: Bank Smart Contract Class Diagram

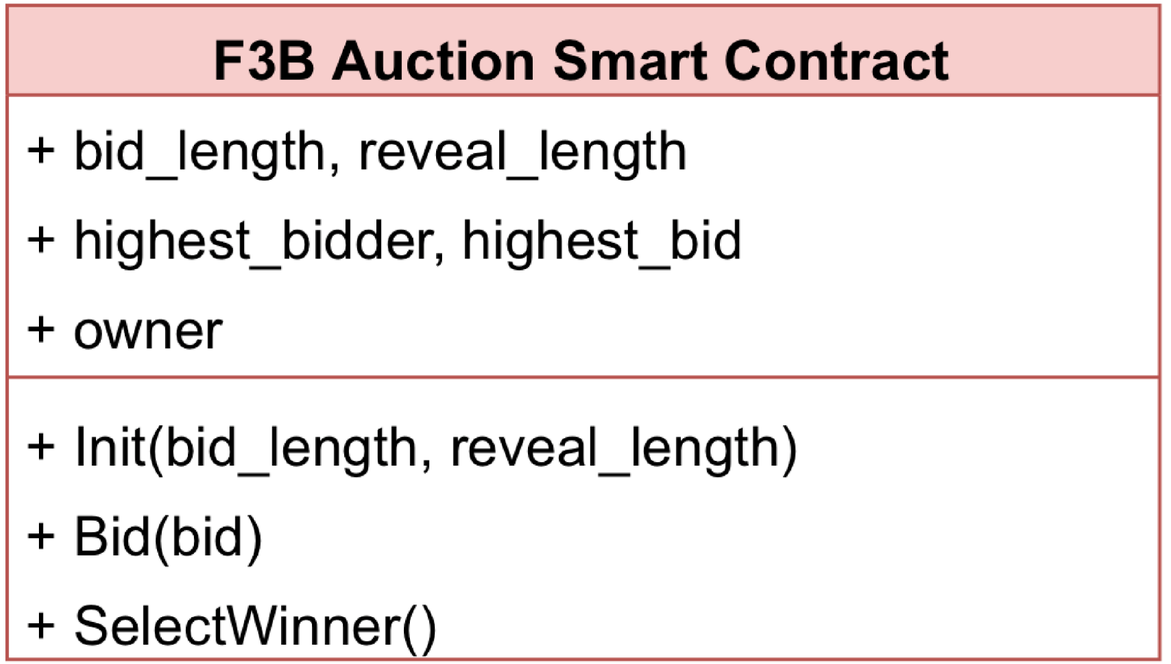


Figure 7: F3B Auction
Smart Contract Class Diagram

F3B Integration

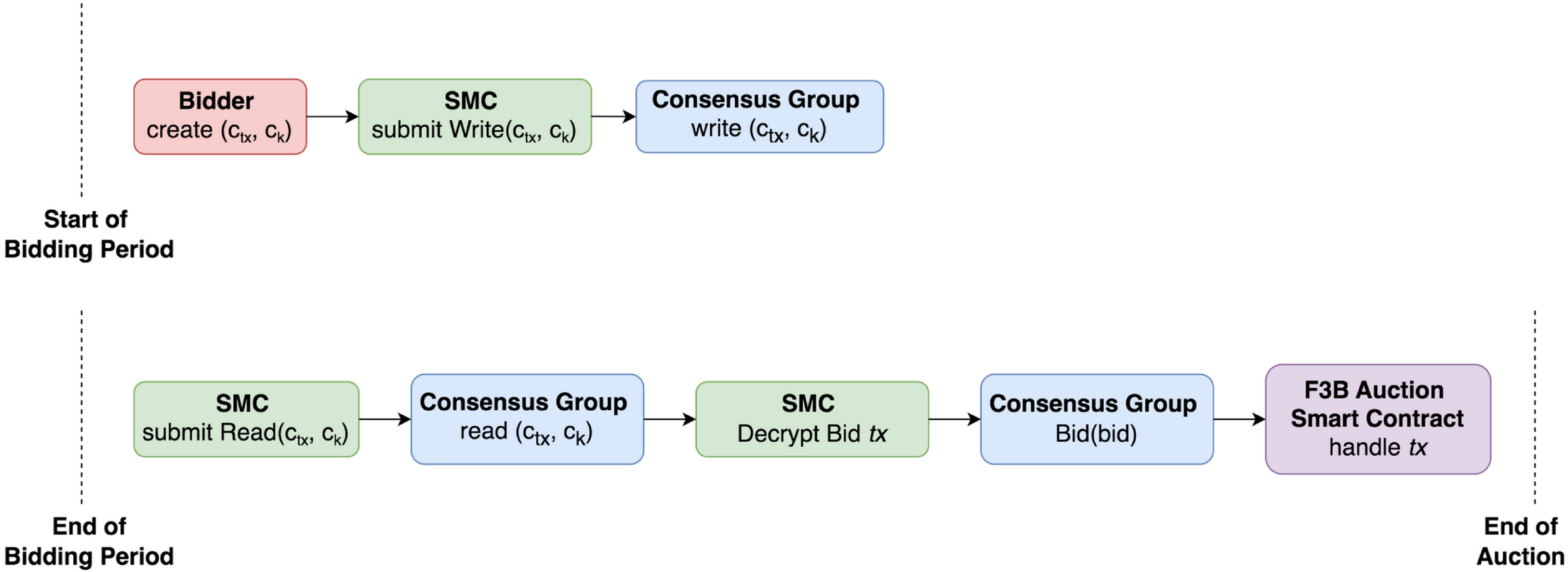


Figure 8: Flow of F3B Auction Transaction

Table of Contents

Qualitative Evaluation

	TRADITIONAL AUCTION	F3B AUCTION
Sealed-bid	✓	✓
Fund binding	✓	✓
One transaction latency		✓
No deposit		✓

Table 1: Design Properties of Traditional and F3B Auctions

Quantitative Evaluation

1. Storage
2. Throughput
3. Auction Runtime

Evaluation Used:

- Macbook Pro with a 2.2GHz Intel core i7 processor
- 3 Dela Nodes

Storage Requirements

Storage significantly lower for F3B Auction

NUMBER OF BIDS	TRADITIONAL AUCTION (BYTES)	F3B AUCTION (BYTES)
10	3,148	260
50	14,668	260
100	29,068	260

Table 2: Storage vs Number of Bids for Traditional and F3B Auctions

Throughput

Throughput significantly greater for Traditional Auction

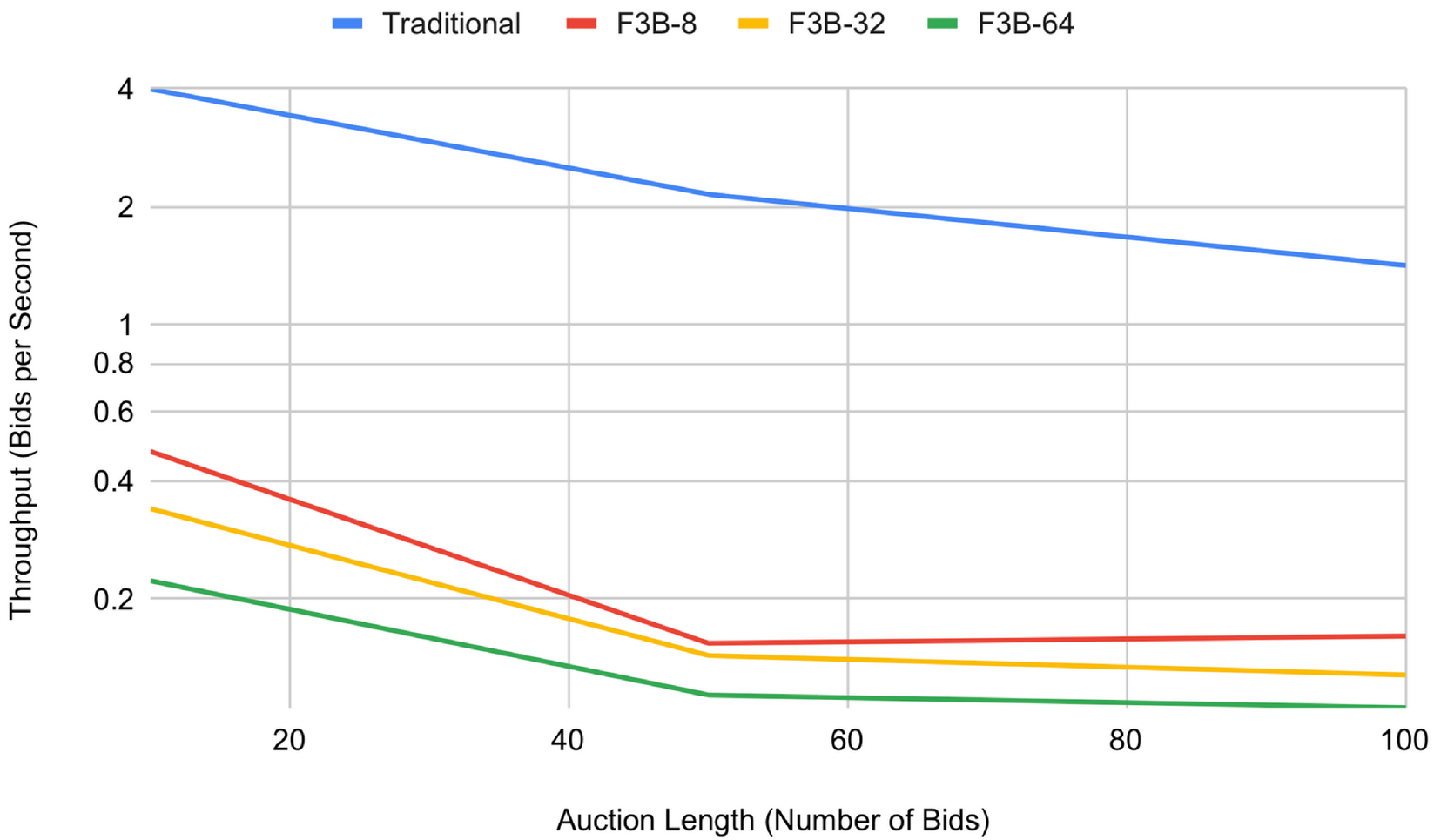


Figure 9: Auction Length vs Throughput of Traditional and F3B Auctions

Auction Runtime

Runtime significantly lower for Traditional Auction

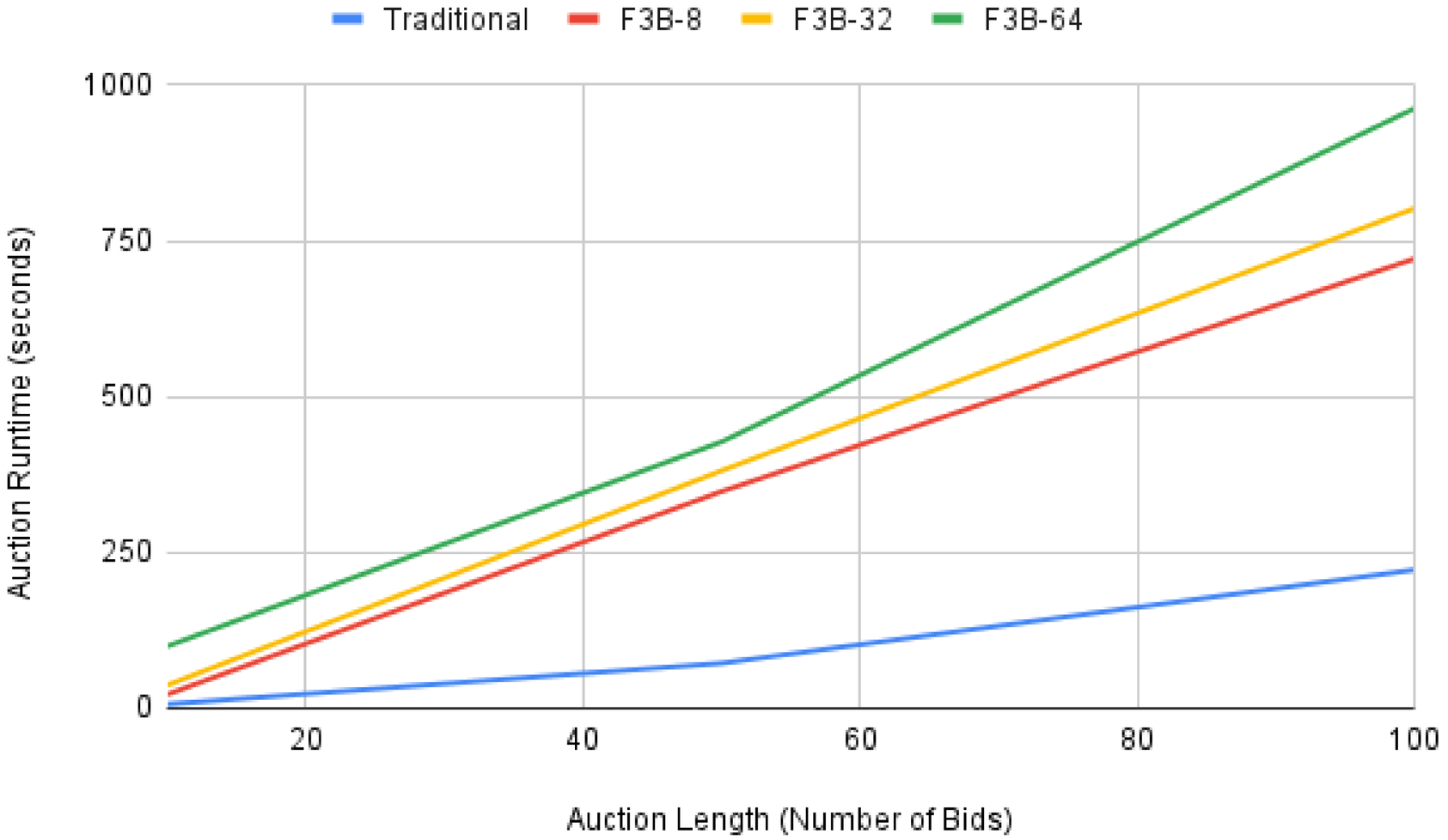


Figure 10: Auction Length vs Auction Runtime of Traditional and F3B Auctions

Table of Contents

Demo

Table of Contents

Conclusion

F3B Auction Advantages

- One transaction latency
- No deposit
- Low storage

F3B Auction Drawbacks

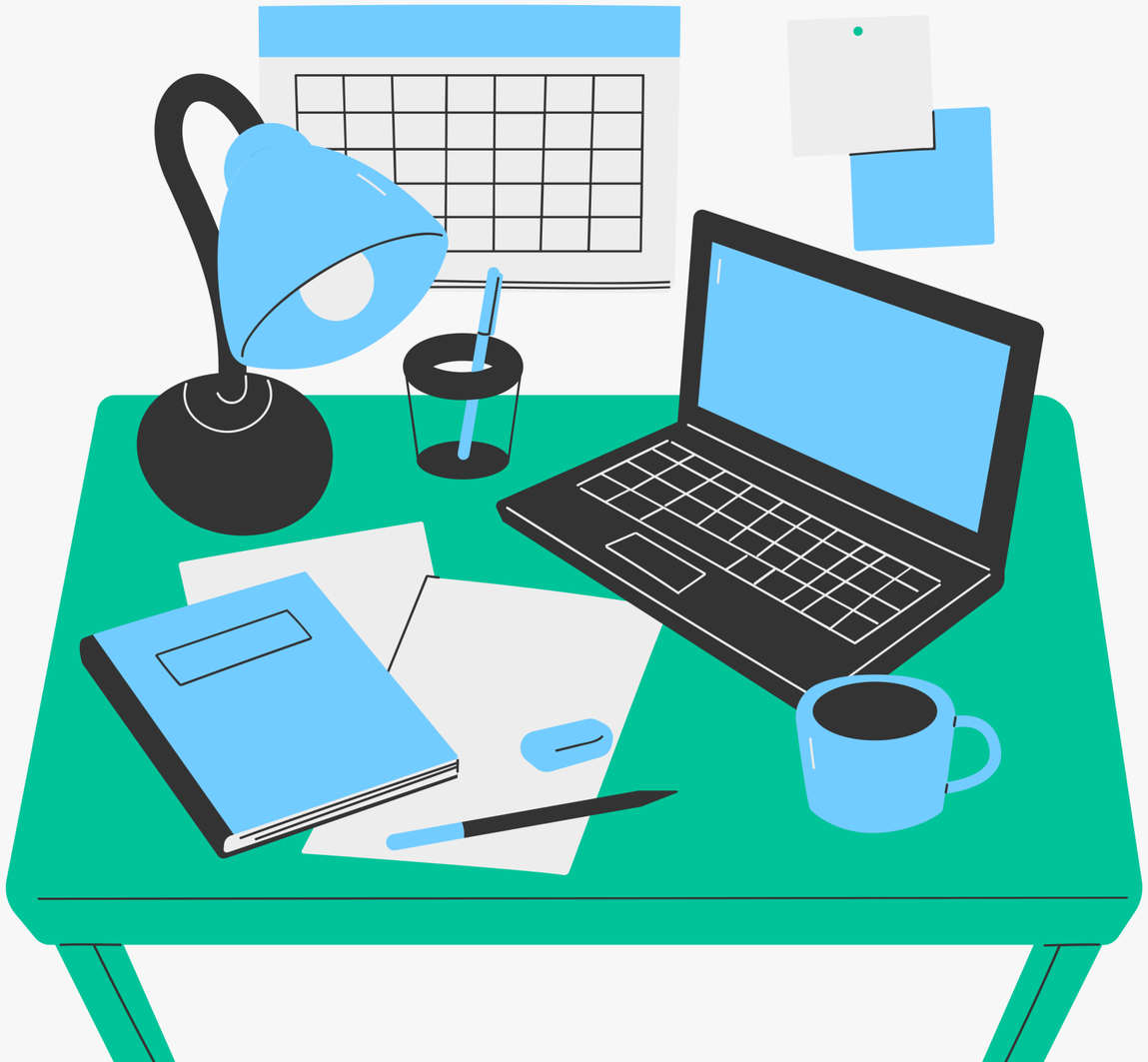
- Low throughput
- High auction runtime

Thank you for listening! Questions?

Table of Contents

- **Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit**
- **Sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt**

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.



Title

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.

Title

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.

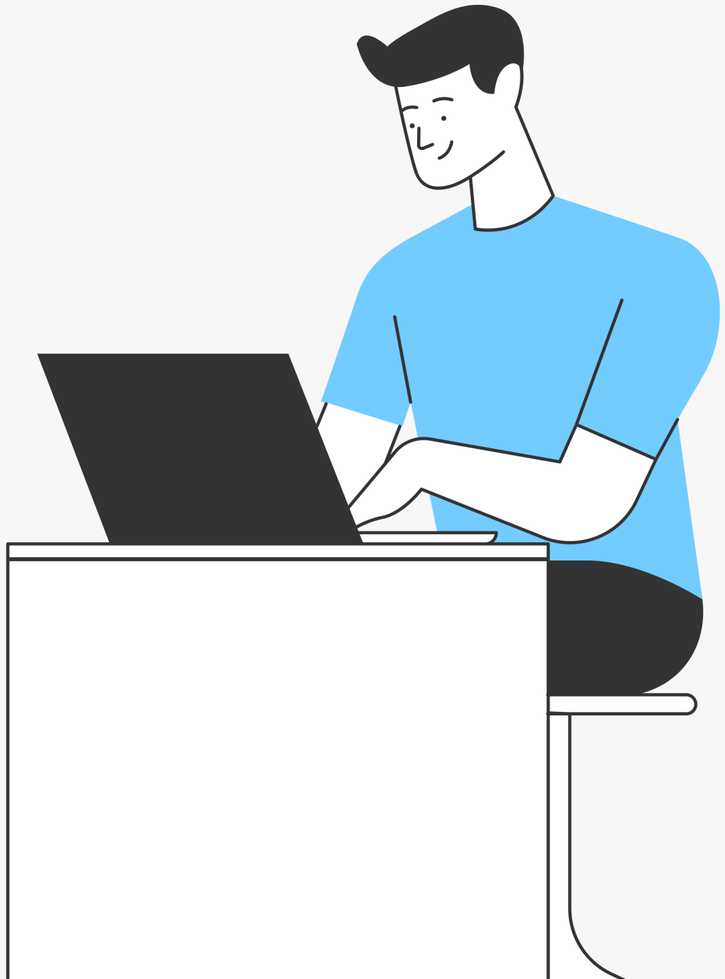
Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt

Hypothesis 1

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

- 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.

- 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.



Hypothesis 2

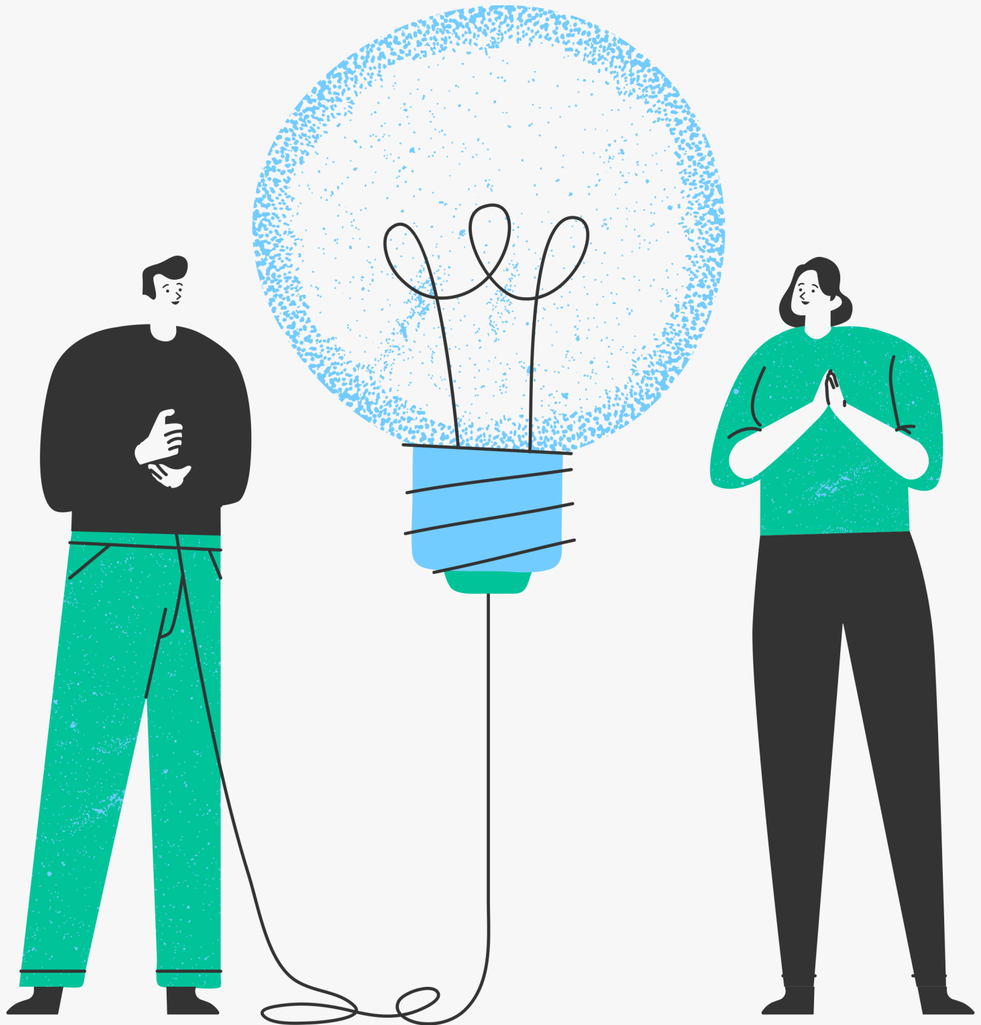
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- 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.
- 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.

Hypothesis 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt.

- 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.



III Methodology

Method

Survey

Location

City, Country

Collected Sample

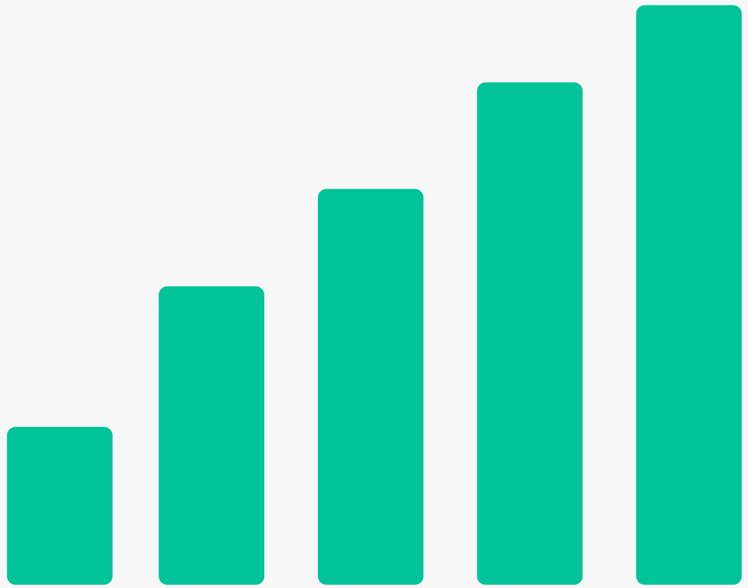
300 completed survey

Duration

2021 January -December

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.

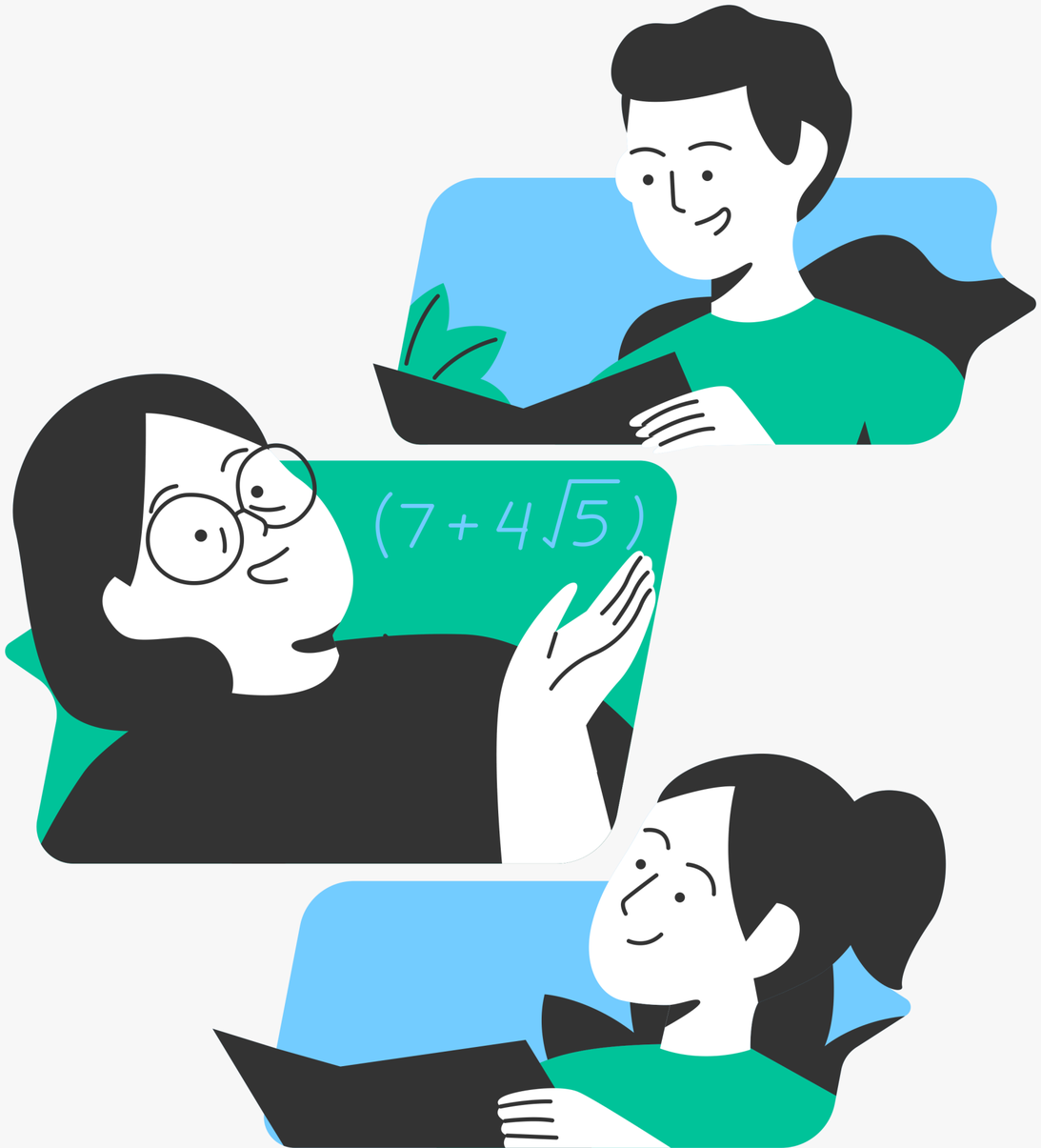
Bar Chart



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

Pie Chart

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



Title

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

Title

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

Title

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

Title

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

Title

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

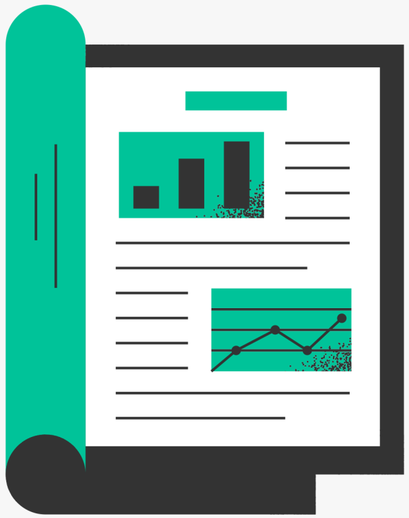
Title

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

V Conclusion & Discussions

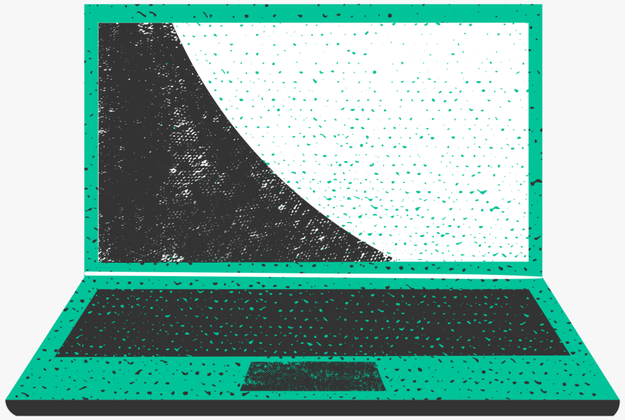
Title

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



Title

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



Title

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

Day, Date

Department, University

ADVISOR

Name

STUDENT

Name
Student ID

Thank you for listening!