École Polytechnique Fédérale de Lausanne

Sealed-Bid Blockchain Auctions using Flash Freezing Flash Boys

by Michael Gysel

Master Project Report

Prof. Bryan Ford
Thesis Advisor

Haoqian Zhang
Thesis Supervisor

EPFL IC IINFCOM DEDIS
BC 160 (Bâtiment BC)
Station 14
CH-1015 Lausanne

September 30, 2023

Contents

Chapter 1

Introduction

Auctions are a significant component of the global economy, with the three leading auction houses earning US$12.6B annually [2]. Furthermore, online auctions account for an increasing percentage of auction sales at $5B in revenue annually [13]. The most common auction forms are open-bid auctions and sealed-bid auctions. In open-bid auctions, bids are transparent and bidders actively compete against one another until the highest bidder is selected [1]. In sealed-bid auctions however, all bidders submit secret bids during the bidding period. When the bidding period is complete, the bids are unsealed and the highest bidder is declared the winner [10]. Arguably the greatest advantage of sealed-bid auctions results from the sealing of bids stifling active competition. This prevents collusion between bidders and incentivizes bidders to bid their valuation of the asset [7].

The implementation of sealed-bid auctions on blockchains presents challenges because bids must be kept secret while blockchain transactions are transparent. Thus, a bid submitted in the form of a transaction would be viewable to all bidders, making it an unsealed bid.

Numerous blockchain sealed-bid auction protocols have been proposed to resolve this issue. These proposals rely on a commit-reveal scheme, where bidders commit to a bid during the bidding period and reveal their bid when the bidding period is complete. [9, 11] propose a commit transaction that includes a small deposit, a reveal transaction, and a purchase transaction from the winning bidder. The small deposit is confiscated if the winning bidder does not submit the purchase transaction in order to disincentivize such behavior. However, [9, 11] require three transactions from the winning bidder, two transactions from all losing bidders, and do not require the winning bidder purchase the asset. [3–6, 14, 15] propose a commit transaction that includes a deposit at least as large as the bid itself and a reveal transaction. However, these proposals require two transactions for all bidders, reduce the liquidity of losing bidders, and do not entirely mask the bid price of all bidders. Furthermore, bidders are left with the option of increasing their deposit, which obscures their bid price and reduces their liquidity, or decreasing their deposit, which exposes their bid price and improves their liquidity.

Given the drawbacks of these previous proposals, the purpose of this paper is to implement a sealed-bid blockchain auction with the following properties:

- sealed-bid: This guarantees each bid is kept secret from all other bidders during the bidding period.
- fund binding: This guarantees the winning bidder purchases the asset.
- one transaction latency: This guarantees that each bidder is required to submit only one transaction.
- no deposit: This guarantees that bidders do not submit a deposit.

This paper proposes a sealed-bid blockchain auction with these properties on EPFL Decentralized and Distributed Systems Laboratory's Dela blockchain utilizing Flash Freezing Flash Boys (F3B) [8, 16]. F3B relies on a commit-reveal scheme that enables encrypted bid transactions and delayed execution. First, bidders submit encrypted bid transactions to a secret-management committee during the bidding period. When the bidding period is complete, the secret-management committee decrypts the bid transactions and submits them to the consensus group where they are executed. Finally, an auction smart contract receives these bid transactions and determines the winner. Notably, the auction smart contract only accepts payment from the highest bidder and immediately refunds the previously highest bidder.

A prototype of this protocol and the traditional deposit protocol were both implemented in Go and the results compared. These will be referred to as the traditional and F3B systems, respectively. The F3B system met the sealed-bid, fund binding, one transaction latency, and no deposit properties while the traditional system met only the sealed-bid and fund binding properties. Furthermore, the F3B system requires significantly less storage at only 260B for auctions of any size; the traditional system requires storage that increases linearly with the number of bidders, requiring 29,068B for an auction with 100 bidders. The throughput of the F3B system however, performed significantly worse than that of the traditional system. For an auction with 100 bids, the throughput of the F3B system with an SMC of size 8 resulted in 0.16 bids per second while the traditional system resulted in 1.42 bids per second.

The key contributions of this paper include:

1. To our knowledge, this is the first work to design and implement a sealed-bid blockchain auction system meeting each of the sealed-bid, fund binding, one transaction latency, and no deposit properties.
2. An evaluation comparing the traditional and F3B sealed-bid blockchain auction systems.

Chapter 2

Background

This section presents a brief background on Dela and the Flash Freezing Flash Boys (F3B) protocol utilized to develop the sealed-bid blockchain auction systems.

2.1 Dela

The EPFL Decentralized and Distributed Computing Laboratory's Dela was utilized to develop the traditional and F3B sealed-bid blockchain auction systems [8]. Dela is a set of modular abstractions and an implementation of a distributed ledger architecture whose purpose is to provide a modular and universal framework that can be used to run a distributed ledger. For the purposes of this project, Dela was utilized run a blockchain for both the traditional and F3B sealed-bid blockchain auction systems.

Dela is built around three abstractions: the transaction pool, validation service, and ordering service.

- transaction pool: The transaction pool offers clients a single entry point for transactions to be propagated throughout the network. Transactions are sent to the transaction pool while the ordering service waits for enough transactions to create a new block.
- validation service: The validation service protects against malicious behavior by ensuring transactions are valid. This service protects against replay attacks, ensures transaction execution is correct, and provides a manager to help create and sign transactions.
- one transaction latency: The ordering service creates blocks, thereby extending the blockchain. While the ordering service does not determine the consensus method, it does define how values are read from the ledger.

2.2 Flash Freezing Flash Boys (F3B)

Flash Freezing Flash Boys (F3B) was utilized for the F3B sealed-bid blockchain auction system to allow for encrypted bid transactions and delayed execution of these transactions after the bidding period [16]. Originally designed to prevent front-running attacks, F3B relies on a commit-reveal scheme where encrypted transactions are committed and then later revealed by a decentralized secret-management committee. As shown in Figure 2.1, a transaction sender encrypts their transaction tx with a symmetric key k, resulting in the encrypted transaction c_{tx}. Next, the sender encrypts k with the public key of the secret-management committee, resulting in c_k. Finally, the sender submits both c_{tx} and c_k in the form of a write transaction. Once the transaction is committed, the secret-management committee releases secret key shares to the underlying consensus group, where the secret key is reconstructed. With the secret key reconstructed, the consensus group is able to decrypt c_k and obtain k, decrypt c_{tx} and obtain tx, and execute tx.

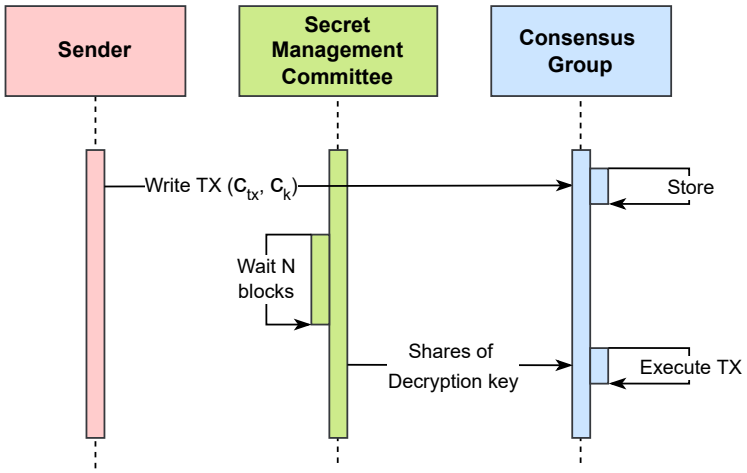

Figure 2.1: Flash Freezing Flash Boys Architecture

Chapter 3

Design

This section presents the system design for both the traditional and F3B sealed-bid blockchain auction systems.

3.1 Design Goals

As mentioned previously, the design goals of the auction systems are the following:

- sealed-bid: This guarantees each bid is kept secret from all other bidders during the bidding period.
- fund binding: This guarantees the winning bidder purchases the asset.
- one transaction latency: This guarantees that each bidder is required to submit only one transaction.
- no deposit: This guarantees that bidders do not submit a deposit.

3.2 Traditional Sealed-Bid Blockchain Auction Design

A blockchain sealed-bid auction was implemented using the traditional deposit method, whose architecture is shown in Figure 3.1.

In this architecture, each bidder submits a bid transaction during the bidding period and a reveal transaction during the reveal period. The bid transaction consists of both a commit and deposit. The bidder's commit is the SHA256 hash of the bid and a chosen random nonce. The

bidder's deposit is a payment at least as large as the bid itself.The reveal transaction consists of the bid and random nonce.

During the bidding period, the auction smart contract stores the bidder's commit and deposit. During the reveal period, the auction smart contract checks that each reveal matches its corresponding bid and stores the matching reveals. When the reveal period is complete, the auction smart contract selects the highest bidder as the winner and refunds the deposit of each losing bidder.

The most significant design decision made regarding the traditional auction method involved what method to use. As stated previously, most blockchain sealed-bid auction proposals relied on small deposits that were confiscated if the winning bidder did not purchase the asset, or a deposit at least as large as the bid. The latter option was chosen as this method enables fund binding and thus better met the design goals. Secondly, the length of the auction could be defined in a variety of ways, such as the number of bids, block length, or time. In order to simplify development, the number of bids was selected. It is important to note that In a production-ready blockchain auction system, this would not be ideal as an auction could fail to finish if the specified bid number is not met. Furthermore, the traditional auction utilises a commit-reveal scheme where bidders commit to their bid and nonce, and later reveal them. While a variety of interactive and non-interactive commitment schemes exist, a non-interactive commitment scheme was clearly preferable to reduce latency. The widely used SHA256 hash was used for bidder commitments to simplify commitments for bidders and to make use of the existing crypto package which provides SHA256 hash functionality.

This traditional design does not meet the design goals. While it enables sealed-bids and fund binding, each bidder is required to make two transactions and a deposit.

- sealed-bid: The design achieves sealed-bids because each bidder commits to a secret bid during the bidding phase, which is hidden from all other bidders.
- fund binding: The design achieves fund binding because a deposit is required at least as large as the bid itself. If the revealed bid is greater than the deposit, the bid is not considered.
- one transaction latency: One transaction latency is not met because two transactions are required for each bidder, the bid and reveal transactions.
- no deposit: No deposit is not met, as each bidder is required to make a deposit at least as large as the bid itself. This reduces the liquidity of the bidder during the auction period and leaks information of the bid amount.

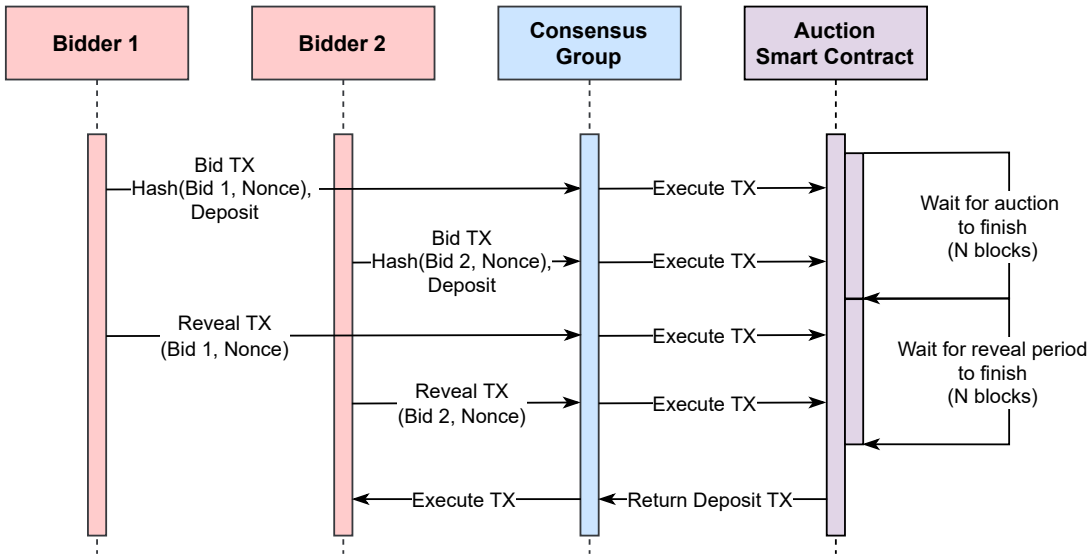

Figure 3.1: Architecture of Traditional Sealed-Bid Blockchain Auction

3.3 F3B Sealed-Bid Blockchain Auction Design

A blockchain sealed-bid auction was also implemented using the F3B method, whose architecture is shown in Figure 3.2.

In this architecture, each bidder submits an encrypted bid transaction that is stored on the blockchain. This encrypted bid transaction consists only of the bid, which is transferred to the auction smart contract if it is the highest bid. When the bidding period is complete, the secret-management committee releases the decryption keys for each bid transaction, and the bid transactions are decrypted and executed. The auction smart contract then receives the executed bid transactions. The auction smart contract stores the bid of the highest bidder and does not accept bids of lower bidders. Thus, when a higher bid is received, the auction smart contract stores this new highest bid and bidder and refunds the bid from the previous highest bidder.

Outside of the system architecture, the most significant design decisions made involved the symmetric encryption used to encrypt and decrypt bid transactions and how to measure auction length. To encrypt and decrypt bid transactions, AES was used with 512-bit keys because it is the most widely used symmetric cipher and regarded as secure [12]. As such, AES enables parties to easily encrypt and decrypt the bid transactions. Secondly, similar to the traditional auction design, the length of the auction was defined as the number of bid transactions.

This design achieves each of the design goals outlined:

- sealed-bid: The design achieves sealed-bids because all bid transactions are encrypted and not decrypted until the bidding period is complete.

- fund binding: The design achieves fund binding because the encrypted bid transaction includes the bid itself. Thus, when the bid transaction is decrypted and executed, the bid is transferred to the auction smart contract if it is the highest bid.
- one transaction latency: The design achieves one transaction latency, as only the encrypted bid transaction is submitted by each bidder.
- no deposit: The design avoids the need for a deposit, as each bidder submits an encrypted transaction with their bid, which is only transferred to the auction smart contract if it is the highest bid.

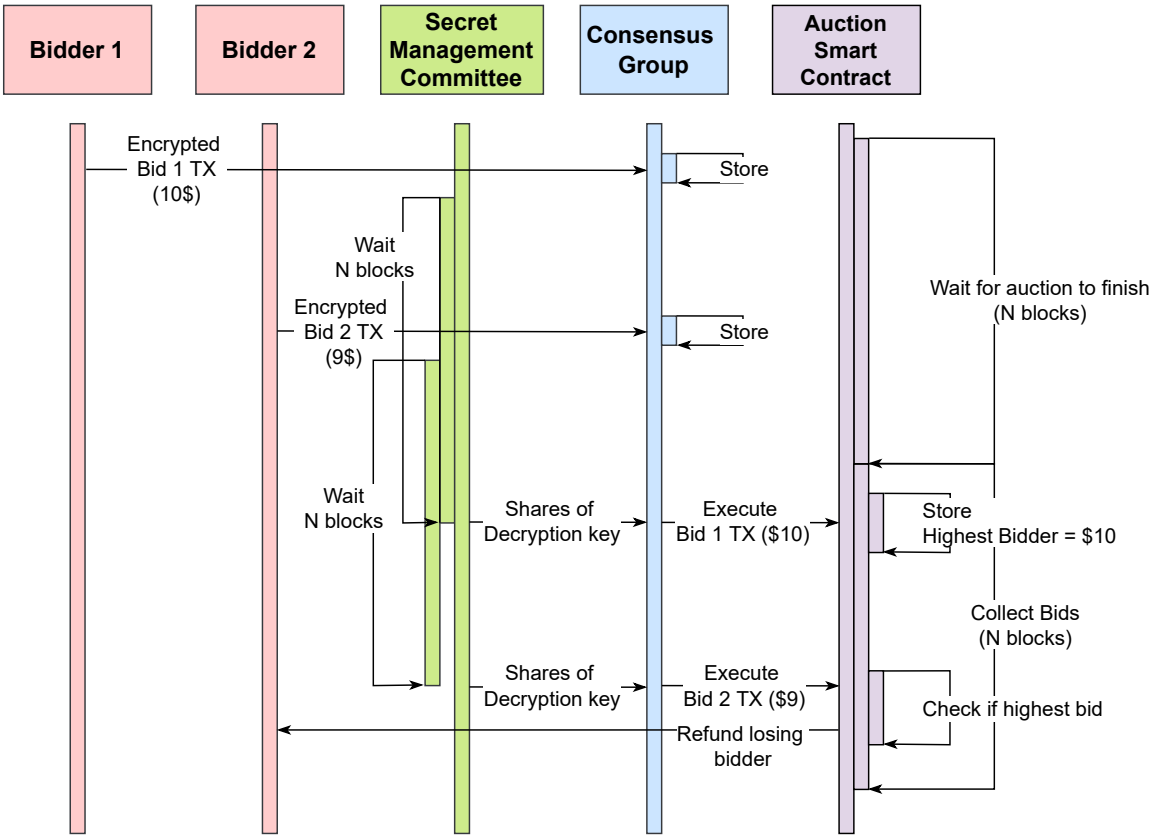

Figure 3.2: Architecture of F3B Sealed-Bid Blockchain Auction

Chapter 4

Implementation

This section presents the implementation of the traditional and F3B sealed-bid blockchain auction systems.

The sealed-bid blockchain auction systems were implemented in Go, consistent with the implementations of Dela and F3B. The traditional and F3B sealed-bid blockchain auction systems were both implemented as smart contracts. Furthermore, a bank smart contract was implemented to enable the management of bidder funds. The implementation of these three smart contracts, the F3B integration, and testing are described below in greater detail.

4.1 Bank Smart Contract

A bank smart contract was developed to manage funds of auction bidders whose class diagram is shown in Figure 4.1. The smart contract contains the following three commands:

- Deposit(amount): Deposit is called by a user to deposit a specific amount into their bank account. The bank smart contract responds by adding the specified amount to the user's bank balance.
- Withdraw(amount): Withdraw is called by a user to withdraw a specific amount from their bank account. If the user has such funds in their bank balance, the bank smart contract removes the specified amount from the user's balance.
- Transfer(account, amount): Transfer is called by a user to transfer a specified amount from their bank account to another user's bank account. If the user has such funds in their bank balance, the bank smart contract responds by transferring the amount from the user account to the specified account.

4.2 Traditional Auction Smart Contract

A traditional auction smart contract was developed to enable the traditional sealed-bid blockchain auction system whose class diagram is shown in Figure 4.2. The smart contract contains the following four commands:

- Init(bid_length, reveal_length): Init is called by the auction owner in order to start a new auction, thereby initialising the auction's owner, bid length, and reveal length. bid_length and reveal_length correspond to the length of the bidding and reveal periods, as measured by the number of bid and reveal transactions in each period respectively.
- Bid(commit, deposit): Bid is called by each bidder, sending their commit and deposit to the auction smart contract. In response, the auction smart contract stores the bidder's public key, commit, and transfers the deposit from the bidder to the auction smart contract.
- Reveal(deposit, nonce): Reveal is called by each bidder, sending their deposit and nonce to the auction smart contract. In response, the auction smart contract hashes the deposit and nonce, compares this to the bidder's previous commit, and stores the reveal if these values match.
- SelectWinner(): SelectWinner can only be called by the contract owner and is used to determine the highest bidder. In response, the auction smart contract determines the highest bidder and refunds all lower bidders. The public key of the highest bidder is returned by the command.

4.3 F3B Auction Smart Contract

An F3B auction smart contract was developed to enable the F3B sealed-bid blockchain auction system whose class diagram is shown in Figure 4.3. The smart contract contains the following four commands:

- Init(bid_length: Init is called by the auction owner in order to start a new auction, thereby initialising the auction's owner and bid length. bid_length corresponds to the length of the bidding period, as measured by the number of bid transactions.
- Bid(bid): Bid is called by each bidder, though its execution is delayed by F3B's secret-management committee, and includes the bidder's bid amount. If the bid is the highest bid thus far, the auction smart contract stores the bidder's public key and transfers the bid from the bidder to the auction smart contract. Furthermore, the auction smart contract refunds the previous highest bidder. If the bid is not the highest bid thus far, the auction smart contract does not transfer the bid.

- SelectWinner(): SelectWinner can only be called by the contract owner and is used to determine the highest bidder. In response, the auction smart contract returns the public key of the highest bidder.

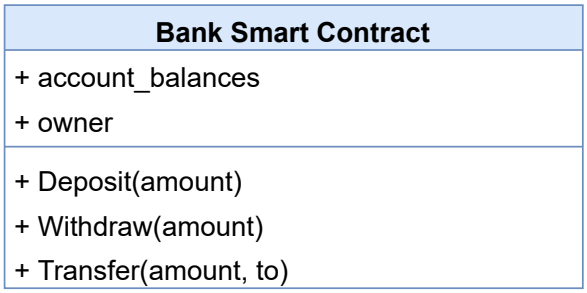

Figure 4.1: Bank Smart Contract Class Diagram

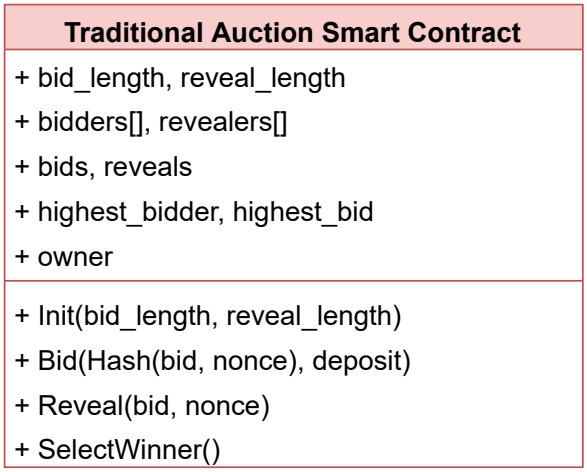

Figure 4.2: Traditional Auction Smart Contract Class Diagram

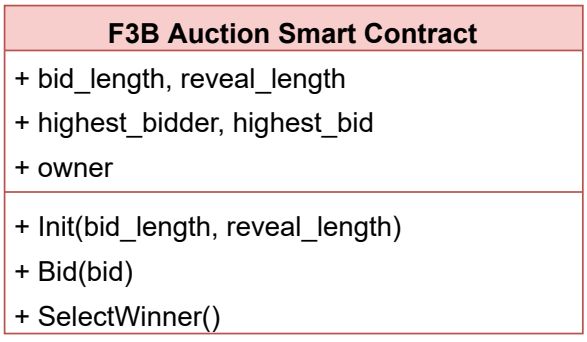

Figure 4.3: F3B Auction Smart Contract Class Diagram

4.4 F3B Integration

F3B was previously implemented on Dela by Mahsa Bastankhah through a summer internship at EPFL, and can be viewed in the DKG package. This past work allows for the secret-management committee (SMC) to setup public keys, setup corresponding secret key shares, encrypt data with the public keys, and decrypt data with the reconstructed secret key shares. To enable the F3B sealed-bid blockchain auction, this F3B implementation was incorporated with the F3B auction smart contract. The integration of F3B is described in greater detail below, by describing the flow of a bid transaction from the start to finish of the auction, as is shown in Figure 4.4.

After the start of the bidding period, the bidder creates the bid transaction tx and AES symmetric key k. The bidder then encrypts tx with k resulting in c_{tx}, and encrypts k with the SMC's public key resulting in c_k. c_{tx} and c_k are then submitted to the SMC. Next, when the SMC receives c_{tx} and c_k, it submits a write transaction to the consensus group, which writes these values to the blockchain.

After the bidding period is complete, the SMC submits a read transaction to the consensus group, allowing the SMC to read c_{tx} and c_k. The SMC then reconstructs its secret key, decrypts c_k, decrypts c_{tx}, and submits tx to the consensus group which executes it. Finally, the auction receives the executed bid transaction and ultimately determines the winner of the auction.

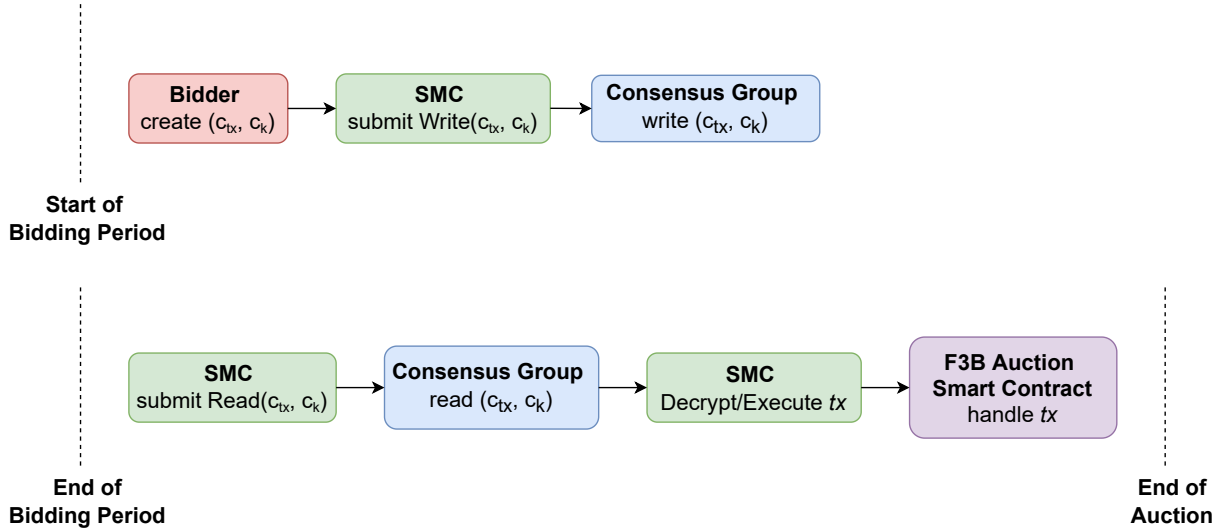

Figure 4.4: Flow of F3B Auction Transaction

4.5 Testing

Unit tests were implemented to test the bank, traditional auction, and F3B auction smart contracts and integration tests were implemented to test the traditional and F3B auction systems.

The code coverage of these unit tests can be seen below:

- Bank Smart Contract: 80.8%
- Traditional Auction Smart Contract: 75.4%
- F3B Auction Smart Contract: 70.1%

Chapter 5

Evaluation

This section presents the evaluation of the traditional and F3B sealed-bid blockchain auction systems.

The system was evaluated using a Macbook Pro laptop with a 2.2 GHz Intel Core i7 processor. Both the traditional and F3B sealed-bid blockchain auctions were compared qualitatively in terms of the design goals and quantitatively in terms of storage, latency, and throughput. Because F3B relies on a decentralized secret-management committee, the secret-management committee size was varied throughout the quantitative testing. Throughout the quantitative testing, three Dela nodes were used.

5.1 Qualitative Evaluation

As mentioned previously, the design goals of the system are the following:

- sealed-bid: This guarantees each bid is kept secret from all other bidders during the bidding period.
- fund binding: This guarantees the winning bidder purchases the asset.
- one transaction latency: This guarantees that each bidder is required to submit only one transaction.
- no deposit: This guarantees that bidders do not submit a deposit.

The F3B sealed-bid blockchain auction meets all four properties while the traditional sealed-bid blockchain auction only meets the sealed-bid and fund binding properties.

- sealed-bid: Both auctions meet the sealed-bid property; however, the traditional auction requires bidders to deposit an amount that is at least as large as their bid. As a result of this, bidders in the traditional auction face the choice of reducing their liquidity which masks their bid, or increasing their liquidity which exposes their bid. The F3B auction does not suffer from this issue, as all bids are encrypted and include the precise bid amount of each bidder. Thus, the F3B auction achieves the sealed-bid property while both increasing the bidder liquidity and better masking the bid.
- fund binding: Both auctions meet the fund binding property as both methods require the bidder to transfer funds to the auction smart contract through the bid transaction.
- one transaction latency: The traditional auction method requires both bid and reveal transactions while the F3B auction only requires one encrypted bid transaction. Furthermore, failure to submit a reveal transaction in the traditional auction nullifies the initial bid. This is significant as auctions typically only require one user action, the bid.
- no deposit: The traditional auction requires a deposit at least as large as the bid while the F3B auction requires no deposit. This is significant for bidder liquidity because the traditional auction requires the payment of the deposit for the duration of the auction. In the F3B auction however, the auction smart contract does not transfer the the bid unless it is the highest bid thus far. Thus, liquidity is not reduced for any losing bidders.

5.2 Quantitative Evaluation

The traditional and F3B sealed-bid blockchain auctions were compared quantitatively in terms of storage, latency, and throughput.

5.2.1 Storage

Blockchains store data across a collection of distributed nodes, and are thus not ideal for storing large quantities of data. In terms of blockchain auctions, this could result in significant energy usage or costs of the auction system. As such, the quantity of data stored by the traditional and F3B auctions was compared.

As shown in Table 5.1, the storage requirements of the traditional auction far exceed that of the F3B auction. Furthermore, because the traditional auction must store all bids and bidders, the storage requirements increase linearly as the number of bids increases. The F3B auction however, requires approximately 260 Bytes of storage, mainly storing the auction owner, highest bidder, and highest bid.

	Storage for different auction types (Bytes)	
Number of Bids	Traditional Auction	F3B Auction
10	3,148	260
50	14,668	260
100	29,068	260

Table 5.1: Storage vs Auction Size for Different Auction Types

5.2.2 Latency

The traditional and F3B auction systems were compared on latency, measured as the time taken from the initialization of the auction to the selection of the winner. Latency is significant in the traditional auction system as the losing bidders are not refunded until the end of the auction. Furthermore, latency is significant in the F3B auction system because secret-management committee (SMC) size can significantly delay the selection of a winner.

Latency was measured for auctions of 10, 50, and 100 bids for the traditional auction and for the F3B auction with 8 SMC members, 32 SMC members, and 64 SMC members. As can be seen in Figure 5.1, the auction latency is significantly greater for the F3B auctions than for the traditional auction. Furthermore, as the size of the SMC increases, the latency of the auction also substantially increases. Thus, while the F3B auctions only require bidders to make one transaction, it requires bidders to wait longer for the results of the auction.

5.2.3 Throughput

The traditional and F3B auctions were compared on throughput, measured as the number of bid transactions that can be executed per second. For popular auctions with large quantities of bidders, throughput could result in significant delays in selecting the winner.

Throughput was measured for the traditional auction and for the F3B auctions with 8 SMC members, 32 SMC members, and 64 SMC members. As can be seen in Figure 5.2, the throughput is significantly lower for the F3B auctions than for the traditional auction. Furthermore, as the size of the SMC increases, the throughput also substantially decreases. Lastly, the throughput for all auction types significantly decreases as the auction length increases. This suggests the F3B auctions, regardless of SMC size, would face challenges with popular auctions with high throughput requirements.

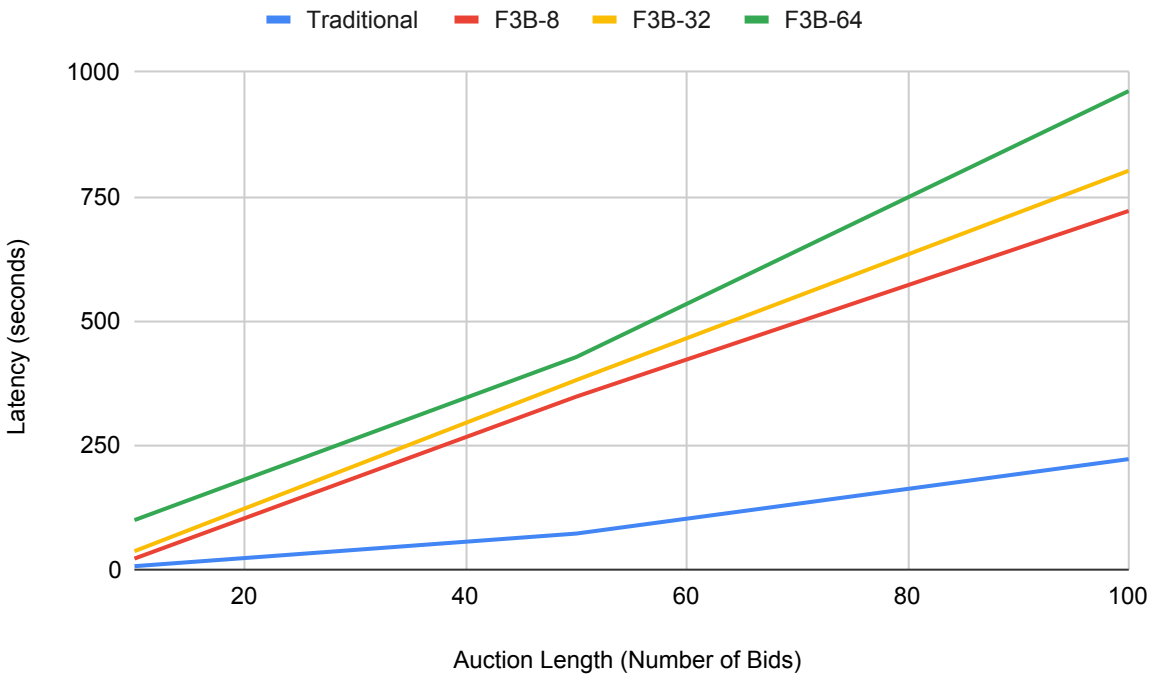

Figure 5.1: Auction Length vs Latency of Sealed-Bid Auctions

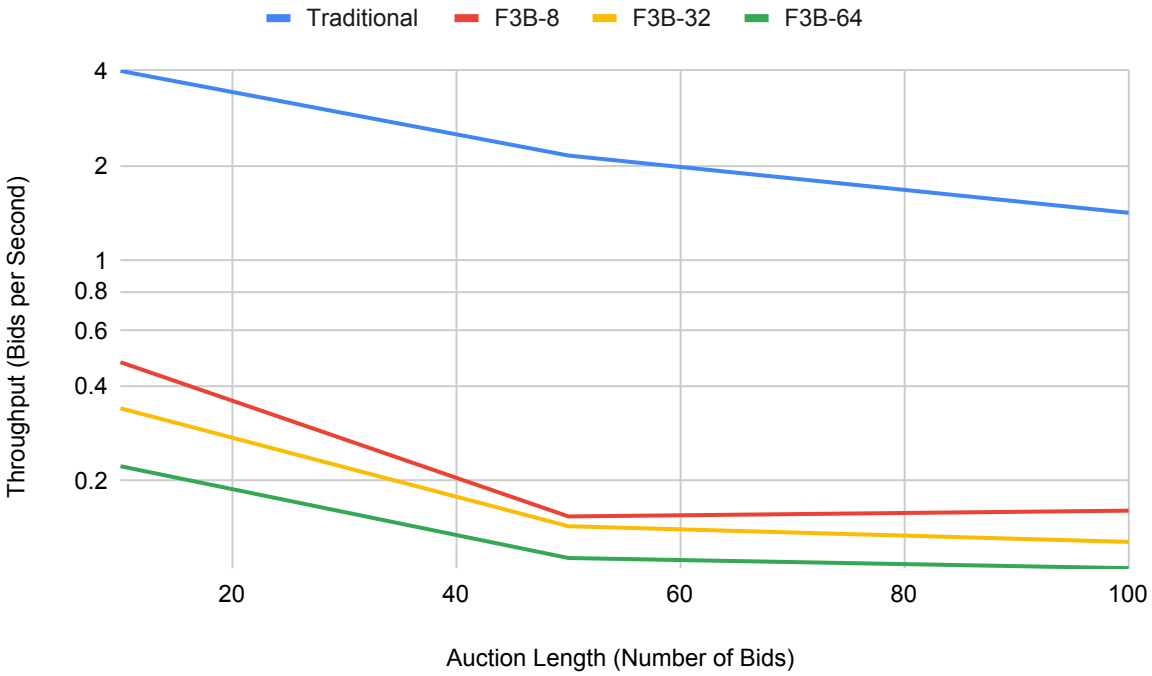

Figure 5.2: Auction Length vs Throughput of Sealed-Bid Auctions

Chapter 6

Limitations and Future Research Directions

This section presents the limitations of the F3B sealed-bid auction system and future research directions.

6.1 Limitations

Low latency is a significant limitation of the F3B sealed-bid blockchain auction system. For auctions with numerous bidders, the throughput of the F3B auction system would be a limiting factor, particularly with large secret-management committees (SMC). For example, an F3B auction with only 8 SMC members yields only 10 transactions per minute. For auctions with thousands of bids, throughput improvements would be required.

A second limitation relates to the access control of Dela's shared database. While the bank smart contract handles bidder deposits, withdrawals, and transfers, any smart contract could easily access this data. Thus, the auction smart contracts could theoretically withdraw and keep all bidder funds. Access controls could be implemented to limit data accesses to specific smart contracts.

Lastly, the auction smart contracts measure the auction length as the number of bids, as opposed to block length. For less popular auctions, this could result in the auction length exceeding the number of bids. This would result in the auction never finishing, a major issue. Enabling smart contracts to access the current block length could resolve this issue, as it would allow the auction length to have a definite end point.

6.2 Future Research Directions

Future research could be conducted to address the limitations of the F3B sealed-bid blockchain auction system. The throughput of the F3B sealed-bid blockchain auction should be addressed by assessing throughput limitations of the smart contracts utilized, F3B's encryption and decryption of transactions, and Dela's execution of transactions. Secondly, additional access controls could be implemented to ensure only specific smart contracts can access certain segments of the shared database.

Furthermore, future research could be conducted to explore the applications of F3B outside of its use in preventing front-running attacks and enabling sealed-bid auctions. F3B allows for encrypted transactions with delayed execution by releasing shares of its secret keys after a specific number of transactions. While this execution delay is currently fixed, the SMC could also delay execution until a specific condition is met. This could enable users to buy or sell limit orders when an asset is at or below a specified price, a significant component of the current financial system. Furthermore, this extension of F3B could also enable subscription payments as users could submit several payments upon a purchase, which could then be released periodically.

Bibliography

[1] Caroline Banton. *What Is an Auction? Definition, How They Work, Pros, and Cons*. URL: https://www.investopedia.com/terms/a/auction.asp. (accessed: 14.10.2022).

[2] Fang Block. *Global Auction Sales Soared to a Record $12.6 Billion in 2021*. URL: https://www.barrons.com/articles/global-auction-sales-soared-to-a-record-12-6-billion-in-2021-01641328947. (accessed: 12.10.2022).

[3] Biwen Chen, Xue Li, Tao Xiang, and Peng Wang. "SBRAC: Blockchain-based sealed-bid auction with bidding price privacy and public verifiability". In: *Journal of Information Security and Applications* 65 (2022), p. 103082. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2021.103082. URL: https://www.sciencedirect.com/science/article/pii/S2214212621002635.

[4] Yi-Hui Chen, Shih-Hsin Chen, and Iuon-Chang Lin. "Blockchain based smart contract for bidding system". In: *2018 IEEE International Conference on Applied System Invention (ICASI)*. 2018, pp. 208–211. DOI: 10.1109/ICASI.2018.8394569.

[5] Kota Chin, Keita Emura, Kazumasa Omote, and Shingo Sato. "A Sealed-bid Auction with Fund Binding: Preventing Maximum Bidding Price Leakage". In: *2022 IEEE International Conference on Blockchain (Blockchain)*. 2022, pp. 398–405. DOI: 10.1109/Blockchain55522.2022.00062.

[6] Theodoros Constantinides and John Cartlidge. "Block Auction: A General Blockchain Protocol for Privacy-Preserving and Verifiable Periodic Double Auctions". In: *2021 IEEE International Conference on Blockchain (Blockchain)*. 2021, pp. 513–520. DOI: 10.1109/Blockchain53845.2021.00078.

[7] Francesco Decarolis. "Awarding Price, Contract Performance, and Bids Screening: Evidence from Procurement Auctions". In: *American Economic Journal: Applied Economics* 6.1 (Jan. 2014), pp. 108–32. DOI: 10.1257/app.6.1.108. URL: https://www.aeaweb.org/articles?id=10.1257/app.6.1.108.

[8] EPFL Decentralized and Distributing Systems Laboratory. *Dela: Dedis Ledger Architecture*. URL: https://dedis.github.io/dela/. (accessed: 01.10.2022).

[9] Hisham S. Galal and Amr M. Youssef. "Trustee: Full Privacy Preserving Vickrey Auction on Top of Ethereum". In: *Financial Cryptography and Data Security*. Ed. by Andrea Bracciali,

Jeremy Clark, Federico Pintore, Peter B. Rønne, and Massimiliano Sala. Cham: Springer International Publishing, 2020, pp. 190–207. ISBN: 978-3-030-43725-1.

[10] Will Kenton. *Sealed-Bid Auction Definition, How It Works in Real Estate Sales*. URL: https://www.investopedia.com/terms/s/sealed-bid-auction.asp. (accessed: 14.10.2022).

[11] Leandros Maglaras, Honglei Li, and Weilian Xue. "A Blockchain-Based Sealed-Bid e-Auction Scheme with Smart Contract and Zero-Knowledge Proof". In: *Security and Communication Networks* 19 (May 2021). URL: https://doi.org/10.1155/2021/5523394.

[12] Cory Maklin. *AES Encryption 256 Bit*. URL: https://towardsdatascience.com/aes-encryption-256-bit-a9ae49cde0b6. (accessed: 27.10.2022).

[13] Research and Markets. *Global Online Auction Market: Analysis By Product Type*. URL: https://www.researchandmarkets.com/reports/5653991/global-online-auction-market-analysis-by-product. (accessed: 12.10.2022).

[14] Bader Al-Sada, Noureddine Lasla, and Mohamed Abdallah. "Secure Scalable Blockchain for Sealed-Bid Auction in Energy Trading". In: *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2021, pp. 1–3. DOI: 10.1109/ICBC51069.2021.9461071.

[15] Gaurav Sharma, Denis Verstraeten, Vishal Saraswat, Jean-Michel Dricot, and Olivier Markowitch. "Anonymous Sealed-Bid Auction on Ethereum". In: *Electronics* 10.19 (2021). ISSN: 2079-9292. DOI: 10.3390/electronics10192340. URL: https://www.mdpi.com/2079-9292/10/19/2340.

[16] Haoqian Zhang, Louis-Henri Merino, Vero Estrada-Galiñanes, and Bryan Ford. "Flash Freezing Flash Boys: Countering Blockchain Front-Running". In: *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. 2022, pp. 90–95. DOI: 10.1109/ICDCSW56584.2022.00026.

Appendix A

Project Files, Setup, Run Auctions

This appendix presents the project folder structure and files as well, the project setup, and how to run the traditional and F3B sealed-bid blockchain auctions.

A.1 Project Files

The project folder structure and files are outlined below:

- contracts
  - bank
    - mod.go: Implementation of bank smart contract
    - mod_test.go: Unit testing of bank smart contract
    - controller
      - mod.go: Controller for bank smart contract
      - mod_test.go: Unit testing of controller
  - auction
    - mod.go: Implementation of traditional auction smart contract
    - mod_test.go: Unit testing of traditional auction smart contract
    - controller
      - mod.go: Controller for traditional auction smart contract
      - mod_test.go: Unit testing of controller
  - auctionF3B
    - mod.go: Implementation of F3B auction smart contract
    - mod_test.go: Unit testing of F3B auction smart contract

        * controller
            · mod.go: Controller for F3B auction smart contract
            · mod_test.go: Unit testing of controller

- dkg
  - pederson: Mahsa Bastankhah's implementation of F3B
- test
  - SymmetricEncrypt_test.go: Implementation of AES encryption and decryption.
  - TraditionalAuction_test.go: Integration testing for the traditional auction system
  - TraditionalAuction_evaluation_test.go: Latency and Throughput evaluation of the traditional auction system
  - F3BAuction_test.go: Integration testing for the F3B auction system
  - F3BAuction_evaluation_test.go: Latency and Throughput evaluation of the F3B auction system
  - F3B_test: Mahsa Bastankhah's implementation of F3B

A.2 Project Setup

The project was developed using Go v1.18, consistent with the F3B implementation. The project can be built using the project Makefile.

1. Install Go v1.18.
2. Install the *crypto* utility from Dela:

   ```
   git clone https://github.com/dedis/dela.git
   cd dela/cli/crypto
   go install
   ```

   Go will install the binaries in $GOPATH/bin, so be sure this it is correctly added to you path (e.g. export PATH=$PATH:/Users/user/go/bin).

A.3 Run Traditional and F3B Sealed-Bid Blockchain Auctions

For the traditional sealed-bid blockchain auction, a sample auction can be run in TraditionalAuction_test.go. For the F3B sealed-bid blockchain auction, a sample auction can be run in F3BAuction_test.go.