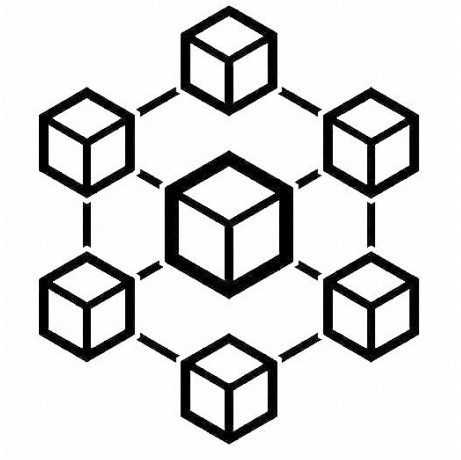
RUNNING AN AUCTION USING BLOCKCHAIN

Isha Patel

Purpose

- Blockchain is a fairly new technology.
  - Emerged with BitCoin
  - Not widely known
- There are many uses of blockchain.
  - Used to manage an auction
    - Safe, secure, and accurate



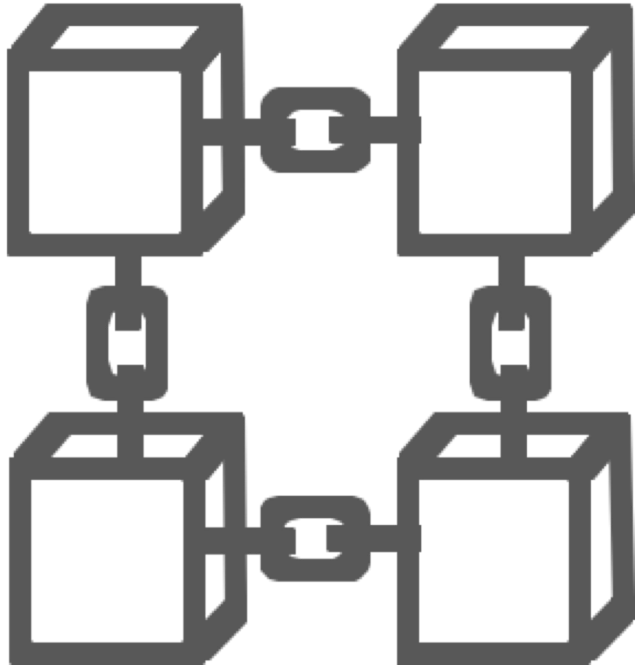
Goal

- The goal was to build a smart contract of a blockchain-based auction.
  - Addition of the Vickrey auction
    - Highest bidder pays second-highest bid

Blockchain

What is that?

A blockchain is a digital ledger that records all transactions and stores each transaction as immutable blocks



Decentralized

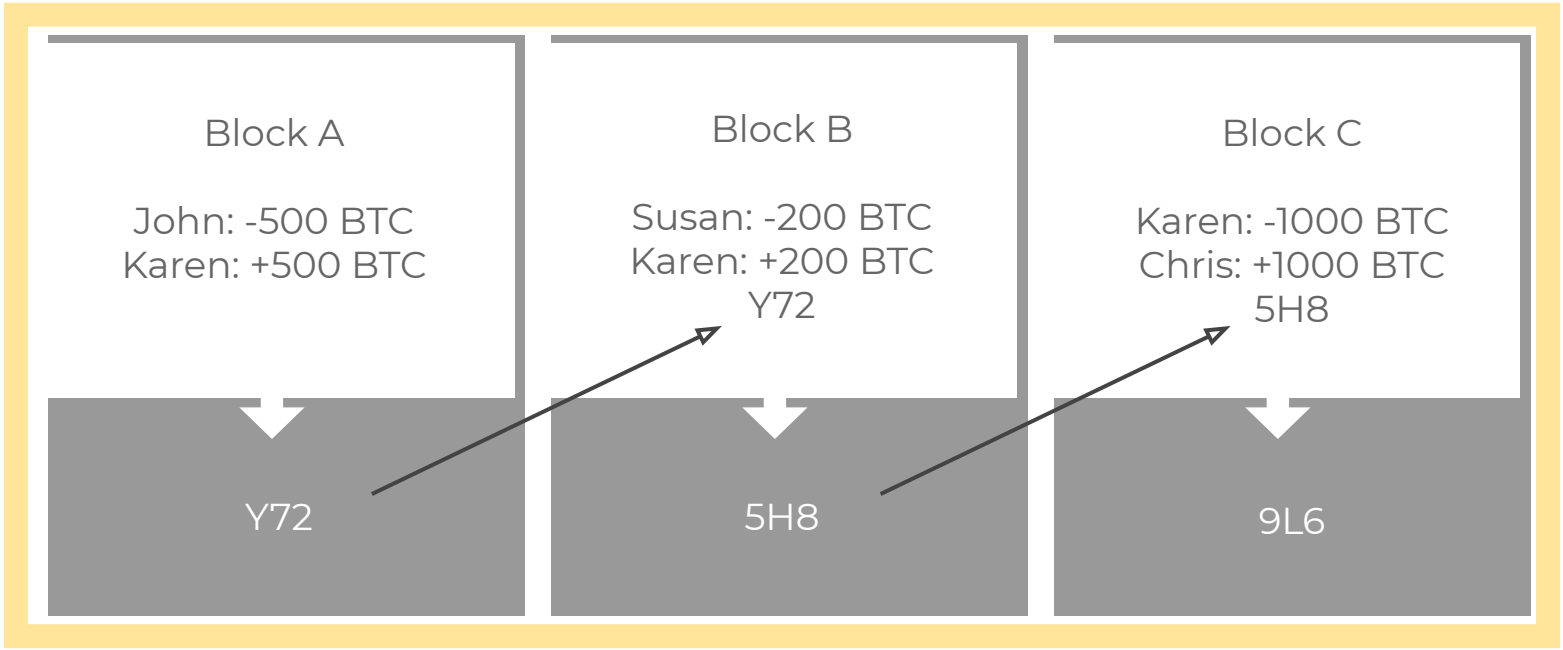
- Data is distributed throughout the whole network.
  - No central authority
  - Ledger visible to network
    - Private individual identities

flaticon.com/authors/ddara

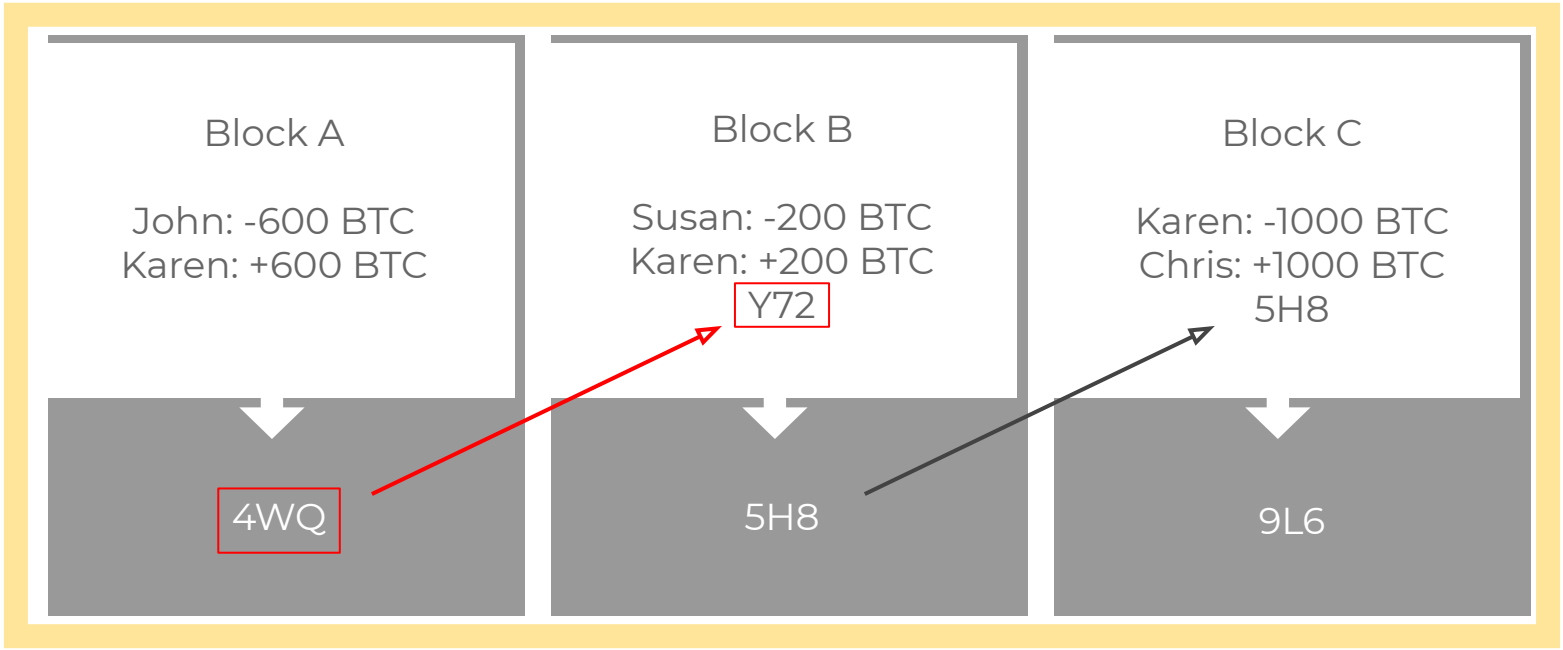
Immutable

- Blocks are connected by their hashes.
  - Hashing: generating a fixed-length output from a given input
    - Hash: the output value generated from an input value that was put through a hash function
- Hashing makes it almost impossible to alter the ledger.

Hashing

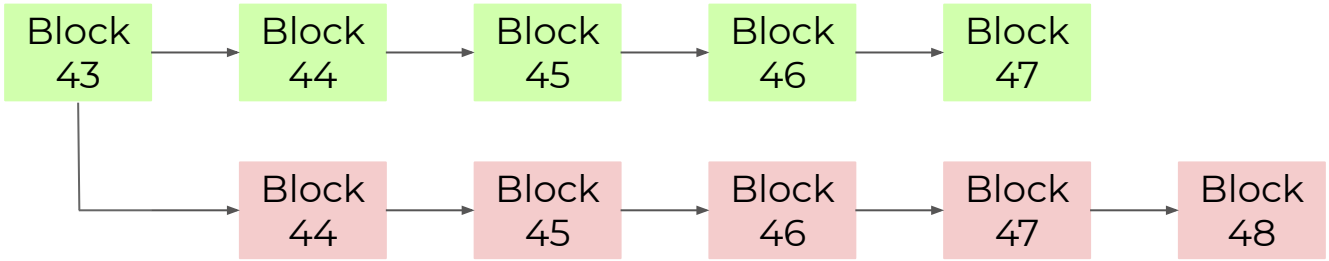

Block A
John: -500 BTC
Karen: +500 BTC
Y72
Block B
Susan: -200 BTC
Karen: +200 BTC
Y72
5H8
Block C
Karen: -1000 BTC
Chris: +1000 BTC
5H8
9L6

Hashing


Block A
John: -600 BTC
Karen: +600 BTC
4WQ
Block B
Susan: -200 BTC
Karen: +200 BTC
Y72
5H8
Block C
Karen: -1000 BTC
Chris: +1000 BTC
5H8
9L6

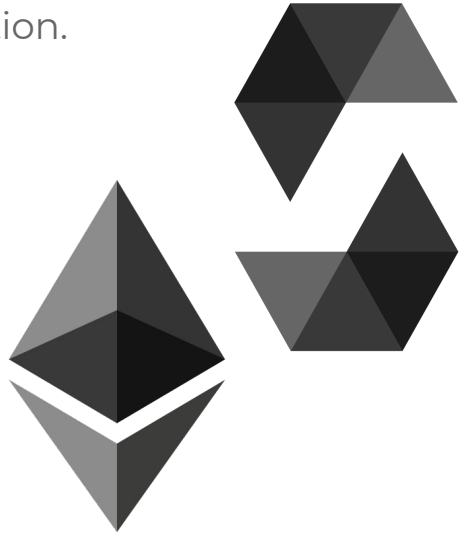
51% Attack

- 51% of the network can topple a blockchain.
  - Has happened, but is rare
  - Not likely in a blockchain owned by one company

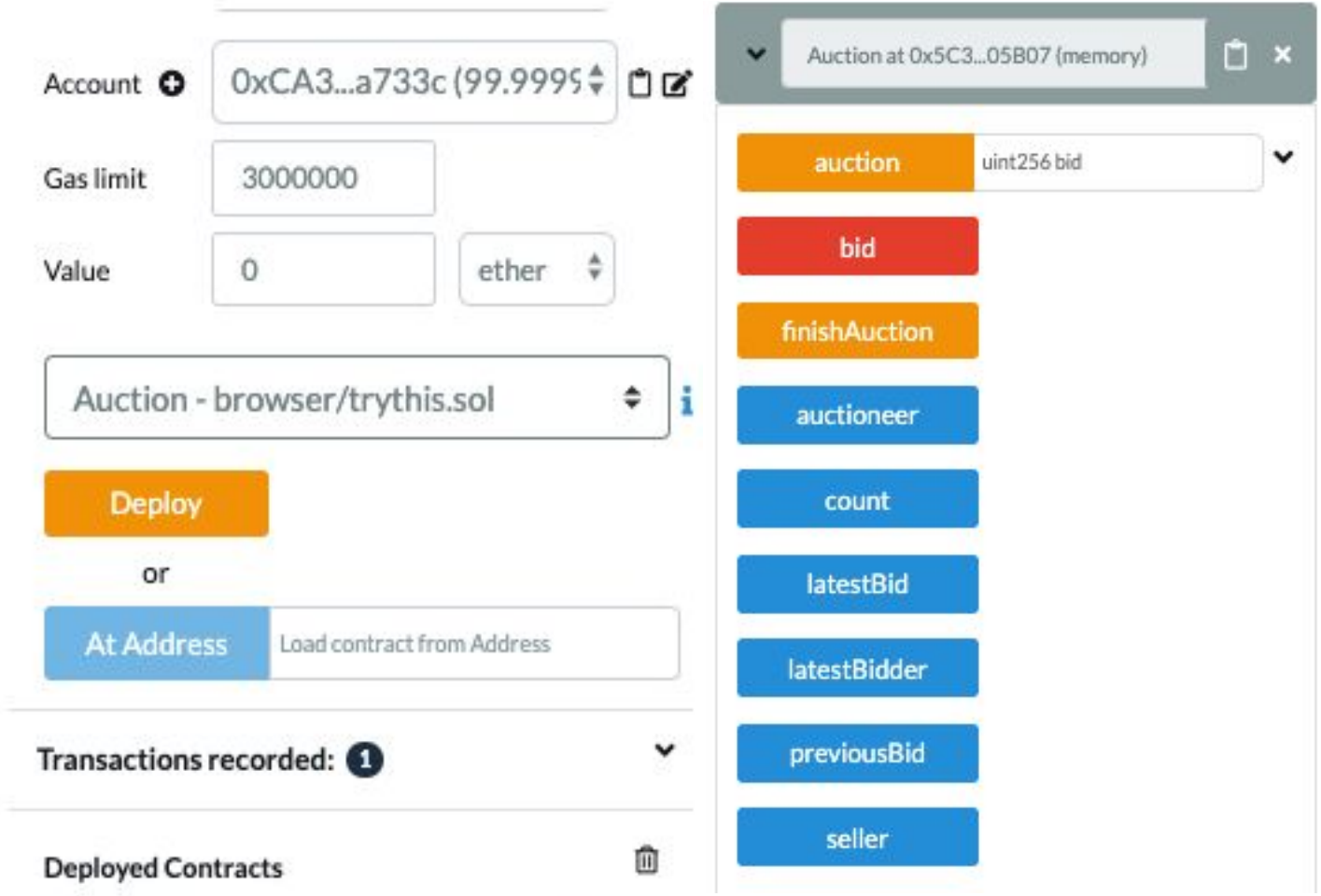


Procedures

- Open-sourced code was used to set a foundation.
  - Remix: Ethereum IDE
  - Solidity
- Vickrey auction feature
- If statement for varied number of bidders
- Auction was run multiple times for testing.



wikipedia.org


Account
0xCA3...a733c (99.999
Gas limit
3000000
Value
0
ether
Auction - browser/trythis.sol
Deploy
or
At Address
Load contract from Address
Transactions recorded: 1
Deployed Contracts
Auction at 0x5C3...05B07 (memory)
auction
uint256 bid
bid
finishAuction
auctioneer
count
latestBid
latestBidder
previousBid
seller

Running the Auction

AUCTIONEER

An auctioneer is selected; they open the auction and are the only ones that can close the auction

OPENING

An auction is opened by the auctioneer and the currency is set to ethers

SELLER

A different account is selected for the seller. The seller sets the minimum bid.

BIDDER

The remaining accounts are bidders. To bid, a bidder account is selected and a bid is placed.

BID

After each bid, the bidder gives the auctioneer the sum and the sum collected from the previous bid is returned to its respective bidder.

CLOSING

To close the auction, the auctioneer must be selected. The latest bidder then pays the seller the second-highest bid. The auction is closed.

Results

- If there are no bids placed, the auction would be closed without any ethers spent.
- If only one bid is placed, then the bidder pays that bid.
- If more than two bids are placed, then the highest bidder pays the second-highest bid.

```
[vm] from:0x4b0...4d2db to:Auction.bid() 0x692...77b3a value:5000000000000000000 wei data:0x199...8aeef logs:0 hash:0xc20...822d8
```

Debug

```
transact to Auction.bid pending ...
```

```
[vm] from:0xdd8...92148 to:Auction.bid() 0x692...77b3a value:15000000000000000000 wei data:0x199...8aeef logs:0 hash:0x24d...a9ae7
```

Debug

```
transact to Auction.bid pending ...
```

```
[vm] from:0x4b0...4d2db to:Auction.bid() 0x692...77b3a value:20000000000000000000 wei data:0x199...8aeef logs:0 hash:0x5bb...ab99c
```

Debug

```
transact to Auction.bid pending ...
```

```
[vm] from:0x583...40225 to:Auction.bid() 0x692...77b3a value:25000000000000000000 wei data:0x199...8aeef logs:0 hash:0x51e...da773
```

Debug

```
transact to Auction.finishAuction pending ...
```

```
[vm] from:0x583...40225 to:Auction.finishAuction() 0x692...77b3a value:0 wei data:0x430...ca46f logs:0 hash:0x989...bf7db
```

Debug

```
transact to Auction.finishAuction errored: VM error: revert.
revert  The transaction has been reverted to the initial state.
Note: The called function should be payable if you send value and the value you send should be less than your current balance.  Debug the transaction to get more information.
```

[vm] **from:**0x4b0...4d2db **to:**Auction.bid() 0x692...77b3a **value:**5000000000000000000 wei **data:**0x199...8aeef **logs:**0 **hash:**0xc20...822d8 Debug

status	0x1 Transaction mined and execution succeed
transaction hash	0xc2068ec58020cee14c4fee1687a6b58d9fe5250a6d74829b41d8f978678822d8
from	0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db
to	Auction.bid() 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	90659 gas
execution cost	69387 gas
hash	0xc2068ec58020cee14c4fee1687a6b58d9fe5250a6d74829b41d8f978678822d8
input	0x199...8aeef
decoded input	{}
decoded output	{}
logs	[]
value	5000000000000000000 wei

transact to Auction.bid pending ...

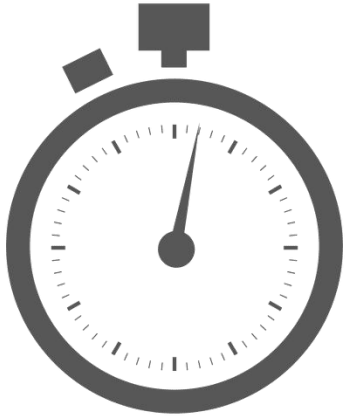
[vm] **from:**0xdd8...92148 **to:**Auction.bid() 0x692...77b3a **value:**15000000000000000000 wei **data:**0x199...8aeef **logs:**0 **hash:**0x24d...a9ae7 Debug

Conclusion

- The project successfully met the criteria:
  - Smart contract of an auction
    - Addition of Vickrey auction

Future Research

- Third-party timers
- Automatic closing
- Front-end
  - Different people are the bidders



RUNNING AN AUCTION USING BLOCKCHAIN

Isha Patel