Surveying Front-running attacks on Decentralized Exchanges

Mingcheng & Sean
Goal

- Introduce a special kind of attack on decentralized exchange
- Try to propose a mitigation in the end
What is this?

7,531.52 United States Dollar

Apr 24, 3:24 AM UTC · Disclaimer

1
7531.52 United States Dollar

Data provided by Morningstar for Currency and Coinbase for Cryptocurrency
Blockchain Introduction

blockchain is essentially a decentralized, distributed “database” (ledger) recording transactions, which cannot be altered retroactively without the alteration of all subsequent blocks.

- Distributed
- Decentralized
- Non-centralized Trust
- Immutable
### Blockchain workflow: block and block generation

Blockchain consists of blocks.

1. Each block consists of a head and a body.
   - **Body** records transactions.
   - **Head** includes the cryptographic hash (SHA256) of the body and the prior block.

### Transaction Details

<table>
<thead>
<tr>
<th>Hash</th>
<th>Amount (BTC)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>e4634fa7c50d9a334bd015a0f2e8f701b998881de21d05e6d0aed4...</td>
<td>12.87625877 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.56652188 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.94351828 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.72028600 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.66090120 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.59571369 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.56473076 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.54066334 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.54799571 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>12.61917307 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1GFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>289.52436879 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1GFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>0.13870557 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1GFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>0.04572787 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1GFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>0.02884744 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1GFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>0.00530365 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>1GFHE7w8BhaENAswwryaoccDb6qcT6DbYY</td>
<td>311.24788734 BTC</td>
<td>2020-04-26 18:47</td>
</tr>
</tbody>
</table>

Load more inputs... (9 remaining)

**Fee**

- **0.00000000 BTC**
- *(0.000 sat/B - 0.000 sat/WU - 3618 bytes)*

**Fee Reward**

- **0.08282373 BTC**
Blockchain workflow: block and block generation

**Head:**
- Time: Timestamp
- hashMerkleRoot: Hash of Body
- hashPrevBlock: Hash of previous Block
- Bits: Target Value
- Nonce: Magic Number

**Body:**
- Transactions...

---

```
<table>
<thead>
<tr>
<th>Hash</th>
<th>000000000000000000056cf2bf26dcebc27fd6d18879e2bcaed78343d4f3b378</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirmations</td>
<td>1</td>
</tr>
<tr>
<td>Timestamp</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>Height</td>
<td>627784</td>
</tr>
<tr>
<td>Miner</td>
<td>F2Pool</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>2,300</td>
</tr>
<tr>
<td>Difficulty</td>
<td>15,958,652,328,578.42</td>
</tr>
<tr>
<td>Merkle root</td>
<td>afcc304adfb2344d9c41037f6e42cd6d9154ffe189a08a19733de8aa8f3e9f</td>
</tr>
<tr>
<td>Version</td>
<td>0x20002000</td>
</tr>
<tr>
<td>Bits</td>
<td>387,031,859</td>
</tr>
<tr>
<td>Weight</td>
<td>3,998,680 WU</td>
</tr>
<tr>
<td>Size</td>
<td>1,108,855 bytes</td>
</tr>
<tr>
<td>Nonce</td>
<td>1,238,480,872</td>
</tr>
<tr>
<td>Transaction Volume</td>
<td>3168.84300466 BTC</td>
</tr>
<tr>
<td>Block Reward</td>
<td>12,500000000 BTC</td>
</tr>
<tr>
<td>Fee Reward</td>
<td>0.08282373 BTC</td>
</tr>
</tbody>
</table>
```
Blockchain workflow: block and block generation

**Head:**
- Time: Timestamp
- hashMerkleRoot: Hash of Body
- hashPrevBlock: Hash of previous Block
- Bits: Target Value
- Nonce: Magic Number

When SHA256(Head, Nonce++) < Bits (Target Max/Difficulty level)

**Body:**
- Transactions...

**New Block**
- prev: H()
Blockchain workflow: block and block generation

Blockchain consists of blocks.

Each block consists of head and body.

- Body records transaction
- Head includes the cryptographic hash (SHA256) of the body and the prior block

Block Miner can get block reward and operation fee.

- proof-of-work

<table>
<thead>
<tr>
<th>Hash</th>
<th>00000000000000000000056cf2b1f26dcebc27fd6d18879e2bcade78343db4f3b378</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirmations</td>
<td>1</td>
</tr>
<tr>
<td>Timestamp</td>
<td>2020-04-26 18:47</td>
</tr>
<tr>
<td>Height</td>
<td>627784</td>
</tr>
<tr>
<td>Miner</td>
<td>F2Pool</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>2,300</td>
</tr>
<tr>
<td>Difficulty</td>
<td>15,958,652,328,578.42</td>
</tr>
<tr>
<td>Merkle root</td>
<td>afcb304adfb2344d9c41037f6e42cd6d9154f6e189a08a19733de8aa8fe3e9f</td>
</tr>
<tr>
<td>Version</td>
<td>0x20002000</td>
</tr>
<tr>
<td>Bits</td>
<td>387,031,859</td>
</tr>
<tr>
<td>Nonce</td>
<td>1,238,489,672</td>
</tr>
<tr>
<td>Size</td>
<td>1,108,855 bytes</td>
</tr>
<tr>
<td>Transaction Volume</td>
<td>3168.84300446 BTC</td>
</tr>
<tr>
<td>Block Reward</td>
<td>12.50000000 BTC</td>
</tr>
<tr>
<td>Fee Reward</td>
<td>0.08282373 BTC</td>
</tr>
</tbody>
</table>
## Blockchain workflow: broadcast and census

<table>
<thead>
<tr>
<th>Hash</th>
<th>BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>e4634fa7c50d9a334bd015a0f2e8f701b999881de21d05e6d0aed4...</td>
<td></td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.87625877 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.56652188 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.94351828 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.72028600 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.86091200 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.59571369 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.56473076 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.54063344 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.54799571 BTC</td>
</tr>
<tr>
<td>1KFHE7w8BhaENAswwryaccDb6qcT6DbYY</td>
<td>12.61917307 BTC</td>
</tr>
</tbody>
</table>

Load more inputs... (9 remaining)

**Fee**

0.00000000 BTC  
(0.000 sat/B - 0.000 sat/WU - 3618 bytes)

**Transactions Total**

1Gx28yLjVWux7ws4UQ9FB4MnLH4UKTP2z  
392NrbX3E28aWjQMj6aa2EjLQDZdECr7Y  
36gpliTj55sBzAYpV25e1vLe9Y77gwLFGv76  
e1UtSa07njVcA723UjryHiT0hXhQEUwe7  
1LwpfazVb9qDc4he6A4rPTPBCT2c1tY1  
1KFHE7w8BhaENAswwryaccDb6qcT6DbYY  
311.24788734 BTC

**Transaction Details**

- **Hash**: 600.99084056 BTC  
- **Confirmation**: 1 Confirmations
Blockchain workflow: broadcast and census

- If divert, the chain has been seen by the majority will be validated forever.
- To keep consistent, bitcoin is designed to generate new block in average 10 mins by adjusting the difficulty level.
Problems with bitcoin blockchain:

Just ledger!!

Wasting powers/resource!!
Add More Flavors: Ethereum Virtual Machine and Smart Contract

- Lightweight computer programs executed on blockchain network without user interaction when certain conditions are made.
  - When someone wants to get a particular task done in Ethereum they initiate a smart contract with one or more peers.

- The EVM provides better deterministic, terminable and isolated environment for the smart contracts. (Like JVM)
  - EVM is turning complete
The Ethereum Network
The Ethereum Network
Ethereum Gas and Fee

- Gas is a unit that measures the amount of computational effort that it will take to execute certain operations.
  - Every line of code in Solidity requires a certain amount of gas to be executed.

- Gas Limit $\geq$ Gas needed
- Gas Fee = Gas Limit $\times$ Gas Price (Gwei)
- Gas Fee is the maximum profit code runner can get
The Scale of Ethereum Network

- Ethereum is now the 2nd largest blockchain Network in the world
  Market Cap = $20+ Billion

- Frequent Transactions

Data Collected from etherscan https://etherscan.io/
ICO on Ethereum = Fundraising

ERC20 Tokens

(ERC20 is a Protocol for Ethereum Cryptocurrencies, it allow direct interaction between parties)

Public

Ether

Developer

Initial Coin Offering
Smart Contract

Gather Piles of Ether => Money

17
Functionalities of ERC20 Tokens

- **Toll**: A token can act as a gateway to the Dapp.

- **Voting Rights**: The tokens may also qualify the holders to have certain voting rights.

- **Value Exchange**: Tokens can help create an internal economic system within the application.
A Need for Exchange

Cryptocurrency Exchange

TokenA

TokenB

TokenC
Centralized Exchange
Decentralized Exchange (DEXs)

Core Contract

Matcher

Order Book

The Exchange Smart Contracts

Maker

TokenA

Taker

TokenB

I offer 1 TokenA for 2 TokenB

"I take the great TokenA with 2 TokenB"

1A for 2B

Proxy Contract 1A for 2B

Great Deal!
Decentralized Exchange

- **Core Contract**
- **Algorithmic Matcher**
- **Algorithmic Marketmaker**

“Taker” says, “I want to buy TokenA with TokenB”

“Maker” says, “I want to buy TokenB with TokenA”

Proxy Contract

A ↔ B

With a Calculated Rate

Buy Order -> Price UP
Sell Order -> Price DOWN

References:
- Decentralized Exchange
- Core Contract
- Algorithmic Matcher
- Algorithmic Marketmaker
- TokenA
- TokenB
Algorithmic DEX Example - Bancor

Token Bancor

Feature Tip: Track historical data points of any address with the analytics module!

Overview [ERC-20]

<table>
<thead>
<tr>
<th>PRICE</th>
<th>FULLY DILUTED MARKET CAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0.1999 @ 0.001031 Eth (-1.60%)</td>
<td>$13,826,012.43</td>
</tr>
</tbody>
</table>

| Total Supply: 69,148,641.563497… BNT |
| Holders: 23,706 addresses |
| Transfers: 2,596,732 |

\[
\text{price} = \frac{\text{connector balance}}{\text{Smart Token’s outstanding supply} \times CW}
\]
Industry Designs are more complexed

Kyber Network

Transaction Visibility
## Transaction Delay

<table>
<thead>
<tr>
<th>Overview</th>
<th>Internal Transactions</th>
<th>Event Logs (9)</th>
<th>State Changes</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Transaction Hash:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Status:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Block:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Timestamp:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. From:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. To:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Tokens Transferred:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Value:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Transaction Fee:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Transaction Hash:** 0xda6b1da028259823685eebdf8163665876c0b2256f1444244dc194049e32ed01
- **Status:** Success
- **Block:** 9933626, **2 Block Confirmations**
- **Timestamp:** 40 secs ago (Apr-24-2020 06:29:26 AM +UTC)
- **From:** 0xc828092697970751a6a86f259d73fc7726460e0
- **To:** 0x818e6f66cc3849da6684f3ec860887b755 (Kyber: Proxy)
- **Tokens Transferred:**
  - From 0x3c100e43cc0715... To Kyber: Contract 2 For 180.02328759 ($46.05) UniBright (UBT)
  - From Kyber: Contract 2 To 0xc82809269797075... For 180.02328759 ($46.05) UniBright (UBT)
- **Value:** 0.25 Ether ($46.96)
- **Transaction Fee:** 0.002829344 Ether ($0.53)

**Note:** Generally Required at least 7 Confirmations
Transaction Order is Not Guaranteed

Confirmed Block

Confirmed Block

Miner’s Block

TX8 is more likely to be included in a block along the chain

Pending TX Queue

- TX5, 0.01 Gwei
- TX6, 0.03 Gwei
- TX7, 0.02 Gwei
- TX8, 0.15 Gwei
Profit Through a Backge TX Order

TokenA price goes up

Algorithmic Exchange

TX1: Buys 1000 TokenA
0.01 Gwei

TX2: Buys 10 TokenA
0.02 Gwei

TX3: Sells 10 TokenA
0.009 Gwei
Another Frontrunning Scenario

[Diagram showing transactions between two Decentralized Exchanges (DEX A and DEX B).]

**TEX A**
- Decentralized Exchange
- Sell 1 for 5 ETH

**TEX B**
- Decentralized Exchange
- Buy 1 for 6 ETH

**Confirm TX**
- TX: Buy 5 from A and Sell to B
- 0.2 Gwei

**Pending TX**
- 0.1 Gwei

Bot
Another Frontrunning Scenario

**DEX A**
Decentralized Exchange

Sell 1 for 5 ETH

**DEX B**
Decentralized Exchange

Buy 1 for 6 ETH

TX: Buy 5 from A and Sell to B
0.3 Gwei

TX: Buy 5 from A and Sell to B
0.2 Gwei

Confirm TX

Bot*

Bot

Pending TX 0.1 Gwei
Another Frontrunning Scenario

**DEX A**
Decentralized Exchange
Sell 1 for 5 ETH

**DEX B**
Decentralized Exchange
Buy 1 for 6 ETH

Confirm TX
→ TX... 0.4 Gwei
→ TX... 0.3 Gwei
→ TX... 0.2 Gwei
→ Pending TX 0.1 Gwei
Another Frontrunning Scenario

Inefficiency to the blockchain
And Slows down the confirmation of other TXs
Scale of Frontrunning Bots

Fig. 3. Deployed PGA measurement infrastructure architecture.

Fig. 18. Pure revenue bot breakdown, as described in Section IV, showing revenue without subtracting transaction costs.
Frontrunning Vulnerability

- TX are visible to everyone
- TX takes time to get confirmed
- Pending TX can be reordered

= Frontrunning Attack!
Mitigation - Reduce Visibility

Decentralized Exchange Order Tracker

A total of 13,977,518 transactions found
(Showing the last 100k records)

<table>
<thead>
<tr>
<th>Txn Hash</th>
<th>Time</th>
<th>Maker</th>
<th>Taker</th>
<th>Price</th>
<th>DEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xda061da0282b9...</td>
<td>32 secs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0xdd0ca71f0f100a6...</td>
<td>32 secs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x3d30eac45d08a6...</td>
<td>2 mins</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x6b990a24a9c7e...</td>
<td>2 mins</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x54993aaf487256...</td>
<td>2 mins</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mitigation - Encryption

The Exchange Smart Contracts

Core Contract

Order Book

Matcher

I offer 1 TokenA for 2 TokenB

Maker

TokenA

I take the TokenA with 2 TokenB

Taker

TokenB
Mitigation - Encryption

Core Contract

Order Book

Matcher

1A for 2B

Maker

TokenA

“1A for 2B”

Taker

TokenB

The Exchange Smart Contracts

Wallet Address

Key

Key Map

Wallet Address
Mitigation - Encryption

"I offer ENCRYPT for ENCRYPT"

Core Contract

Trader

Order Book

The Exchange Smart Contracts

Maker

TokenA

Taker

"I take the ENCRYPT with ENCRYPT"

TokenB

Key

Matcher

Trade Info

Trusted Execution Environment (Inspired by Tesseart)
Countering Algorithmic Frontrunning

TokenA price goes up

Algorithmic Exchange

TX1: Buys 1000 TokenA
0.01 Gwei
Countering Algorithmic Frontrunning

Create Transaction:

???

???

TX1: Buys ENCRYPT
0.01 Gwei

Algorithmic Exchange

??? price goes up

Time
Countering Frontrunning Bot

**DEX A**
Decentralized Exchange

Sell 1 for 5 ETH

**DEX B**
Decentralized Exchange

Buy 1 for 6 ETH

TX: Buy 5 from A and Sell to B
0.2 Gwei

Confirm TX

Pending TX 0.1 Gwei
Countering Frontrunning Bot

What is E and how many?

TX: Buy E from A and Sell E to B
0.2 Gwei

Pending TX
0.1 Gwei

Bot

Bot*

Confirm TX

DEX A
Decentralized Exchange
Sell 1 for 5 ETH

DEX B
Decentralized Exchange
Buy 1 for 6 ETH
Our current progress

- Last semester, one of the research in the lab developed a blockchain network that allows cross-chain exchange between Bitcoin and Ethereum

- We got the task to survey current exchange, their vulnerabilities, and possible mitigations

- The lab group we work with are designing the protocol for communications between TEE and Blockchain Network.