### Surveying Front-running attacks on Decentralized Exchanges

Mingcheng & Sean

## Goal

• Introduce a special kind of attck on decentralized exchange

• Try to propose a mitigation in the end

### What is this?



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

Hash	000000000000000000056cf2b126dcebc27fd6d16879e2bcaed78343db4fb378 📋
Confirmations	1
Timestamp	2020-04-26 18:47
Height	627784
Miner	F2Pool

Hash

e4634fa7c50d9a334bd015a0f2e8f701b999881de21d05e6d0aed4...

12.87625877 BTC 🌐

12.56652188 BTC 🌐

12.94351828 BTC 🌐

12,72028600 BTC 🌐

12.66090120 BTC 🌐

12.59571369 BTC 🌐

12.56473076 BTC 🌐

12.54066334 BTC 🌐

12.54799571 BTC 🌐

12.61917307 BTC 🌐

1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY

#### Load more inputs... (9 remaining)

0.0000000 BTC (0.000 sat/B - 0.000 sat/WU - 3618 bytes) 2020-04-26 18:47

 1GX28yLjVWux7ws4UQ9FB4MnLH4UKTPK2z
 289.52436879 BTC (#)

 392NRxN3E2BaWjQMj6aa2EjLQDZxdECr7Y
 0.13870557 BTC (#)

 36p1iTj5sBzAYpV25e1vLe9Y77gwLFGv76
 0.04572787 BTC (#)

 1eUtsAo7hjVcA736UjryHiTohXhQEUwe7
 0.02884744 BTC (#)

 1LwpzfazVb9qDc4he6A4rPTPBCtC2c1tY1
 0.00530365 BTC (#)

 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY
 311.24788734 BTC (#)

Fee Reward

0.08282373 BTC

600.99084066 BTC

**1** Confirmations

Fee

## Blockchain workflow: block and block generation

Hash



Confirmations	1
Timestamp	2020-04-26 18:47
Height	627784
Miner	F2Pool
Number of Transactions	2,300
Difficulty	15,958,652,328,578.42
Merkle root	afcb304adfb2344d9c41037ffe42cd6d9154ffef89a08a19733de8aa6fee3e9f
Version	0×20002000
Bits	387,031,859
Weight	3,998,680 WU
Size	1,108,855 bytes
Nonce	1,238,489,672
Transaction Volume	3168.84300466 BTC
Block Reward	12.5000000 BTC
Fee Reward	0.08282373 BTC



# 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

Hash	000000000000000000056cf2b126dcebc27fd6d16879e2bcaed78343db4fb378 📋				
Confirmations	1				
Timestamp	2020-04-26 18:47				
Height	627784				
Miner	F2Pool				
Number of Transactions	2,300				
Difficulty	15,958,652,328,578.42				
Merkle root	afcb304adfb2344d9c41037ffe42cd6d9154ffef89a08a19733de8aa6fee3e9f				
Version	0×20002000				
Bits	387,031,859				

neration fee	1,108,855 bytes	
Nonce	1,238,489,672	
Transaction Volume	3168.84300466 BTC	
Block Reward	12.5000000 BTC	
Fee Reward	0.08282373 BTC	8

### Blockchain workflow: broadcast and census

Hash

Fee

e4634fa7c50d9a334bd015a0f2e8f701b999881de21d05e6d0aed4...

1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY

Load more inputs... (9 remaining)

12.87625877 BTC (1) 12.56652188 BTC (1) 12.94351828 BTC (1) 12.72028600 BTC (1) 12.66090120 BTC (1) 12.59571369 BTC (1) 12.56473076 BTC (1) 12.54066334 BTC (1) 12.54799571 BTC (1) 12.61917307 BTC (1) 2020-04-26 18:47

IGX28yLjVWux7ws4UQ9FB4MnLH4UKTPK2z	289.52436879 BTC 🏶
392NRxN3E2BaWjQMj6aa2EjLQDZxdECr7Y	0.13870557 BTC 🏶
36p1iTj5sBzAYpV25e1vLe9Y77gwLFGv76	0.04572787 BTC 🏶
leUtsAo7hjVcA736UjryHiTohXhQEUwe7	0.02884744 BTC 🏶
ILwpzfazVb9qDc4he6A4rPTPBCtC2c1tY1	0.00530365 BTC 🏶
IKFHE7w8BhaENAswwryaoccDb6qcT6DbYY	311.24788734 BTC 🏶

600.99084066 BTC

### Blockchain workflow: broadcast and census

• If divert, the chain has been seen

• To keep consistent, bitcoin is desi mins by adjusting the difficulty lev

Hash	00000000000000000056cf2b126dcebc27fd6d16879e2bcaed78343db4fb378 📋
Confirmations	1
Timestamp	2020-04-26 18:47
Height	627784
Miner	F2Pool
Number of Transactions	2,300
Difficulty	15,958,652,328,578.42
Merkle root	afcb304adfb2344d9c41037ffe42cd6d9154ffef89a08a19733de8aa6fee3e9f
Version	0×20002000
Bits	387,031,859
Weight	3,998,680 WU
Size	1,108,855 bytes
Nonce	1,238,489,672
Transaction Volume	3168.84300466 BTC
Block Reward	12.5000000 BTC
Fee Reward	0.08282373 BTC

### 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 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 Etheruem 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 >= Gas needed
- Gas Fee = Gas Limit \* Gas Price (Gwei)
- Gas Fee is the maximum profit code runner can get



#### Gas Needed

### The Scale of Ethereum Network

• Ethereum is now the 2nd largest blockchain Network in th world

Market Cap = \$ 20+ Billion

• Frequent Transactions



Data Collected from etherscan https://etherscan.io/

### ICO on Ethereum = Fundraising



it allow direct interaction bewteen parties)

### 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



TokenC

### **Centralized Exchange**

#### Centralized Exchange







### Algorithmic DEX Example - Bancor

Token Banco	r	
Bancor Liquidity		
Feature Tip: Track h	istorical data points c	of any address with the <b>analytics module !</b>
Overview [ERC-20]		
PRICE		FULLY DILUTED MARKET CAP 3
\$0.1999 @ 0.001031 Eth	1 (-1.60%)	\$13,826,012.43
Total Supply:	69,148,641	I.563497 BNT 🗓
Holders:	23,706 add	Iresses
Transfers:	2,596,732	
Transfers:	2,596,732	

 $price = \frac{connector \ balance}{Smart \ Token's \ outstanding \ supply \times \ CW}$ 

### Industry Designs are more complexed



**Kyber Network** 

"Kyber: An On-Chain Liquidity Protocol," Apr. 22, 2019. https://files.kyber.network/Kyber\_Protocol\_22\_April\_v0.1.pdf (accessed Apr. 13, 2020).

### **Transaction Visibility**

Etherscan		۵	All Filters V Search by Address / Txn Hash / Block / Token / Ens			/ Ens	٩			
Eth: \$187.83 (+4.98%)				Home E	Blockchain 🗸	Tokens ~	Resources -	More ~	<b>9</b> Sign In	\$
Decentralized Exchange	e Order Tracker									
Select DEX 👻 🌔 DEX Pie Chart	≓ Order Books									٩
A total of 13,977,518 transactions (Showing the last 100k records)	found						First <	Page 1 of 4	1000 >	Last
Txn Hash	Time	Maker		Taker			Price		DE	x
0xda6b1dba028259	32 secs ago	0.25 ETH	-	180.023	328759 UBT		0.001388	37 ETH	0	
0xddca7f140f180a6	32 secs ago	0.049925 ETH	-	• 9.351305 USDC		0.0053388 ETH		6		
0x36c8eac45dc8e6	2 mins ago	0.106921005702961 ETH	-	20 PAX			0.005346	6 <mark>1 ET</mark> H	0	
0x6b990a24a9cc7e	2 mins ago	200 USDT	-	1.06531	4612 WETH		0.005326	6 WETH	0	
0x54993aaff487256	2 mins ago	0.0137183 ETH	8	117.782	491140038 PM	NK	0.000116	5 ETH	0	

### **Transaction Delay**

Overview Internal Transactions	Event Logs (9) State Changes Comments
⑦ Transaction Hash:	0xda6b1dba028259823681eebfd8163665876c0b2256f444244dc194049e32ed01
⑦ Status:	Success
⑦ Block:	9933626 2 Block Confirmations Generally Required at least 7 Confirmations
⑦ Timestamp:	© 40 secs ago (Apr-24-2020 06:29:26 AM +UTC)
⑦ From:	0xc828092697970751a6e86f259d73fcf7726460e0
⑦ To:	Q Contract 0x818e6fecd516ecc3849daf6845e3ec868087b755 (Kyber: Proxy)      C     L TRANSFER 0.25 Ether From Kyber: Proxy To → Kyber: Contract 2     L TRANSFER 0.25 Ether From Kyber: Contract 2 To → 0xfe08bc8bc12595c1c871
⑦ Tokens Transferred: 2	From 0x3c100e43cc0715       To       Kyber: Contract 2       For       180.02328759 (\$46.05)       Image: UniBright (UBT)         From Kyber: Contract 2       To       0xc8280926979707       For       180.02328759 (\$46.05)       Image: UniBright (UBT)
⑦ Value:	0.25 Ether (\$46.96)
⑦ Transaction Fee:	0.002829344 Ether (\$0.53)



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

### ProfitrTuhroinghAttaakge TX Order

TokenA price goes up











### Scale of Frontrunning Bots



Fig. 3. Deployed PGA measurement infrastructure architecture.

Philip Daian, Steven Goldfeder, et al. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instabil® in Decentralized Exchanges". *ArXiv* abs/1904.05234 .2019.

### Scale of Frontrunning Bots



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

Philip Daian, Steven Goldfeder, et al. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instabil® in Decentralized Exchanges". *ArXiv* abs/1904.05234 .2019.

### Frontrunning Vulnerability



Frontrunning Attack!

### Mitigation - Reduce Visibility

Eth: \$187.83 (+4.98%)		All Filters	All Filters v Search by Address / Txn Hash / Block / Token / Ens					
		Home	Home Blockchain - Tokens -			Resources - More - OSign In		
Decentralized Exchange	e Order Tracker							
Select DEX 👻 🏟 DEX Pie Chart	. # Order Books							٩
A total of 13,977,518 transactions (Showing the last 100k records)	s found					First <	Page 1 of 4	4000 > Last
Txn Hash	Time	Maker	Take	er		Price		DEX
0xda6b1dba028259	32 secs ago		-					()
0xddca7f140f180a6	32 secs ago		-					(\$
0x36c8eac45dc8e6	2 mins ago		-					()
0x6b990a24a9cc7e	2 mins ago		-					Q
0x54993aaff487256	2 mins ago		-					0







### **Countering Algorithmic Frontrunning**

TokenA price goes up



### **Countering Algorithmic Frontrunning**



### **Countering Frontrunning Bot**



### **Countering Frontrunning Bot**



### **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 protocl for communications between TEE and Blockchain Network.