

The background of the image is a composite. It features a Shiba Inu dog's head and shoulders emerging from a large, billowing cloud of orange-brown dust or smoke. This cloud is positioned over a high-angle, aerial view of a city with a grid-like street pattern. The sky in the background is a mix of orange, yellow, and grey, suggesting a sunset or sunrise. The overall tone is dramatic and somewhat ominous.

**MEV**

**Dark Forest**と**Front-Running**

**ETHEREUM**

やさしくないDeFi by udon.eth

CIXIN LIU

TRANSLATED BY JOEL MARTINSEN

# THE DARK FOREST

"Vivid, imaginative  
and rooted in cutting-  
edge science... Cixin  
stands at the top tier  
of speculative fiction"

DAVID BRIN



迷いの森

セーブ中

AM 10:00



# Ethereum is a Dark Forest

- Dark Forestの由来は、ParadigmのDan Robinsonが書いた、「[Ethereum is a Dark Forest](#)」という記事

そこで書かれていたこと

- ある人がUniswapのLPトークンをLPコントラクトアドレスに送ってしまった
- 引き出しはとても簡単にできる。できるが、誰でも実行して受け取れる
- Ethereumの世界にはGeneralized Front-running Botがいるので、簡単にポチッと実行すればいいだけではない...
- Generalized Front-Runnerは、mempoolにあるあらゆるtxを監視し、資金を横取りできそうなものを選別し、自分が横取りしようと実行するbot



# Ethereum is a Dark Forest

- いろんなエンジニアの手を借りて難読化を試みた。txを二つに分割し、一回ではできないようにした。
- けれどInfuraがエラーを返したこともあり、二つ目のtxを次のブロックに入れたら、、、その間にFront-runnerが奪い去った



# Front-runningってそもそも何？

ある取引をみた上で、それに先回りしてFront-runnerがtxを送ることで利益を得ること。









- 例)
  - 現在の売値は100円に1単位、102円に1単位
  - 1単位分の成行買注文があり、それを検知したFront-Runnerはすぐさま100円の売り板を約定し、101円に1単位の売り注文を置く
  - 1単位分の成行買注文は101円で約定する。Front-runnerは1円ほぼノーリスクで抜ける

# Ethereumの世界でのFront-Running

- EthereumではMinerがブロックにいれるtxとその実行する順番を決めているため、Minerは潜在的にtxから価値を抽出できる(Miner Extractable Value = MEV)
- DeFiが出てきたことによって、MEVはさらに増大した。特に自らFront-Runningすれば莫大な価値を得ることができる。
  - Arbitrage
  - ICOの優先参加
  - 精算

# MinerによるMEV抽出の実例

- 異常にやすいtx(<https://twitter.com/FrankResearcher/status/1311350189131616256>)



Block 10840267 mined by Spark Pool				
0x51bf0d49542d...	 Binance USD 0x4fab...	0.00000 ETH	0.00003 ETH	1 GWei
0x51bf0d49542d...	 Curve.fi: BUSD Deposit 0xb6c0...	0.00000 ETH	0.00076 ETH	1 GWei
0x5159748551e2...	0x778a2537b38e...	0.01000 ETH	0.00420 ETH	200 GWei
0xcdef4f34e5ce...	 Tether USD 0xdac1...	0.00000 ETH	0.00742 ETH	180 GWei
0xf8bb041e3395...	0x74cb7c657163...	0.04597 ETH	0.00378 ETH	180 GWei
0x95b564f3b3ba...	 Loopring: LRC Token 0xbbbb...	0.00000 ETH	0.00903 ETH	174 GWei
0xf57bce0083c9...	 0x3c9d954a5e9f...	0.00000 ETH	0.02424 ETH	165 GWei
Huobi 4 0xeee2...	 Tether USD 0xdac1...	0.00000 ETH	0.00888 ETH	158 GWei
Huobi 7 0xad2...	 Tether USD 0xdac1...	0.00000 ETH	0.00651 ETH	158 GWei
Huobi 9 0x1062...	 Tether USD 0xdac1...	0.00000 ETH	0.00651 ETH	158 GWei



# MinerによるMEV抽出の実例
















- 不自然な順番のblock(<https://twitter.com/FrankResearcher/status/1311350197176471552>)

## Block 10813361 mined by F2Pool

0xb6a9c3926027...	 Uniswap V2: Router 2 0x7a25...	0.00000 ETH	0.01311 ETH	105 GWei
0x0e916f50c4ac...	0xb235d9148da3...	10.76930 ETH	0.00525 ETH	250 GWei
0x8aa1adb7829a...	0x997771cd503a...	2.63217 ETH	0.00525 ETH	250 GWei
0x6c2d992b7739...	 0x: Exchange v3 0x6193...	0.00000 ETH	0.00764 ETH	211 GWei
0x07f4098af304...	0x12993fde6c72...	0.03000 ETH	0.00420 ETH	200 GWei
0x07f4098af304...	0x20dad5d0df3f...	0.03000 ETH	0.00420 ETH	200 GWei
Paykassa Inc. 0x5d9f...	0x9981585db0b0...	0.07417 ETH	0.00420 ETH	200 GWei
0x07f4098af304...	0x0e27dd96df87...	0.03000 ETH	0.00420 ETH	200 GWei

# MinerによるMEV抽出の実例

- Arbを優先的に行う(<https://twitter.com/FrankResearcher/status/1311350204067729409>)

Transaction Hash:	0x36ff2bf6da4ee59974944805c2f64545fa8932474fd1c56c6fa51e8df3904ba4 
Status:	 Success
Block:	Mined by 2Miners: PPLNS 10960155 4750 Block Confirmations
Timestamp:	🕒 17 hrs 52 mins ago (Sep-29-2020 10:56:10 PM +UTC)   ⌚ Confirmed within 17 secs
From:	0xa2cd5b9d50d19dfd2f37cbae0e880f9ce327837 
Interacted With (To):	 Contract 0xf451b59d6db7a6601b15d6250624db7329867bae   ↳ TRANSFER 8 Ether From 0xf451b59d6db7a6601b15d6... To → 0xed2c5bac5baedb7a59f871... ↳ TRANSFER 8.023132686269838988 Ether From Wrapped Ether To → Uniswap V2: Route... ↳ TRANSFER 8.023132686269838988 Ether From Uniswap V2: Route... To → 0xf451b59d6db7a6601b15d6...
Transaction Action:	↳ Swap 2,868.983768  USDC For 8.023132686269838988 Ether On  Uniswap
Tokens Transferred: 	↳ From 0xed2c5bac5baedb... To 0xf451b59d6db7a6... For 0.116592970427504532 (\$2,803.71)  yearn.financ... (YFI) ↳ From 0x0000000000000000... To 0xf451b59d6db7a6... For 0.000152154611125654  Mooniswap V1... (MOON-V...) ↳ From DODO: YFI-USDC To 0xf451b59d6db7a6... For 2,868.983768 (\$2,868.98)  USD Coin (USDC) ↳ From 0xf451b59d6db7a6... To DODO: YFI-USDC For 0.116592970427504532 (\$2,803.71)  yearn.financ... (YFI) ↳ From 0xf451b59d6db7a6... To Uniswap V2: USDC 3 For 2,868.983768 (\$2,868.98)  USD Coin (USDC) ↳ From Uniswap V2: USDC 3 To Uniswap V2: Router 2 For 8.023132686269838988 (\$2,871.56)  Wrapped Ethe... (WETH)

# MinerによるMEV抽出の実例

- Arbを優先的に行う(<https://twitter.com/FrankResearcher/status/1311350204067729409>)

Transaction Hash:	0x6b84d6c7d7377eb2bd7990e803aae2b557c2d0fb77f04f8fcadcaadc00457689
Status:	Success
Block:	Mined by 2Miners: SOLO 10872963 91947 Block Confirmations
Timestamp:	14 days 5 hrs ago (Sep-16-2020 11:45:47 AM +UTC)
From:	0x67fdb08f645cae74607b807d14c09c400ef4f6b7
Interacted With (To):	Contract 0xf451b59d6db7a6601b15d6250624db7329867bae L TRANSFER 8 Ether From 0xf451b59d6db7a6601b15d6... To → 0x75116bd1ab4b0065b44e1... L TRANSFER 8.067826667023362375 Ether From Uniswap: DAI To → 0xf451b59d6db7a6601b15d6...
Tokens Transferred:	3 From 0x75116bd1ab4b00... To 0xf451b59d6db7a6... For 2,862.899396176271975011 (\$2,891.53) Dai Stableco... (DAI) From 0x0000000000000000... To 0xf451b59d6db7a6... For 0.108640571204001516 Mooniswap V1... (MOON-V...) From 0xf451b59d6db7a6... To Uniswap: DAI For 2,862.899396176271975011 (\$2,891.53) Dai Stableco... (DAI)
Value:	0 Ether (\$0.00)

# Escaping the Dark Forest

- Dark Forestからの脱出に成功したところもある。  
(<https://samczsun.com/escaping-the-dark-forest/>)
- LienというDeFiの一つにETHを引き出してしまうバグを見つけたWhite hackerが、Spank Poolに連絡し救出txを直接SpankPool(Mining Pool)に送り、mempoolに載せずに実行し解決した。

# Front-Runningから逃れるために

## 自己対策

- Swap系のProtocolを使うときは、Slippageを流動性もみつつなるべく低めに設定
- 巨額のSwapはGas PriceをFastより上に設定する。(Chef Nomiを見習う!)

## 未来

- StarkwareのVeedoとかでtxの処理順番にランダム性を持たせる
- Patch処理(利便性に難ありなのでL2前提?)