

---

---

# the many sins of web3

stephen morgan

---

—

**\$ whoami**

**Security Consultant**  
**Penetration Tester**  
**Application Security Engineer**  
**Recovering cryptocurrency user**



# blockchains

## technical

decentralised network

consensus mechanism

cryptography

smart contracts

## financial

LINE GO UP

## political

libertarianism

financial freedom

fiat (pejorative)



## **overview**

decentralisation

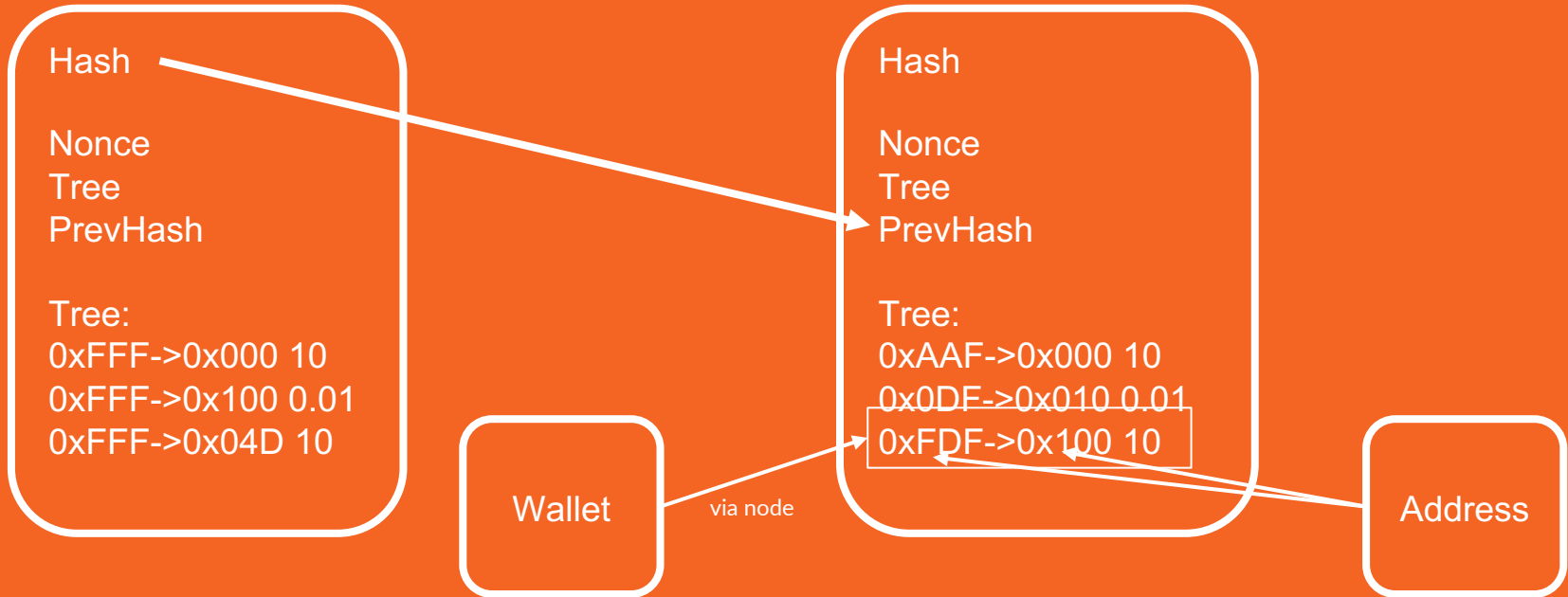
censorship resistance

privacy

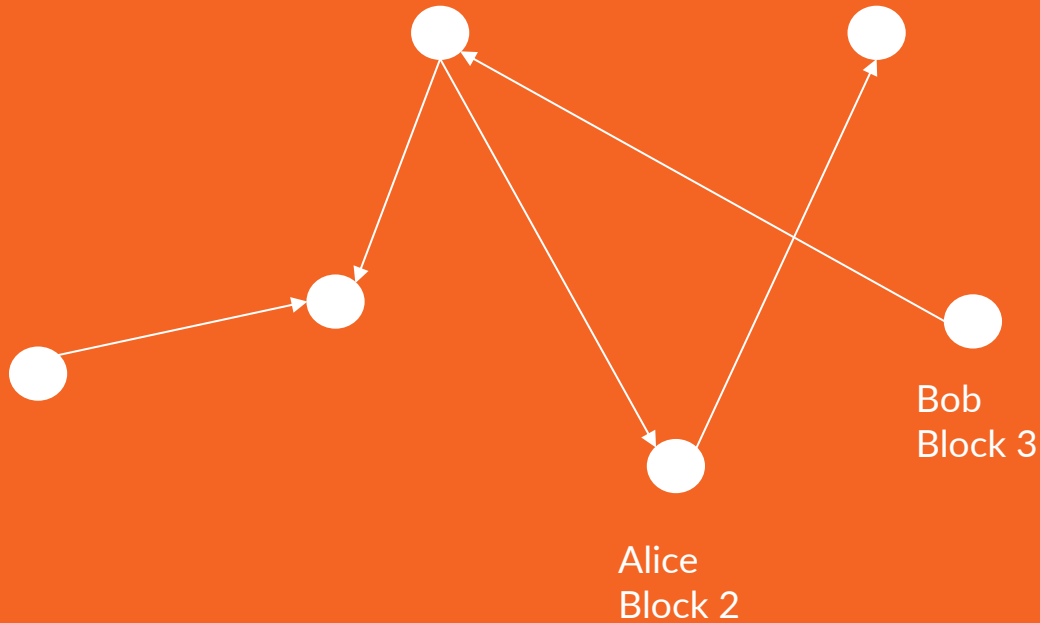
Code is Law

surprise!

# blockchains



# The network



## **gossip**

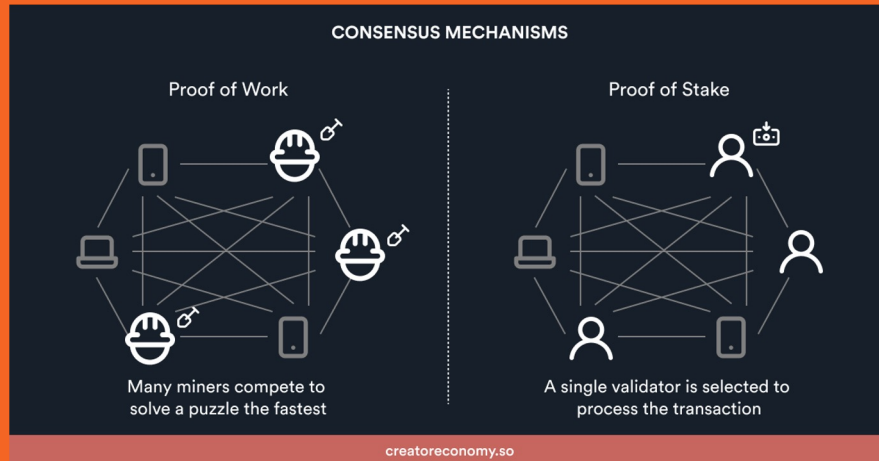
node address

unconfirmed transactions

blocks

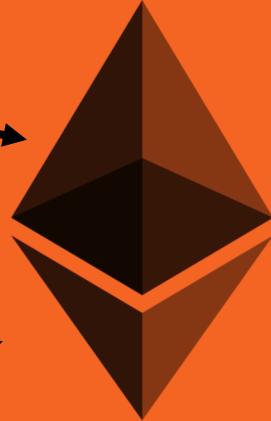
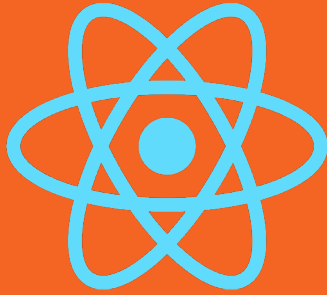
# Proof of Work

$\text{sha256}(\text{block}, \text{math.rand}()) < \text{difficulty}$





# smart contracts



```
pragma solidity ^0.4.17;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

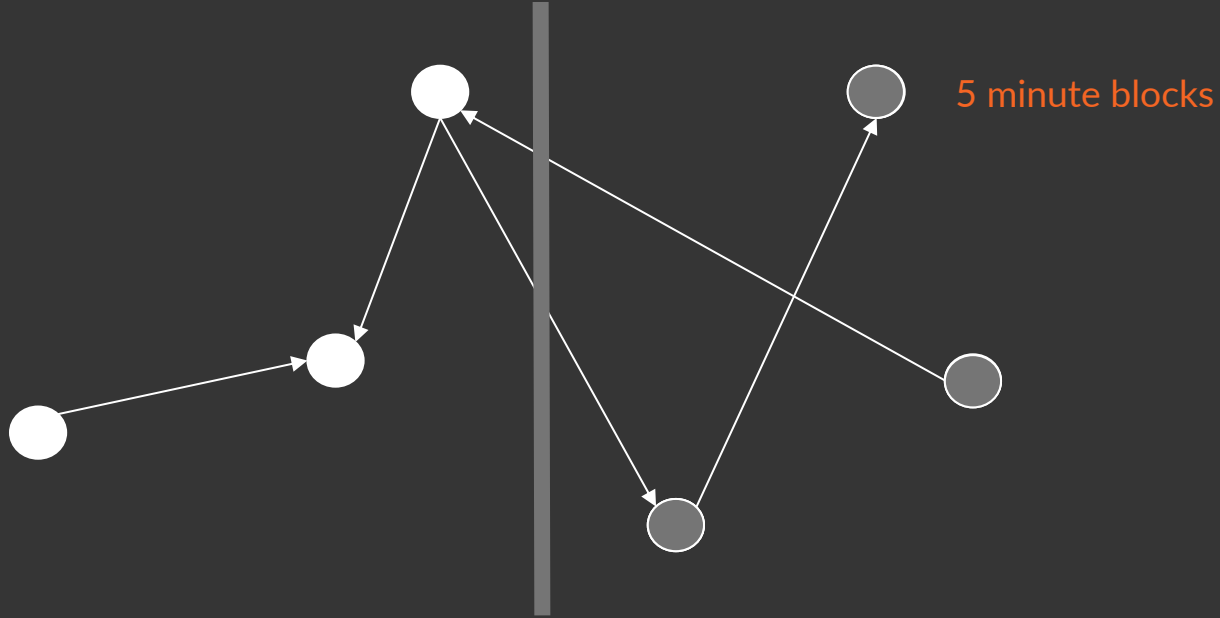
---

# decentralisation

## Political origin

“the transfer of control and decision-making from a centralized entity (individual, organization, or group thereof) to a distributed network. Decentralized networks strive to reduce the level of trust that participants must place in one another, and deter their ability to exert authority or control over one another” - AWS

# decentralisation



---

# decentralisation

Moxie Marlinspike:

“When people talk about blockchains, they talk about distributed trust, leaderless consensus, and all the mechanics of how that works, but often gloss over the reality that clients ultimately can’t participate in those mechanics”

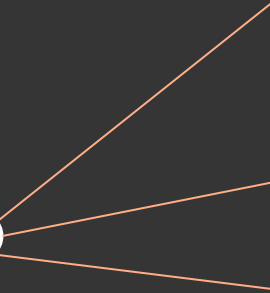
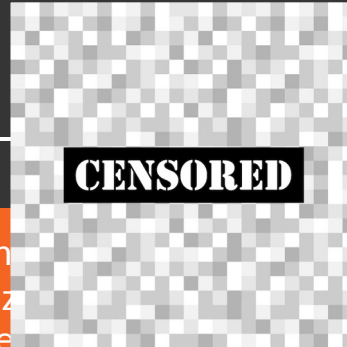
# decentralisation



\$\$

TCP

# decentralisation



“Partisans of the blockchain may be okay if these types of centralization emerge, because the state itself is a function of the blockchain, so if these platforms misbehave clients can simply move elsewhere. However, I would suggest that this is a very simplistic view of the dynamics that make platforms what they are.”

# Moxie's Law of Decentralisation

$$\Sigma d = \min \{ \Omega_1 f_1, \Omega_2 f_2, \Omega_3 f_3 \dots \Omega_n f_n \}$$

“Any given transaction is only as decentralised as its most centralised component.”





# bitcoin decentralisation

core developers:

five developers with  
merge permission

? uploads binary to  
bitcoincore.org

NODES DISTRIBUTION BY USER AGENTS		
16905 nodes as of Mon Jun 26 20:39:24 2023 NZST		
1. Satoshi:24.0.1 (4981)	2. Satoshi:23.0.0 (3439)	3. Satoshi:25.0.0 (2807)
4. Satoshi:22.0.0 (2671)	5. Satoshi:0.21.1 (600)	6. Satoshi:0.20.1 (543)
7. Satoshi:0.21.0 (285)	8. Satoshi:24.0.0 (217)	9. Satoshi:24.1.0 (214)
10. Satoshi:0.20.0 (167)	11. Satoshi:25.99.0 (100)	12. Satoshi:24.99.0 (100)
13. Satoshi:0.18.0 (87)	14. Satoshi:23.1.0 (69)	15. Satoshi:0.19.1 (56)
16. Satoshi:0.17.1 (53)	17. Satoshi:0.18.1 (51)	18. Satoshi:23.99.0 (39)
19. Satoshi:0.19.0.1 (36)	20. Satoshi:0.16.3 (34)	21. Satoshi:0.21.2 (28)
22. Satoshi:0.14.99 (27)	23. Satoshi:22.99.0 (26)	24. btcwire:0.5.0 (24)
25. Satoshi:0.17.0 (18)	26. Satoshi:21.99.0 (15)	27. Satoshi:0.17.0.1 (15)
28. Satoshi:0.12.1 (13)	29. Satoshi:22.1.0 (12)	30. Satoshi:0.16.0 (10)
31. Satoshi:0.14.2 (9)	32. Satoshi:0.17.2 (9)	33. Satoshi:0.15.1 (8)
34. bcoin:2.2.0 (8)	35. Satoshi:21.2.0 (7)	36. Satoshi:0.13.0 (7)
37. Satoshi:0.20.99 (7)	38. Satoshi:0.16.2 (7)	39. Gocoin:1.10.3pre (7)
40. Satoshi:0.17.99 (6)	41. BitcoinPoS:0.21.3 (5)	42. bcoin:2.1.2 (5)
43. KIT-DSN:0.17.0 (5)	44. Satoshi:0.15.2 (4)	45. Aurum:0.12.4 (3)
46. Satoshi:1.0.0 (3)	47. Satoshi:0.16.99 (3)	48. Satoshi:0.19.99 (3)
49. Satoshi:0.18.99 (3)	50. Satoshi:25.99.0 (3)	51. Satoshi:0.20.2 (3)
52. QR5nap:23.0.0 (2)	53. Satoshi:0.9.0 (2)	54. CKCoinD:25.0.0 (2)
55. Satoshi:0.15.0.1 (2)	56. Satoshi:0.16.1 (2)	57. CKCoinD:0.21.1 (2)
58. Satoshi:0.9.1 (2)	59. therealbitcoin.org:... (2)	60. Satoshi:23.2.0 (2)
61. SupportPR#26525:23... (2)	62. Satoshi:0.13.1 (2)	63. Satoshi:0.15.99 (2)
64. Satoshi:0.19.2 (2)	65. Satoshi:0.13.2 (2)	66. Satoshi:0.15.0 (2)
67. BitcoinPoS:0.21.2 (2)	68. Satoshi:0.44.0 (2)	69. Satoshi:0.14.1 (2)
70. Satoshi:22.69.0 (2)	71. Satoshi:0.44.1 (1)	72. Bitcoin ABC:0.15.1 (1)
73. BitcoinUnlimited:1... (1)	74. Satoshi:0.19.0 (1)	75. Satoshi:0.8.3 (1)
76. Bitcoin ABC:0.14.6 (1)	77. Satoshi:0.12.0 (1)	78. Satoshi:0.10.3 (1)
79. Classic:1.2.0 (1)	80. BitcoinStaking:0.21... (1)	81. Satoshi:0.8.6 (1)
82. Satoshi:1.14.5 (1)	83. Satoshi:0.21.99 (1)	84. Eclipse:25.99.0 (1)
85. bcoin:v1.0.0-beta.14 (1)		

“service denial”

“transaction bug”

# Moxie's Law of Decentralisation

$$\Sigma d = \min \{ \Omega_1 f_1, \Omega_2 f_2, \Omega_3 f_3 \dots \Omega_n f_n \}$$

“Any given transaction is only as decentralised as its most centralised component.”

---

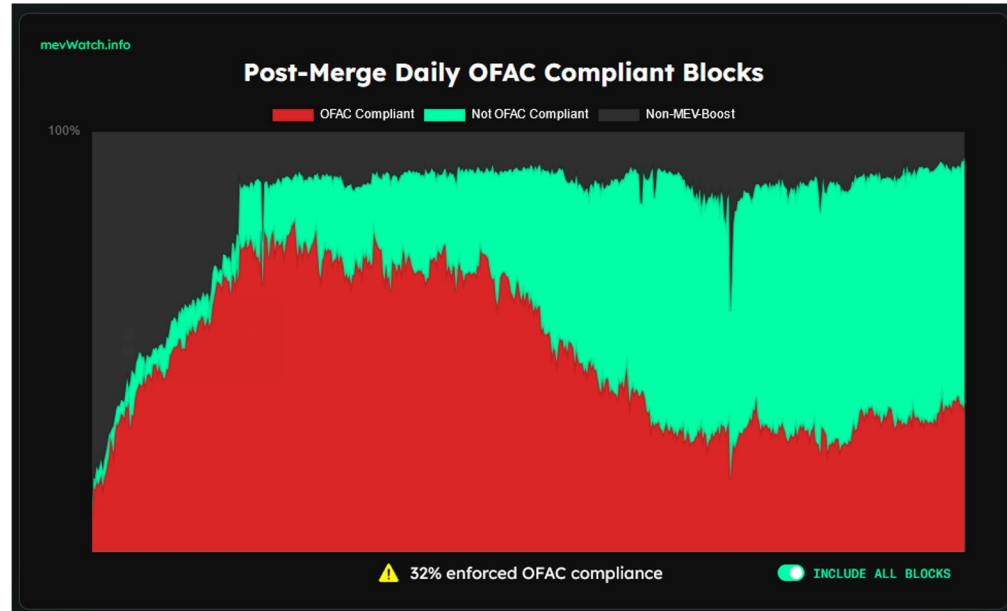
# censorship resistance



# —

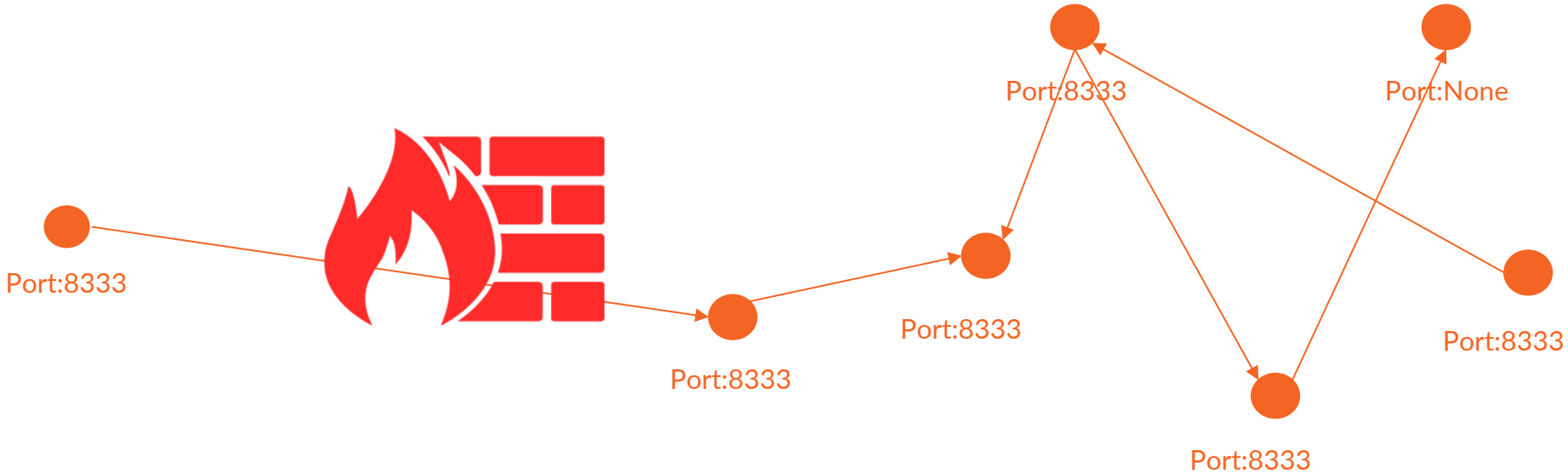
# ensorship resistance

1. The immutability of transactions
2. The freedom from confiscation
3. The freedom to transact



# —

# censorship resistance



# —

# ensorship resistance

Is the Bitcoin Network  
encrypted?  
It is NOT

Network	Magic value	Sent over wire as
main	0xD9B4BEF9	F9 BE B4 D9
testnet/regtest	0xDAB5BFFA	FA BF B5 DA
testnet3	0x0709110B	0B 11 09 07
signet(default)	0x40CF030A	0A 03 CF 40
namecoin	0xFEB4BEF9	F9 BE B4 FE



XBOX LIVE

As Censorship Resistant as Bitcoin

Etherscan Home Blockchain Tokens NFTs Resources Developers More | Sign In

### Transactions

TRANSACTIONS (24H)

**925,771** (8.87%)

PENDING TRANSACTIONS (LAST 1H)

**165,203** (Average)

NETWORK TRANSACTIONS FEE (24H)

**486.45 ETH** (10.13%)

AVG. TRANSACTION FEE (24H)

**4.25 USD** (4.51%)

More than 2,019,044,819 transactions found  
(Showing the last 500k records)

First < Page 1 of 10000 > Last

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
<a href="#">0xe69a900f67956d91d...</a>	Transfer	17610981	16 secs ago	<a href="#">beaverbuild</a>	Fee Recipient: <a href="#">0xE3...8...</a>	0.037746109 ETH	0.00030228
<a href="#">0x33e280022035d4e4...</a>	Mint Batch	17610981	16 secs ago	<a href="#">marsfactory.eth</a>	<a href="#">0x1EB73F...bA14a17E</a>	0.00414 ETH	0.00487502
<a href="#">0x0bfe1da1e81e5e640...</a>	Execute	17610981	16 secs ago	<a href="#">0x1f3CE5...861AC51d</a>	Uniswap: Universal Ro...	0.1 ETH	0.00224126
<a href="#">0x6fed3af114b20a535...</a>	Execute	17610981	16 secs ago	<a href="#">0xEb8E96...11002f94</a>	Uniswap: Universal Ro...	0 ETH	0.00263096
<a href="#">0xeb29915cf7a43df0e...</a>	Transfer	17610981	16 secs ago	<a href="#">0x588de3...91F21ad1</a>	Tether: USDT Stablecoin	0 ETH	0.00091399
<a href="#">0x16b7001b5427feacc...</a>	Transfer	17610981	16 secs ago	<a href="#">0x511815...08711E5D</a>	<a href="#">0x9e32AE...31C0B517</a>	1.242 ETH	0.00030438
<a href="#">0x0bc0bf06dfbe462c2...</a>	Transfer	17610981	16 secs ago	<a href="#">0xC409DE...4976531b</a>	<a href="#">0x7b4089...699E891e</a>	0.03 ETH	0.00030438
<a href="#">0xcbd4d9d6346caf006...</a>	Transfer	17610981	16 secs ago	<a href="#">0xF7ef39...4546d2e5</a>	ADreward: AD Token	0 ETH	0.00085937
<a href="#">0x4d67348e36f772ea8...</a>	Transfer	17610981	16 secs ago	<a href="#">0x272183...44f6C0FF</a>	<a href="#">0xa08287...81D8f48e</a>	0.009256012 ETH	0.00030438
<a href="#">0x1999d1f9da886987f...</a>	Create	17610981	16 secs ago	<a href="#">0x7ae9A8...15368762</a>	<a href="#">0xC549d8...f7CA86eb</a>	0.155511811 ETH	0.0033994
<a href="#">0x21ca6a76074e9cc2...</a>	Transfer	17610981	16 secs ago	<a href="#">0x61C282...75dd0960</a>	<a href="#">0x483bEb...Db00a855</a>	0.042 ETH	0.00030438
<a href="#">0xb690bfc80d3337538...</a>	Transfer	17610981	16 secs ago	<a href="#">0x2360C9...e2dEdD2E</a>	<a href="#">0x87952F...7B8380dc</a>	0.002 ETH	0.00030438
<a href="#">0xbccaca19633fb5b9f...</a>	Register	17610981	16 secs ago	<a href="#">0x6Ed4d...7203D27b</a>	ENS: ETH Registrar Co...	0.002615917 ETH	0.00557705
<a href="#">0xd92e2b262ab016e5...</a>	Transfer	17610981	16 secs ago	<a href="#">0xA0Db0f...034E661A</a>	<a href="#">0xff9B0d...b7D8945b</a>	0.988722089 ETH	0.00030438

"The main properties:

- Double-spend
- No mint or oth
- **Participants**
- New coins are
- The proof-of-v

# privacy

You are anonymous if you:

1. Mine the coin yourself
2. Never spend it

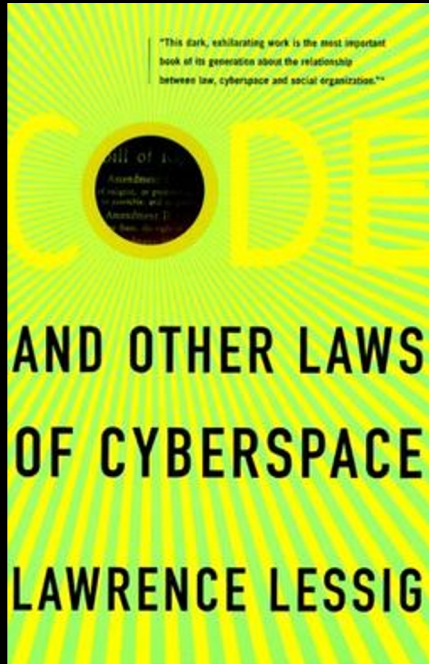
You are de-anonymised if you:

- Buy from a centralised exchange
- Purchase anything off chain
- Use a node provider
- Use a Wallet mobile app
- Connect your wallet to another service

**“Public blockchains are anonymous if you never touch the sides” - Me**



# Code is Law



Ethereum Classic Learn Play News

FAQs Opinionated Content

## Code is Law

February 22, 2022

### Key Points

- Blockchain technology and Smart Contracts have the potential to unlock a new era of human flourishing.
- The value that Smart Contract Platforms introduce is *Code is Law*, the ability to *Build Unstoppable Applications*.
- If positively engaged with, *Code is Law* will be hugely beneficial; those who attempt to stifle its adoption will be left behind.
- Change is likely to disrupt powerful institutions, who may fight against technology that threatens their position.
- Only blockchains committed to *Code is Law* are suitable to take on this challenge; others will become captured.
- Today, most blockchain projects, including Ethereum™, are not committed to *Code is Law*, undermining their value proposition.

---

# Code is Law

## **falsification principle:**

“A theory or hypothesis can be disproven by evidence”

“A theory can never be proven to be true”

## **securifiability principle:**

“A system can never be considered ‘secure’, it can only have no known vulnerabilities.”


 **Contract** 0x395604F1Db081376D0FE5dC9F154d0946065CcAb  

Buy ▾

Exchange ▾

Earn ▾

Gaming ▾

Warning! There are reports that this address was used in a scam. Please exercise caution when interacting with this address. 

 Ethereumfund.io 1 

Source Code

# Scam



More ▾

### Overview

ETH BALANCE

0 ETH

ETH VALUE

\$0.00

TOKEN HOLDINGS

\$0.04 (2 Tokens)



### More Info

PRIVATE NAME TAGS

+ Add

CONTRACT CREATOR

[0xa51048...8E91fa08](#) at txn [0xec337fbc...](#)

### Sponsored

 **Blockscan Chat** <sup>Ad</sup>

Wallet-to-wallet instant messaging platform.



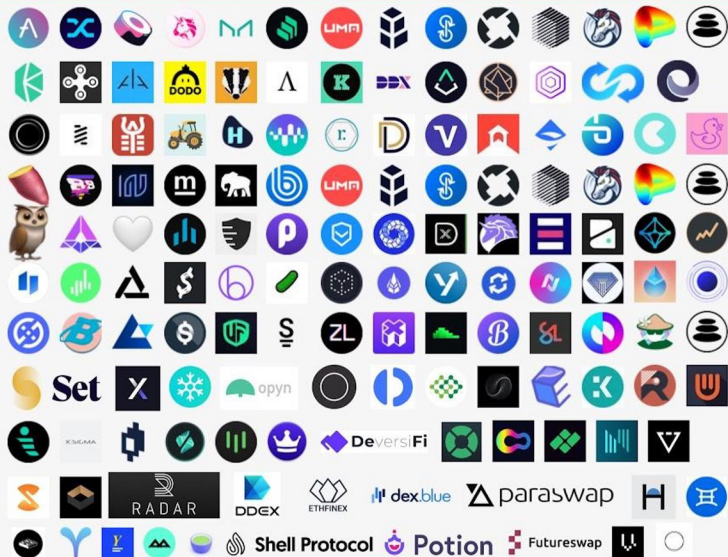
Address: [0xB8c77482e45F1F44dE1745F52C74426C631bDD52](#)

Address: [0xdAC17F958D2ee523a2206206994597C13D831ec7](#)

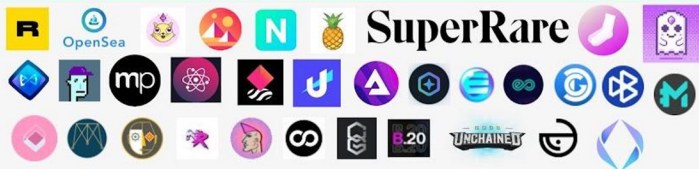
DAO approved

# Ethereum Ecosystem

## DeFi



## NFTs



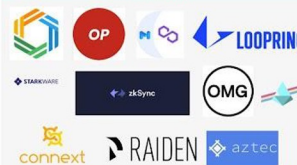
## Centralized Exchanges



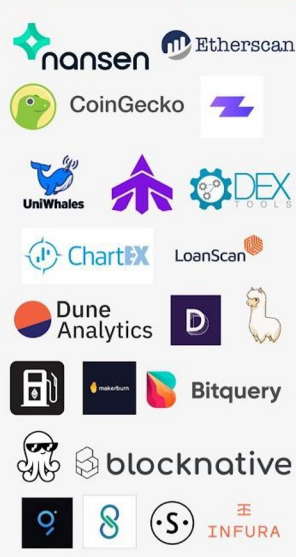
## Active Investors



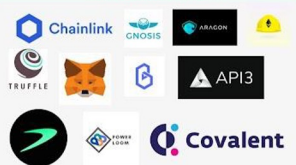
## Scaling



## Data/Analytics



## Infrastructure



## Auditors



## Events



## Corporate Testing (per ConsenSys + Forbes)



# trade offs

centralisation OR decentralisation  
AND AND  
usability OR complexity  
AND AND  
“safe” OR error prone  
AND AND  
mainstream OR niche

# is it worth it?

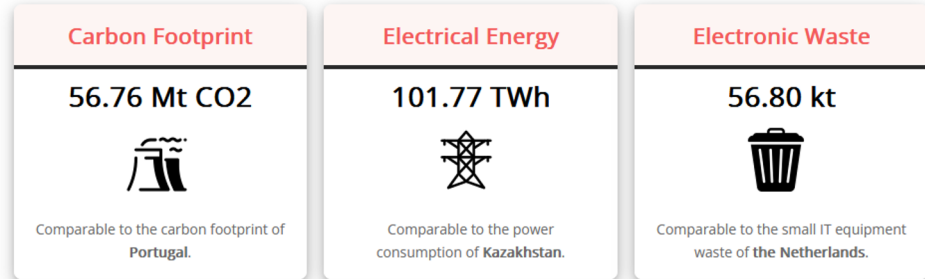
decentralisation

ensorship resistance

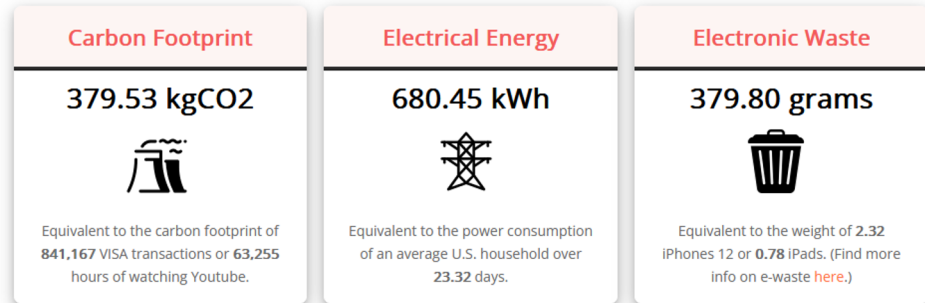
privacy

application security

## Annualized Total Bitcoin Footprints



## Single Bitcoin Transaction Footprints



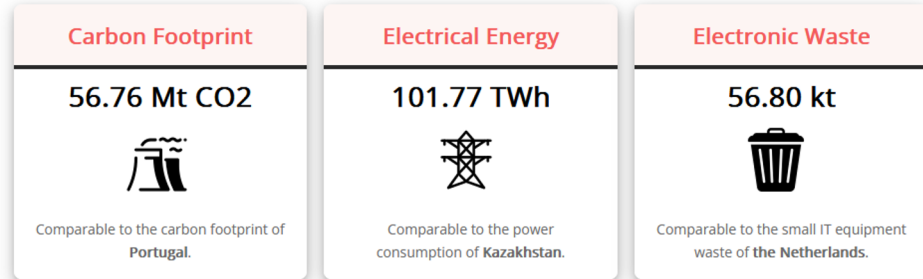
Source: digiconomist.net

# is it worth it?

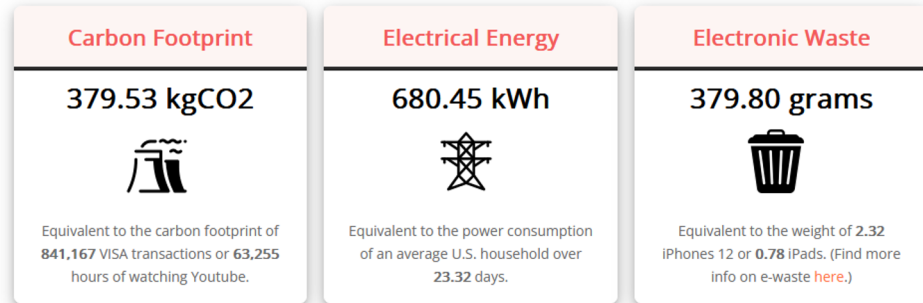
## Popular Proof of Work tokens

- Bitcoin (BTC)
- Dogecoin (DOGE)
- Litecoin (LTC)
- Bitcoin Cash (BCH)
- Monero (XMR)
- Ethereum Classic (ETC)

### Annualized Total Bitcoin Footprints



### Single Bitcoin Transaction Footprints



Source: digiconomist.net

---

**One last thing...**



# discouragement

```
37 // 2. Discouragement. If a peer misbehaves enough (see Misbehaving() in
38 // net_processing.cpp), we'll mark that address as discouraged. We still allow
39 // incoming connections from them, but they're preferred for eviction when
40 // we receive new incoming connections. We never make outgoing connections to
41 // them, and do not gossip their address to other peers. This is implemented as
42 // a bloom filter. We can (probabilistically) test for membership, but can't
43 // list all discouraged addresses or unmark them as discouraged. Discouragement
44 // can prevent our limited connection slots being used up by incompatible
45 // or broken peers.
46 //
```

## Non-listening nodes:

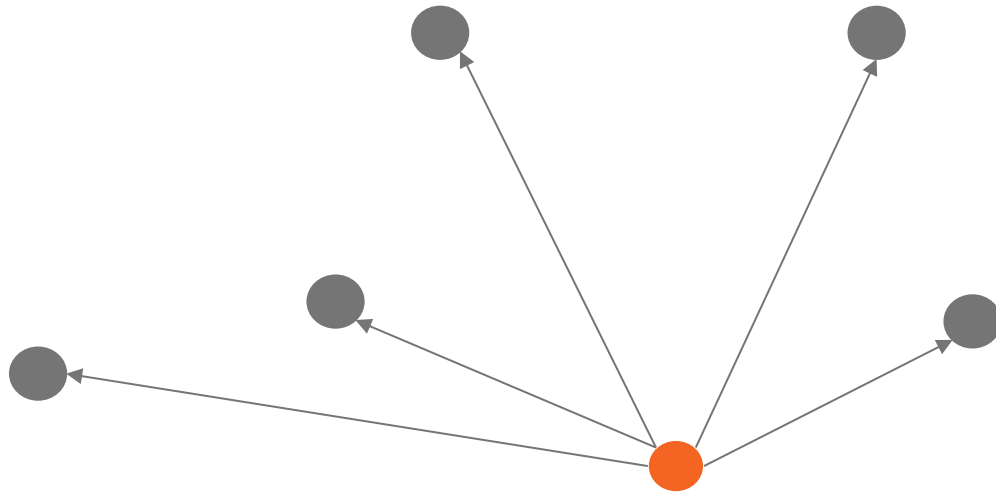
- Priority kicked from busy affected node

## Listening nodes:

- Priority kicked from busy affected node
- Affected node will not connect to you
- Affected node will not share your address with other nodes

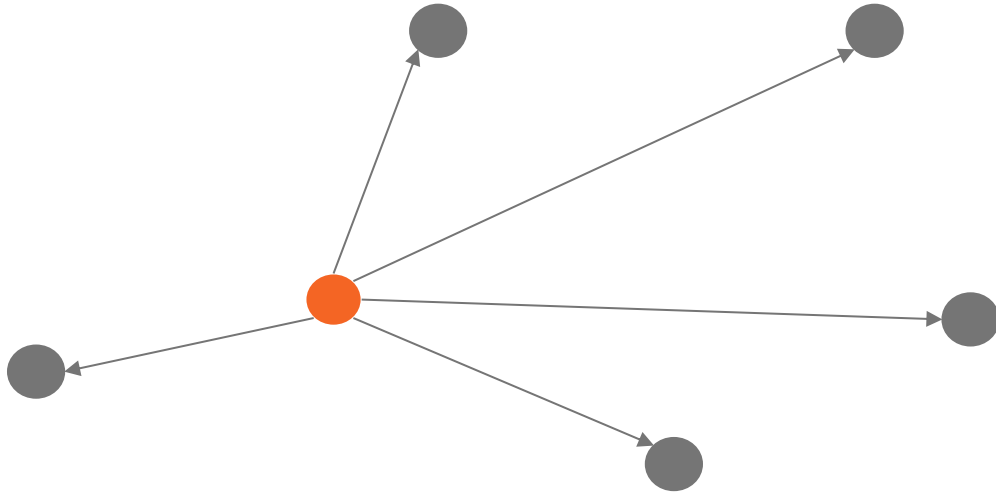
—

**what if...?**



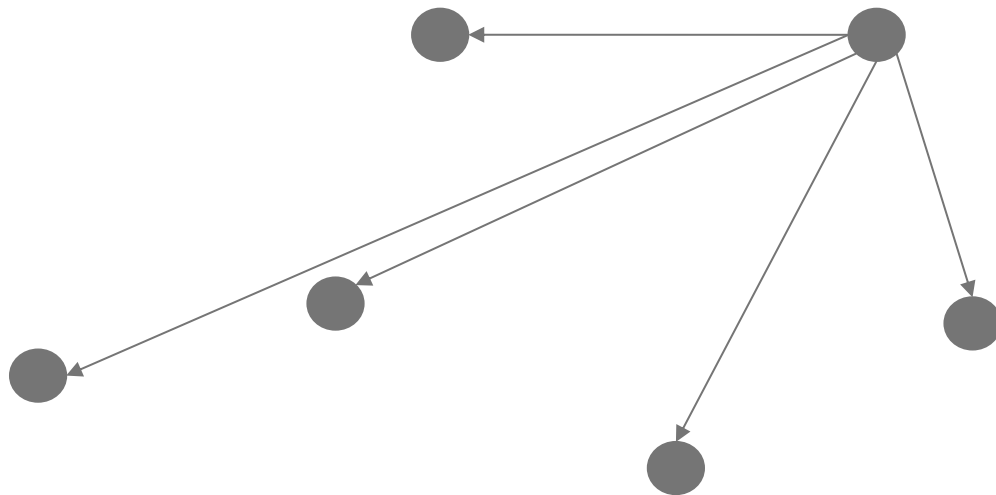
—

# what if...?



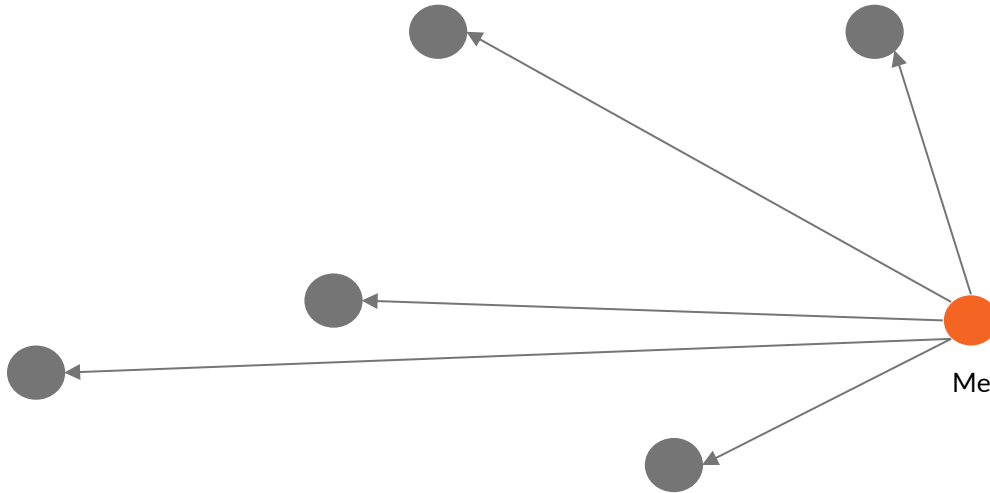
—

# what if...?



**Full TCP Handshake Required**

# what if...?



- ISPs CG-NAT discouraged
- VPN egress discouraged
- TOR exit node discouraged
- Major mining operation...

```
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 161.97.137.101:8333
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 194.5.159.197:8333
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 35.208.165.144:8333
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 193.138.218.162:61144
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 95.216.118.143:8333
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 165.255.61.214:8333
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 104.9.30.99:8333
INFO[2023-06-29T21:48:32+12:00] Successfully discouraged: 172.104.154.196:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 82.221.131.30:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 31.220.77.27:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 116.202.81.17:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 217.182.174.139:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 54.167.40.3:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 85.236.254.80:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 162.55.92.96:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 172.221.171.183:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 185.234.69.187:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 192.31.136.90:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 109.111.79.171:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 70.251.209.207:8333
INFO[2023-06-29T21:48:33+12:00] Successfully discouraged: 18.162.245.103:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 34.207.108.183:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 96.81.219.106:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 185.140.253.169:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 66.29.147.224:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 188.142.199.17:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 71.115.139.170:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 153.127.253.219:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 167.88.11.204:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 207.154.235.64:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 146.190.224.15:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 141.95.217.121:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 147.135.39.240:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 194.182.162.2:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 192.241.135.179:8333
INFO[2023-06-29T21:48:34+12:00] Successfully discouraged: 185.185.50.239:8333
INFO[2023-06-29T21:48:35+12:00] Successfully discouraged: 65.108.77.198:8333
INFO[2023-06-29T21:48:35+12:00] Successfully discouraged: 134.195.196.69:8333
INFO[2023-06-29T21:48:35+12:00] Successfully discouraged: 82.64.108.208:8333
INFO[2023-06-29T21:48:35+12:00] Successfully discouraged: 95.165.93.41:8333
INFO[2023-06-29T21:48:35+12:00] Successfully discouraged: 142.93.171.20:8333
INFO[2023-06-29T21:48:35+12:00] Successfully discouraged: 213.174.156.72:8333
INFO[2023-06-29T21:48:35+12:00] Successfully discouraged: 190.2.152.245:8333
INFO[2023-06-29T21:48:37+12:00] Successfully discouraged: 195.201.126.87:8333
INFO[2023-06-29T21:48:37+12:00] Successfully discouraged: 90.127.246.82:8333
INFO[2023-06-29T21:48:38+12:00] Successfully discouraged: 168.119.139.60:9001
INFO[2023-06-29T21:48:38+12:00] Successfully discouraged: 164.90.150.70:8332
INFO[2023-06-29T21:48:45+12:00] Successfully discouraged: 185.252.235.90:8333
INFO[2023-06-29T21:48:47+12:00] Successfully discouraged: 68.151.5.85:8333
INFO[2023-06-29T21:48:48+12:00] Successfully discouraged: 143.198.134.132:8332
INFO[2023-06-29T21:49:03+12:00] Successfully discouraged your public IP from all IPv4 Bitcoin nodes for 24 hours.
Thanks for caring for the environment.
Please run again tomorrow
```

[https://github.com/doubl  
ethink/maxiban](https://github.com/doubl<br/>ethink/maxiban)

---

**thanks**

<https://github.com/doublethink/maxiban>

Twitter: @doublethink\_sec