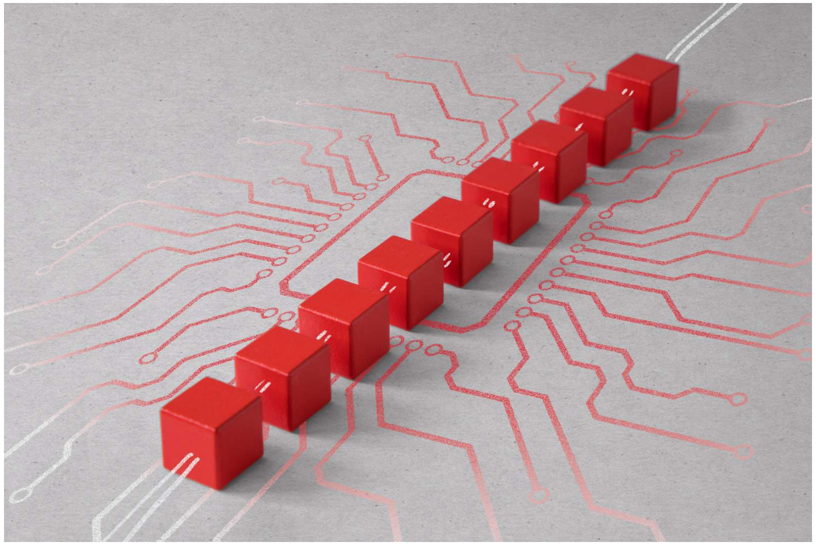
The Blockchain

An Overview



Alan Tobin

2023-03-23

Web 1.0, 2.0, and...

Web 1.0

- **email**
- **static web pages** (fetched from servers)
- appeared amazing: real-time news, online banking/trading

Web 2.0

- **interactivity**
- **social connectivity**
- **user-generated content**

Drivers: mobile internet & powerful mobile devices.

Applications expanded online interactivity & utility:
Airbnb, Facebook, Instagram, TikTok, Twitter, Uber, WhatsApp, YouTube

Web2-centric companies: Apple, Amazon, Ebay, Google, Facebook, Netflix - became World's biggest.

Gig economy enabling millions of people to earn income
by driving, renting their homes, delivering food/groceries, selling goods & services online.

Web 2.0 disrupted many industries being an existential threat to some:
retail, entertainment, media, advertising.

Web3 aka Decentralized Web

- next phase in the evolution of the web/internet
- can be as disruptive as Web 2.0
- big paradigm shift

Defining features of Web3:

- decentralization
- openness
  trustless - no intermediaries
  permissionless - anyone can participate => dApps run on blockchains / decentralized p2p networks.
- greater user utility
- AI & ML (faster, more relevant results)
- connectivity & ubiquity.

Tokens (financial assets)

- will be built into inner workings of everything you do online
- will supplant corporations with decentralized, internet-based orgs
  governed by software protocols & votes of token holders.

Every company became an internet company over time.
Every company will become a digital asset company.

Web3 will have material impact on **business models** across most industries.

Metaverse

- Blockchain is used in metaverse to create a secure and transparent system for **tracking ownership of digital assets** such as virtual real estate, digital art, and other in-game items.
- It also enables **decentralized governance** and allows for the creation of **unique digital identities** for users.

Benefits of Blockchain

Fast, cheap, permissionless, unlimited borderless payments

Open 24/7

Permissionless investment opportunities
in both traditional (stocks, bonds, etc.) and digital assets.

No subjectivity in application of rules - “code is law”.

Decentralized marketplaces

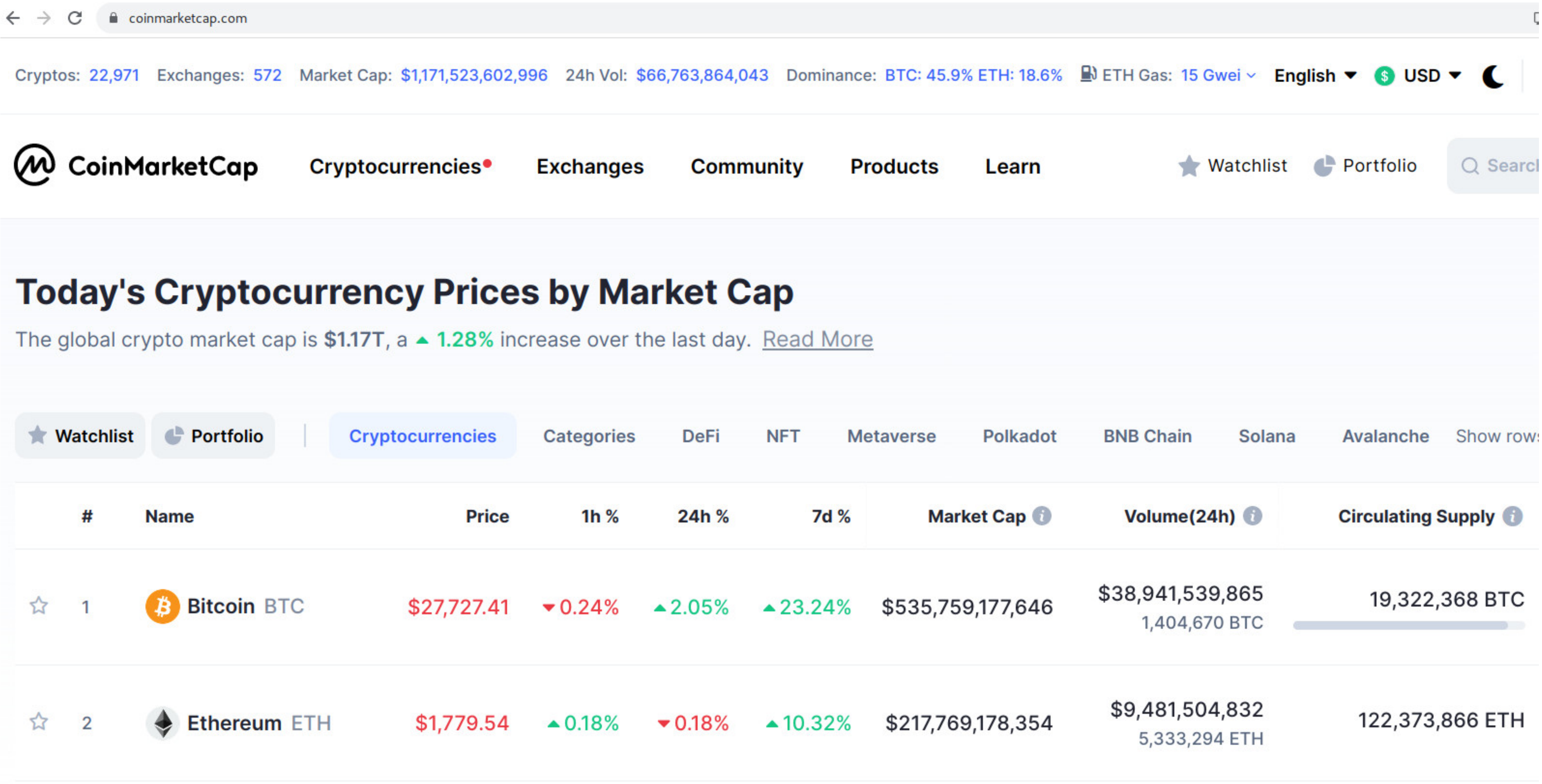
Innovation unencumbered by regulations, conventions.

Impactful Blockchain Applications

Cryptocurrencies
Supply Chain Management
Decentralized Identity
Voting Systems
Asset Tokenization
Peer-to-Peer Marketplaces
Prediction Markets
Cross-Border Payments
Fraud Prevention and Detection

Size of Blockchain Industry

$0.003 tn	blockchain industry
$5 tn	technology industry
$4 tn	automotive industry
$1 tn	pharmaceuticals industry



Cryptos: 22,971 Exchanges: 572 Market Cap: $1,171,523,602,996 24h Vol: $66,763,864,043 Dominance: BTC: 45.9% ETH: 18.6% ETH Gas: 15 Gwei

Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is **$1.17T**, a ▲ 1.28% increase over the last day. Read More

	#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
☆	1	Bitcoin BTC	$27,727.41	▼0.24%	▲2.05%	▲23.24%	$535,759,177,646	$38,941,539,865 1,404,670 BTC	19,322,368 BTC
☆	2	Ethereum ETH	$1,779.54	▲0.18%	▼0.18%	▲10.32%	$217,769,178,354	$9,481,504,832 5,333,294 ETH	122,373,866 ETH

Early Work on Electronic Cash

Wei Dai (**1998**) "B-Money"

In a crypto-anarchy the government is permanently unnecessary.
It's a community where **threat of violence is impotent**
Violence is impossible since its participants cannot be linked
to their names or physical locations.

Community is defined by cooperation of its participants, which needs

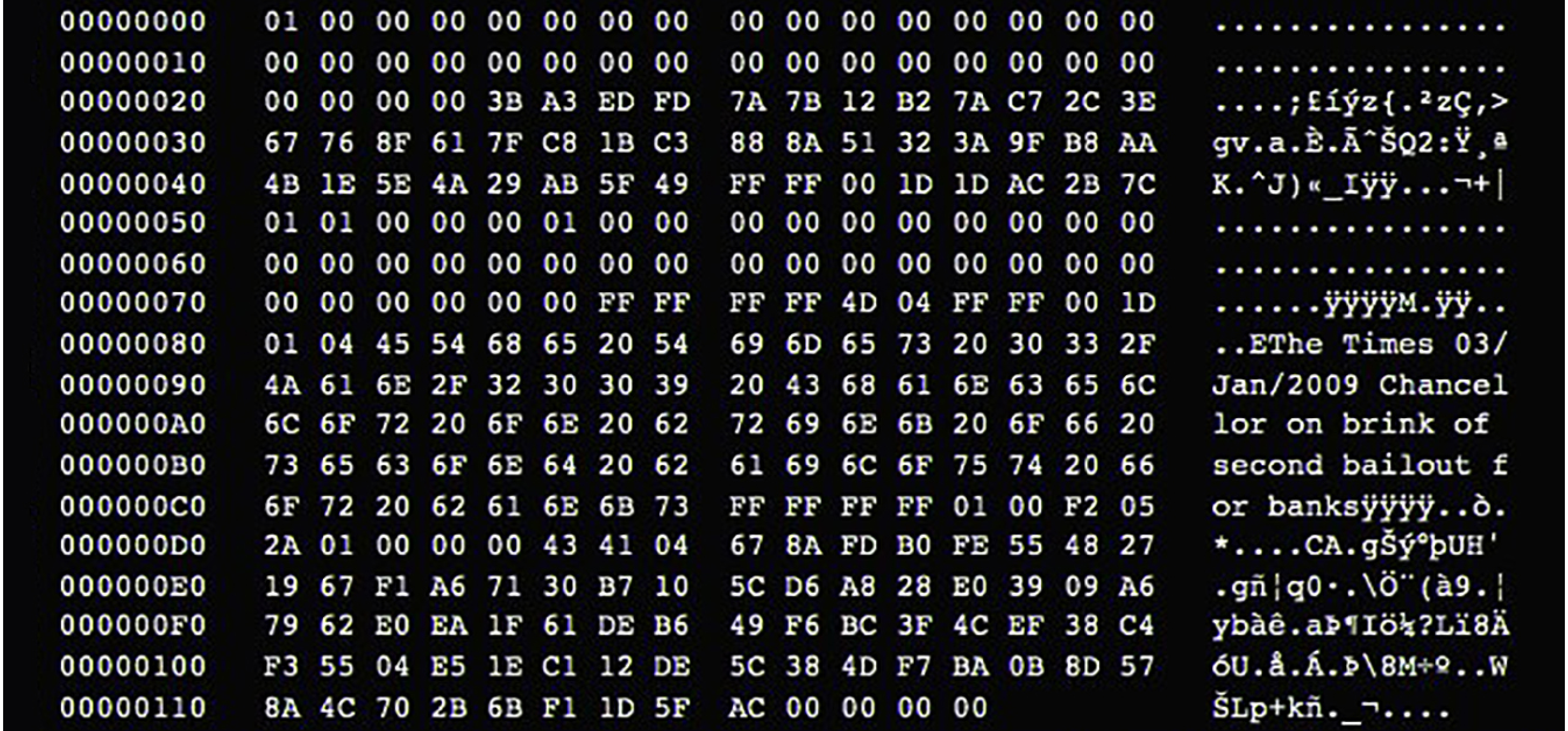
- **medium of exchange (money)**
- **mechanism to enforce contracts**

These services are traditinally provided by government institutions
and only to legal entities. I describe a **protocol** by which these services
can be provided to and by untraceable entities.

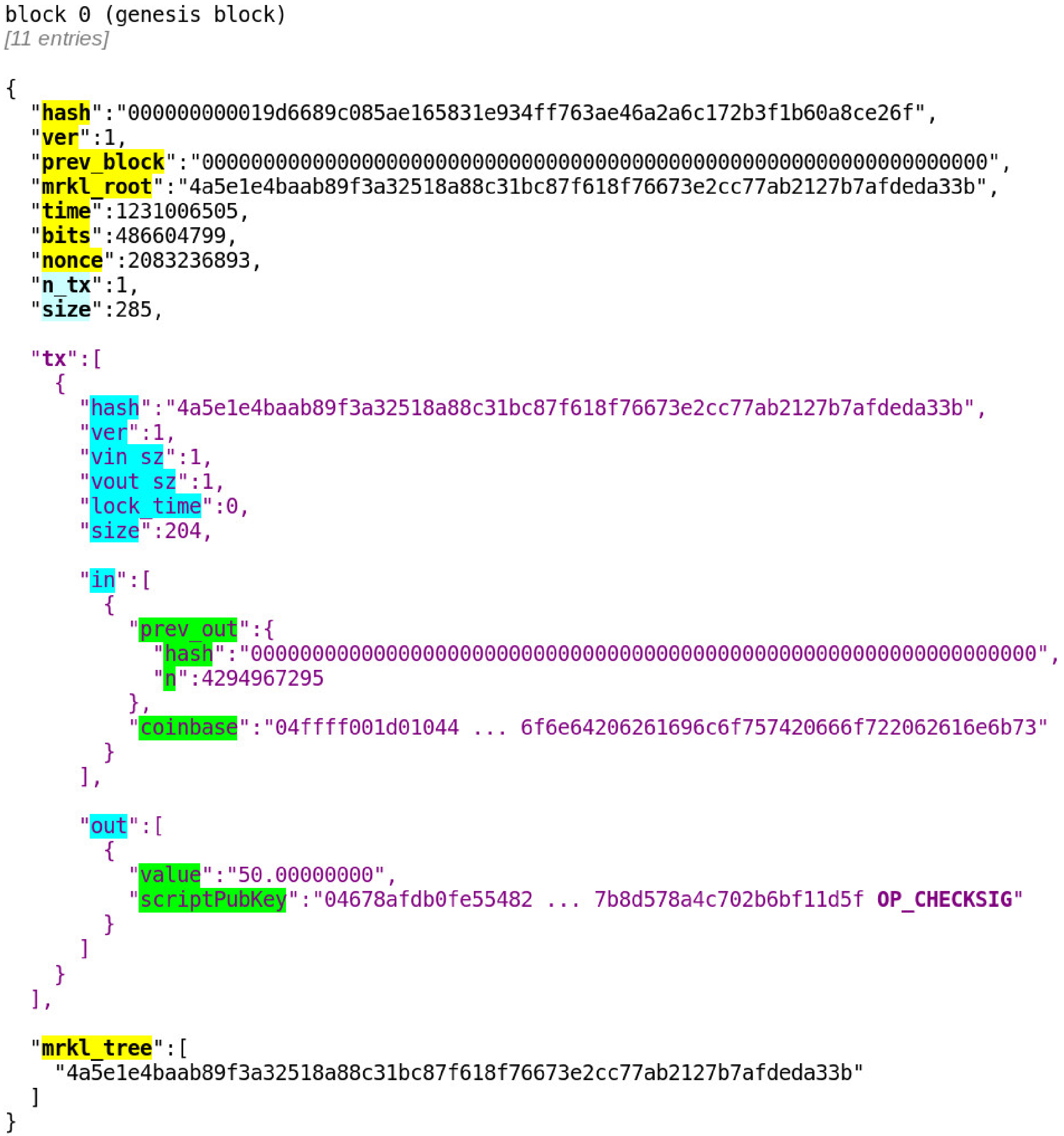
NSA 1996
Office of InfoSec Research and Technology, Cryptology Division.
"How to Make a Mint: Cryptography of **Anonymous Electronic Cash**".

Bitcoin Genesis Block

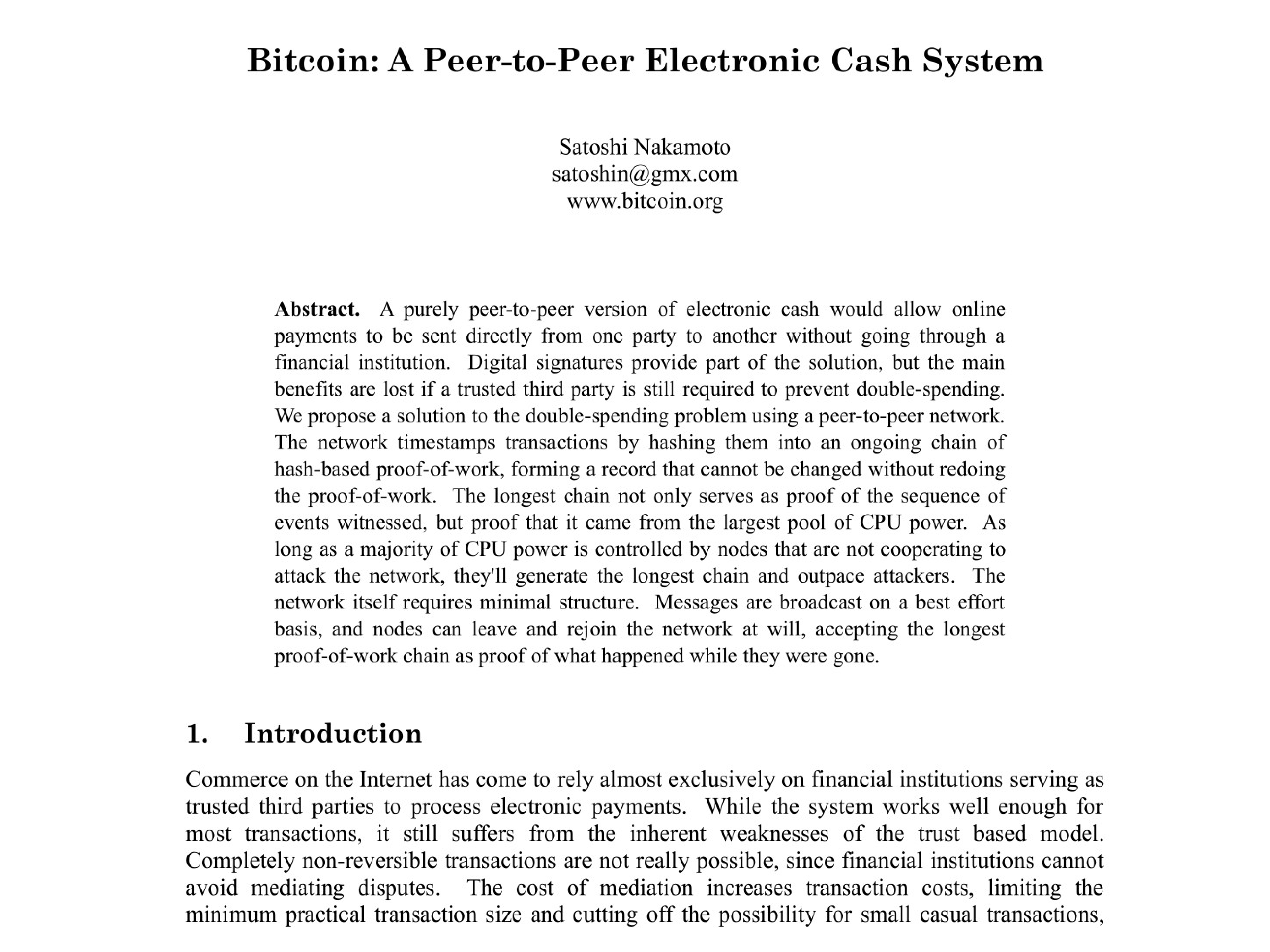
Raw Hex Version



```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```



```
block 0 (genesis block)
[11 entries]

{
  "hash":"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
  "ver":1,
  "prev_block":"0000000000000000000000000000000000000000000000000000000000000000",
  "mrkl_root":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
  "time":1231006505,
  "bits":486604799,
  "nonce":2083236893,
  "n_tx":1,
  "size":285,

  "tx":[
    {
      "hash":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":204,

      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"04ffff001d01044 ... 6f6e64206261696c6f757420666f722062616e6b73"
        }
      ],

      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04678afdb0fe55482 ... 7b8d578a4c702b6bf11d5f OP_CHECKSIG"
        }
      ]
    }
  ],

  "mrkl_tree":[
    "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
  ]
}
```



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

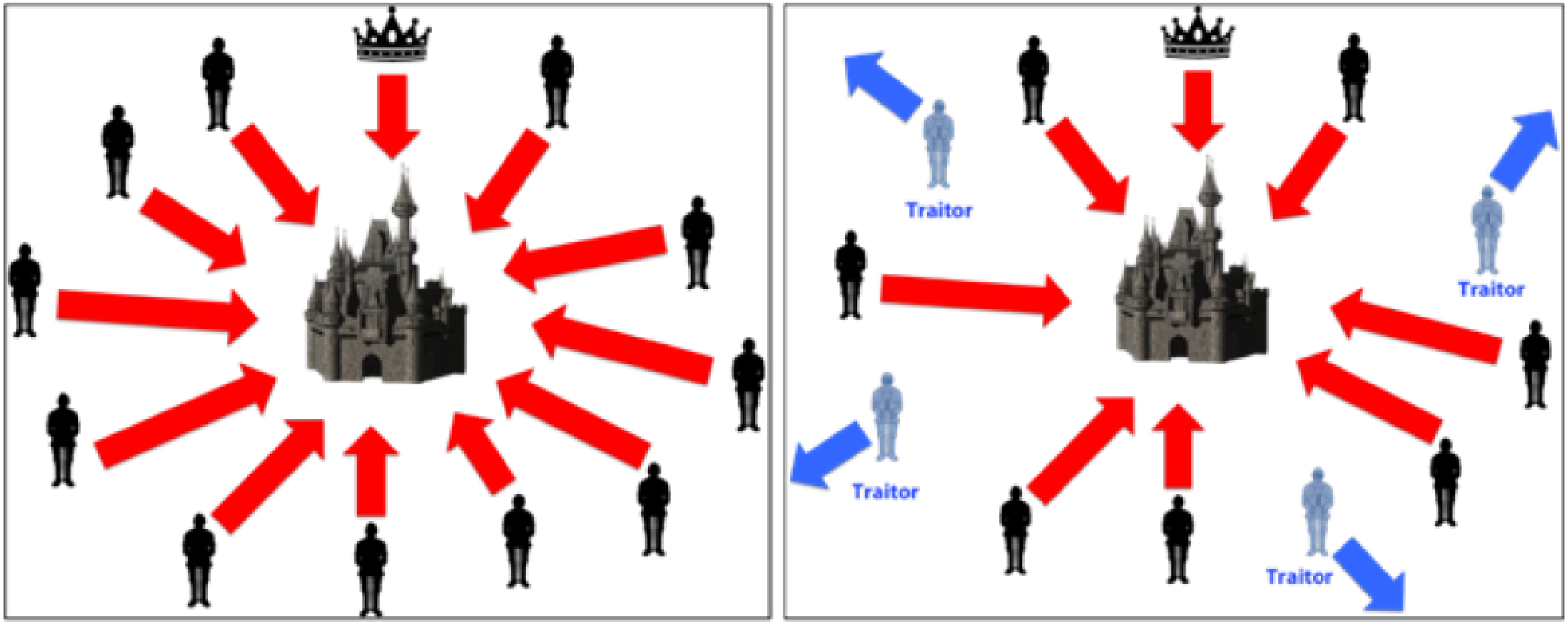
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions,

Consensus

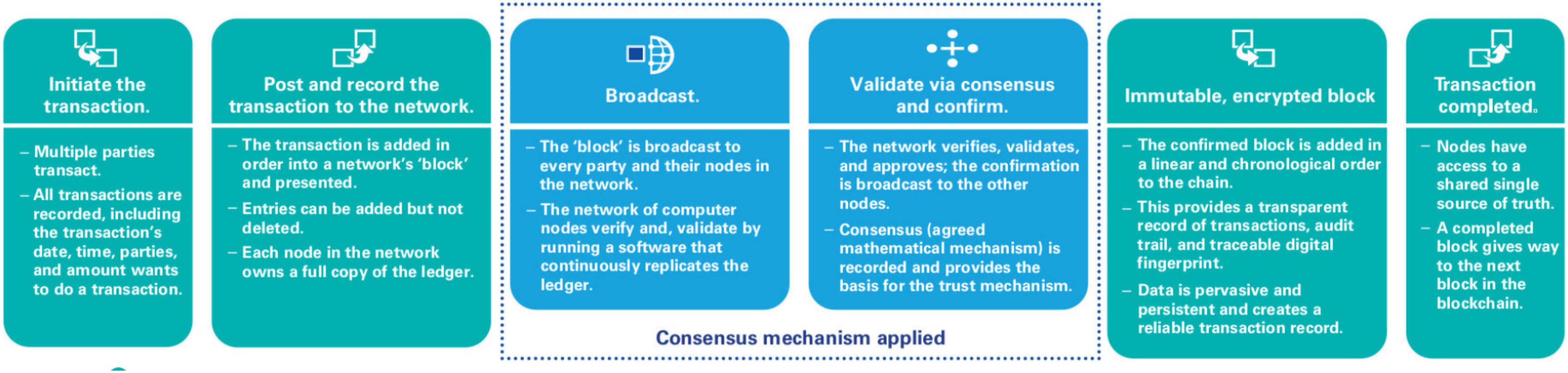
Byzantine fault tolerance



Coordinated Attack Leading to Victory

Uncoordinated Attack Leading to Defeat

Transaction Life Cycle in Blockchain



Initiate the transaction.

- Multiple parties transact.
- All transactions are recorded, including the transaction's date, time, parties, and amount wants to do a transaction.

Post and record the transaction to the network.

- The transaction is added in order into a network's 'block' and presented.
- Entries can be added but not deleted.
- Each node in the network owns a full copy of the ledger.

Broadcast.

- The 'block' is broadcast to every party and their nodes in the network.
- The network of computer nodes verify and, validate by running a software that continuously replicates the ledger.

Validate via consensus and confirm.

- The network verifies, validates, and approves; the confirmation is broadcast to the other nodes.
- Consensus (agreed mathematical mechanism) is recorded and provides the basis for the trust mechanism.

Consensus mechanism applied

Immutable, encrypted block

- The confirmed block is added in a linear and chronological order to the chain.
- This provides a transparent record of transactions, audit trail, and traceable digital fingerprint.
- Data is pervasive and persistent and creates a reliable transaction record.

Transaction completed.

- Nodes have access to a shared single source of truth.
- A completed block gives way to the next block in the blockchain.

Layer 1 Chains

TPS	Block Time (s)	Layer1:	Genesis	Smart contract language	Creator
7	600	**Bitcoin**	2009-01	forth-like stack-based	Nakamoto
25	14	**Ethereum**	2015-07	solidity, vyper, etc.	Buterin
25	20	**Cardano**	2017-09	plutus, marlowe, glow	Hoskinson
100	5	**Binance**	2019-04	solidity, truffle	Binance
65k	0.4	**Solana**	2020-03	rust, c, c++	Yakovenko

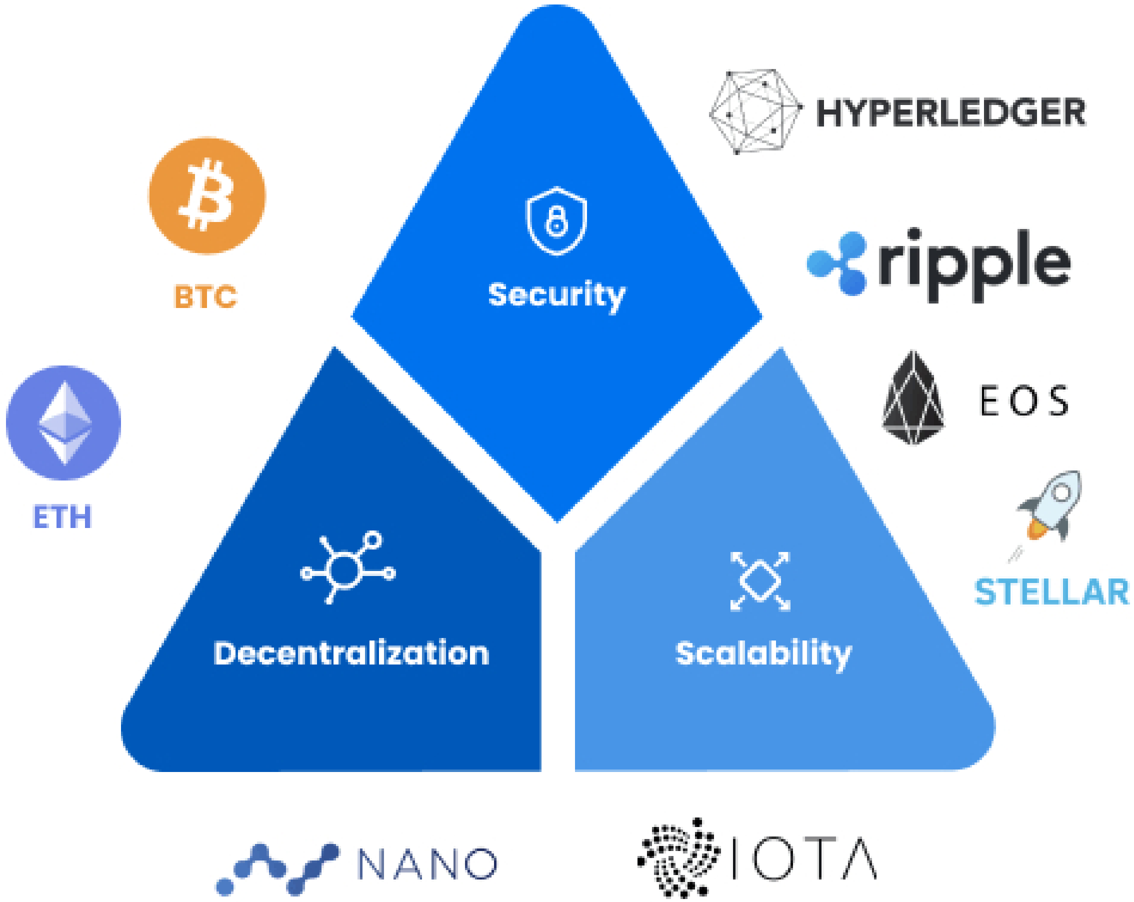
Smart Contracts

- A blockchain system can be viewed as a **distributed computer**.
  The computer code executed on the network makes it possible to form agreements via blockchain. Such agreements are called **smart contracts**. They are **self-executing**, typically with **automatic payments**. Execution of a smart contract cannot be stopped or altered by any authority.
- Smart Property
  property that is controlled, traded, loaned via blockchain using smart contracts. It can be physical (car, house, phone) or non-physical (shares in a company, access rights to a remote computer

Ethereum ~ Internet DAPPS ~ websites that run in it.

Scalability-Decentralization-Security

Trilemma: Can have any 2 of the 3



Blockchain Chronology

2008 Bitcoin whitepaper released.

2009 Bitcoin network launched.

2010 1st bitcoin payment for physical goods - pizza for 10kBTC ~ $.5 bn today :)

2011 Crypto exchanges emerge. Bitcoin USD parity. Litecoin released.

2012 WikiLeaks accepts Bitcoin donations. BitPay launch. Nakamoto disappears.

2013 Ethereum white paper published. MtGox collapse. SilkRoad shutdown.

2014 Altcoins proliferate: Namecoin, Dogecoin, Ripple, Dash, NXT, etc.

2015 Ethereum mainnet launched.

2016 Enterprise blockchains: IBM, Intel, hyperledger, Digital Asset Holdings.

2017 Initial Coin Offerings (ICO). 1st oracle (Chainlink) founded. >20x returns.

2018 Ethereum congestions due to popularity of ICOs & DApps. EOS ICO.

2019 Stablecoins. Security tokens. Institutional crypto. Interoperability.

2020 DeFi boom: TVL $1b->$16b.

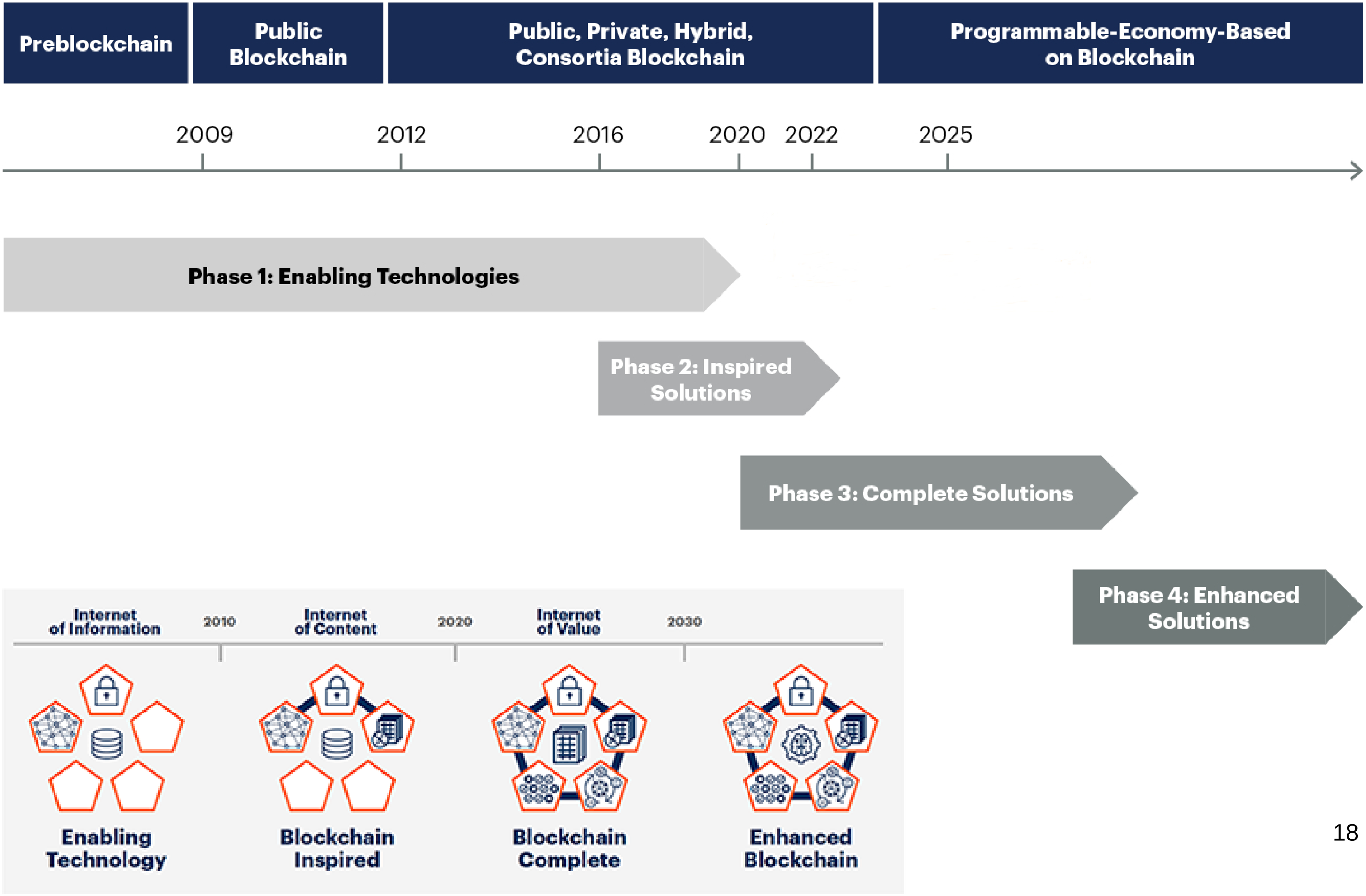
2021 NFT.

2022 Ethereum PoW->PoS. DeFi goes mainstream. Terra, FTX failures.
Layer-2: Optimism 1st launched native token.

2023 Trends: Web3, Tokenization, Multichain (Cosmos)

https://www.coindesk.com/consensus-magazine/2022/12/19/23-**blockchain-predictions-for-2023**/

Blockchain Timeline



Preblockchain

Public Blockchain

Public, Private, Hybrid, Consortia Blockchain

Programmable-Economy-Based on Blockchain

2009 2012 2016 2020 2022 2025

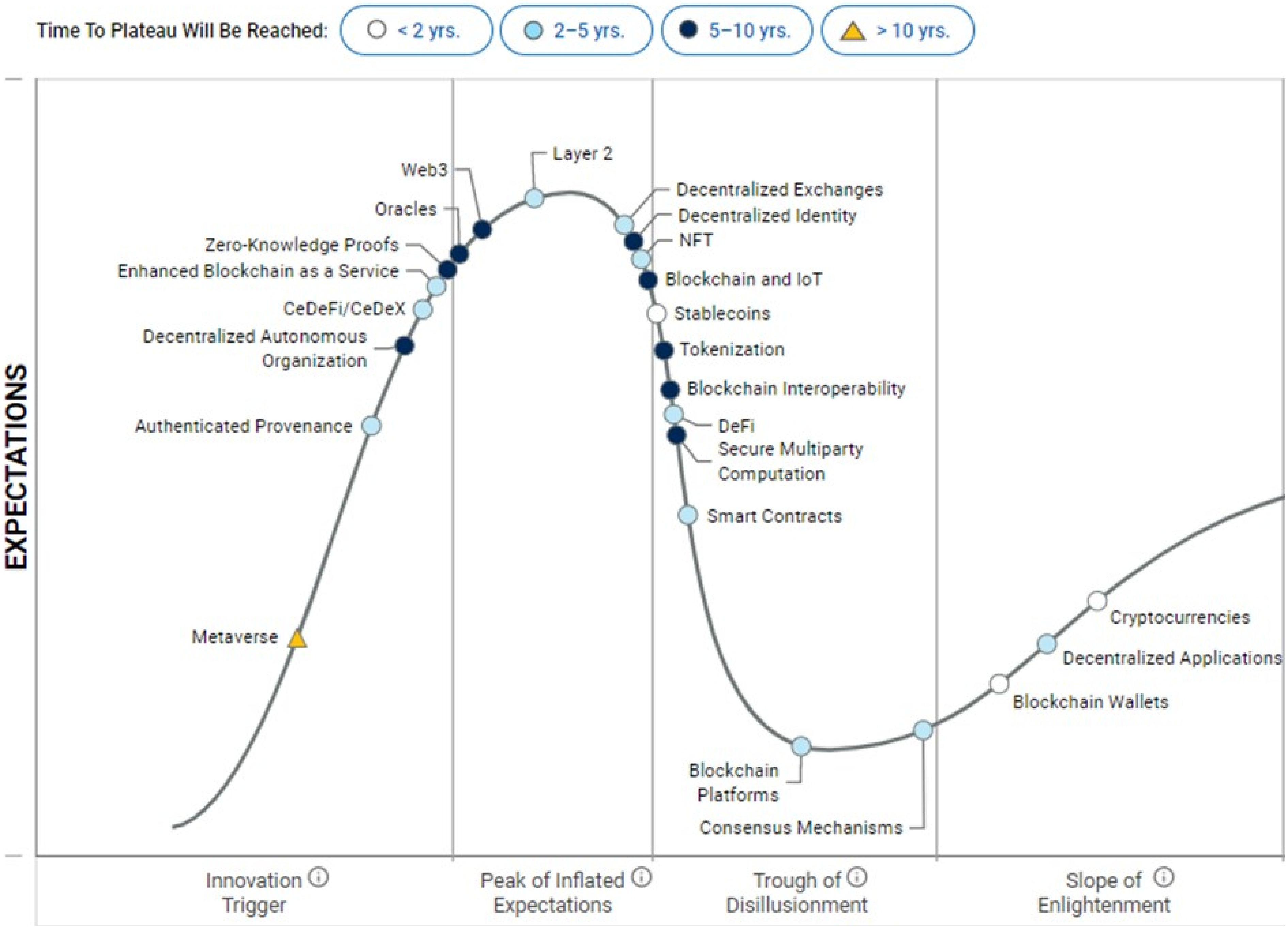
Phase 1: Enabling Technologies

Phase 2: Inspired Solutions

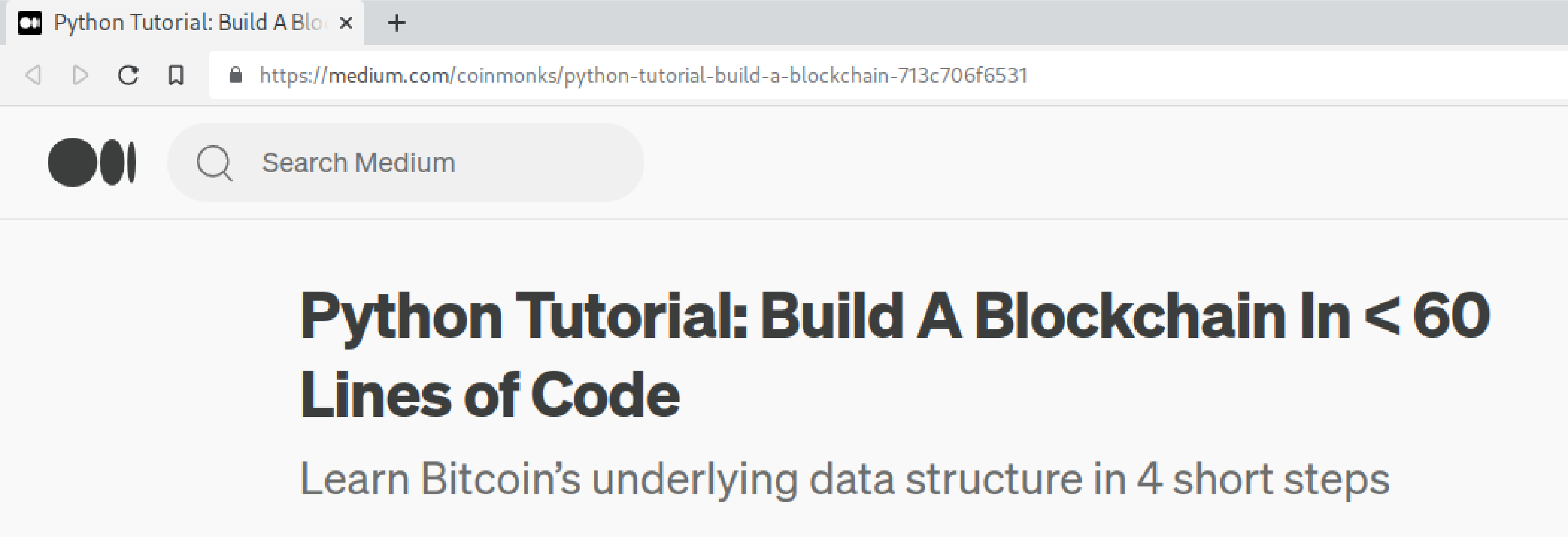
Phase 3: Complete Solutions

Phase 4: Enhanced Solutions

Blockchain Hype Cycle



How to Get Started



https://medium.com/coinmonks/python-tutorial-build-a-blockchain-713c706f6531

Python Tutorial: Build A Blockchain In < 60 Lines of Code

Learn Bitcoin’s underlying data structure in 4 short steps

- Wallets: Metamask
- Crypto Exchanges (Australia-friendly): Binance, Kraken.

Decentralized Society: Finding Web3’s Soul.

Buterin et al. 2022

Web3 today centers around expressing transferable assets, rather than encoding **social relationships of trust**. Yet many core economic activities—such as uncollateralized lending and building personal brands—are built on **persistent, non-transferable relationships**.

In this paper, we illustrate how non-transferable “soulbound” tokens (SBTs) representing the commitments, credentials, and affiliations of “Souls” can encode the trust networks of the real economy to establish provenance and reputation.

More importantly, SBTs enable other applications of increasing ambition, such as community wallet recovery, sybil-resistant governance, mechanisms for decentralization, and novel markets with decomposable, shared rights. We call this richer, pluralistic ecosystem “**Decentralized Society**” (DeSoc)—a co-determined sociality, where Souls and communities come together bottom-up, as emergent properties of each other to co-create plural network goods and intelligences, at a range of scales.