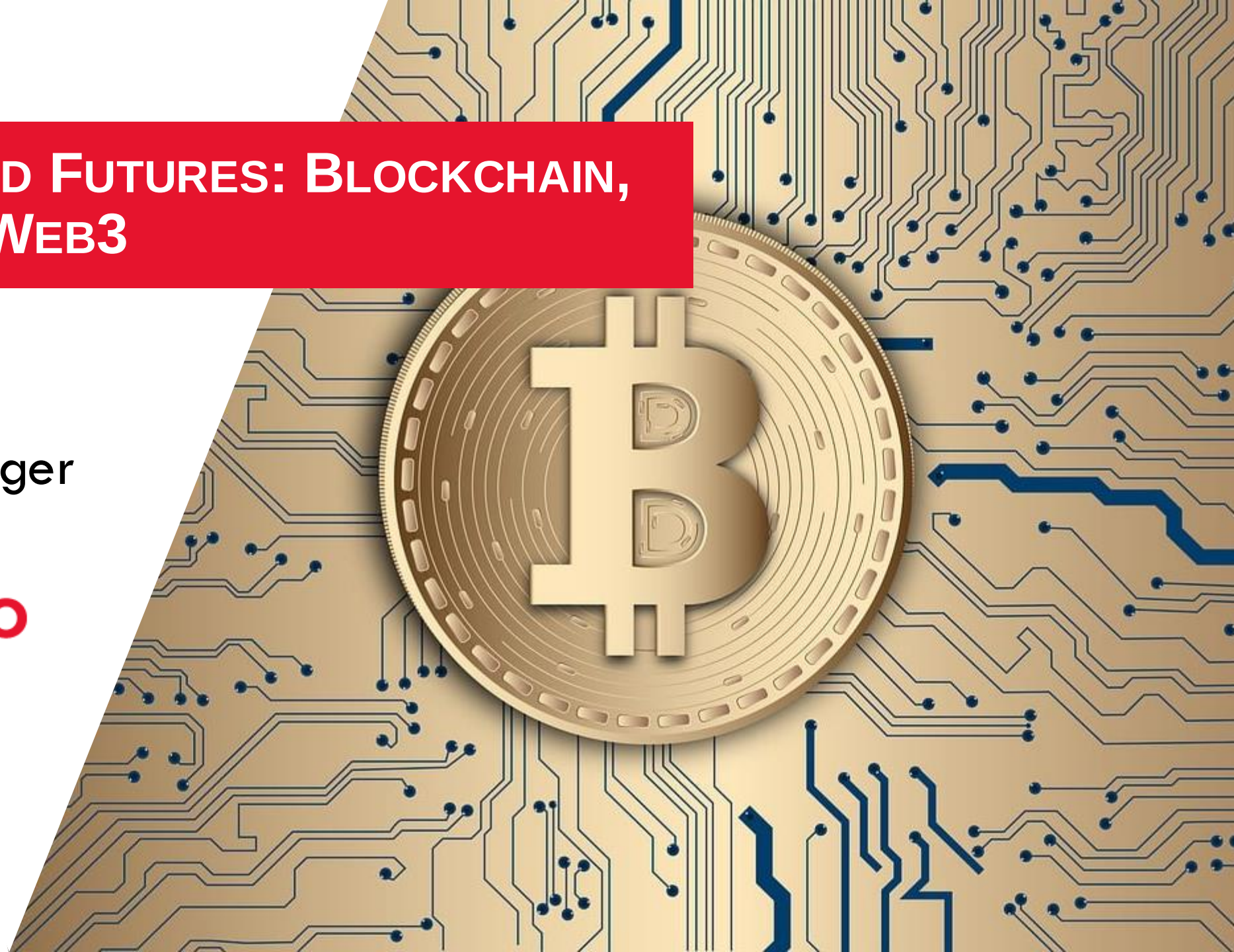
2024-2025

Decentralized Futures: Blockchain, Crypto, and Web3



Jacques-André
Fines Schlumberger

SciencesPo
ÉCOLE DU MANAGEMENT
ET DE L'INNOVATION

Objectives

- Have a clear understanding on how Blockchain technology works
  → Evolution from Traditional – Centralized – Decentralized Structures.

- Explore blockchain applications in various fields
  → Finance
  → Energy, Climate, Supply Chain, Identity…

- Imagine real DECENTRALIZED FUTURES

Plan

Session 1: Introduction to Blockchains
Session 2: Bitcoin, Ethereum
Session 3: Decentralized Finance (DeFi)
Session 4: Energy, Climate and Supply Chains
Session 5: Blockchain and Democracy
Session 6: Final Examination

Notation

- Individual or collective work on a blockchain technology or project (30%)
- Active in-class participation, and MCQ (20%)
- Final exam (50%)
  - use case or
  - essay

Let's get to know each other

1/ Quick survey

2/ Create a wordpress account here:
www.blockchain-x.eu

Session 1: Introduction to Blockchains

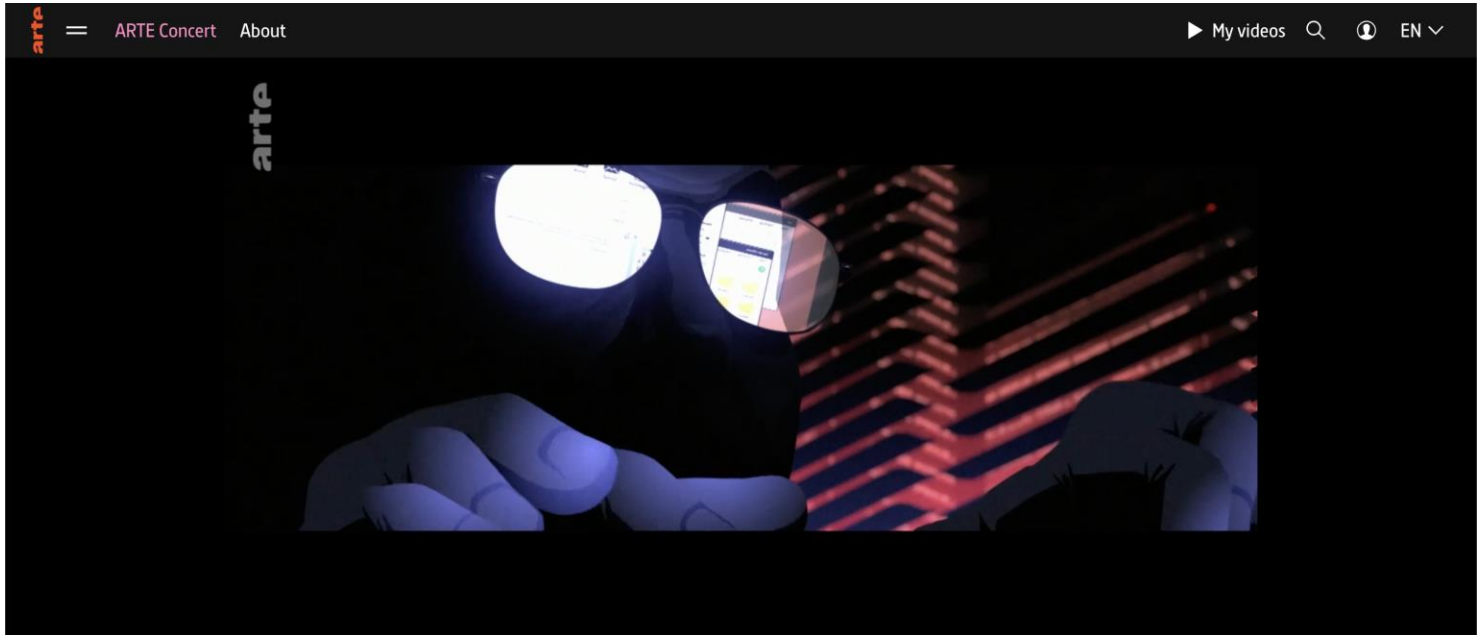
1. Required Viewing and Reading
2. History of digital cash
3. How does Blockchain work?
4. Public or private, permissioned or permissionless?
5. What type of token?
6. Custodial and non custodial wallet?
7. Individual work

What is Bitcoin & bitcoins?

Bitcoin is a peer-to-peer currency
Peer-to-peer means that no central authority issues new money or tracks transactions. These tasks are managed collectively by the network.

The Satoshi Mystery - The Story of Bitcoin

Required viewing



https://www.arte.tv/en/videos/097372-001-A/the-satoshi-mystery-the-story-of-bitcoin/

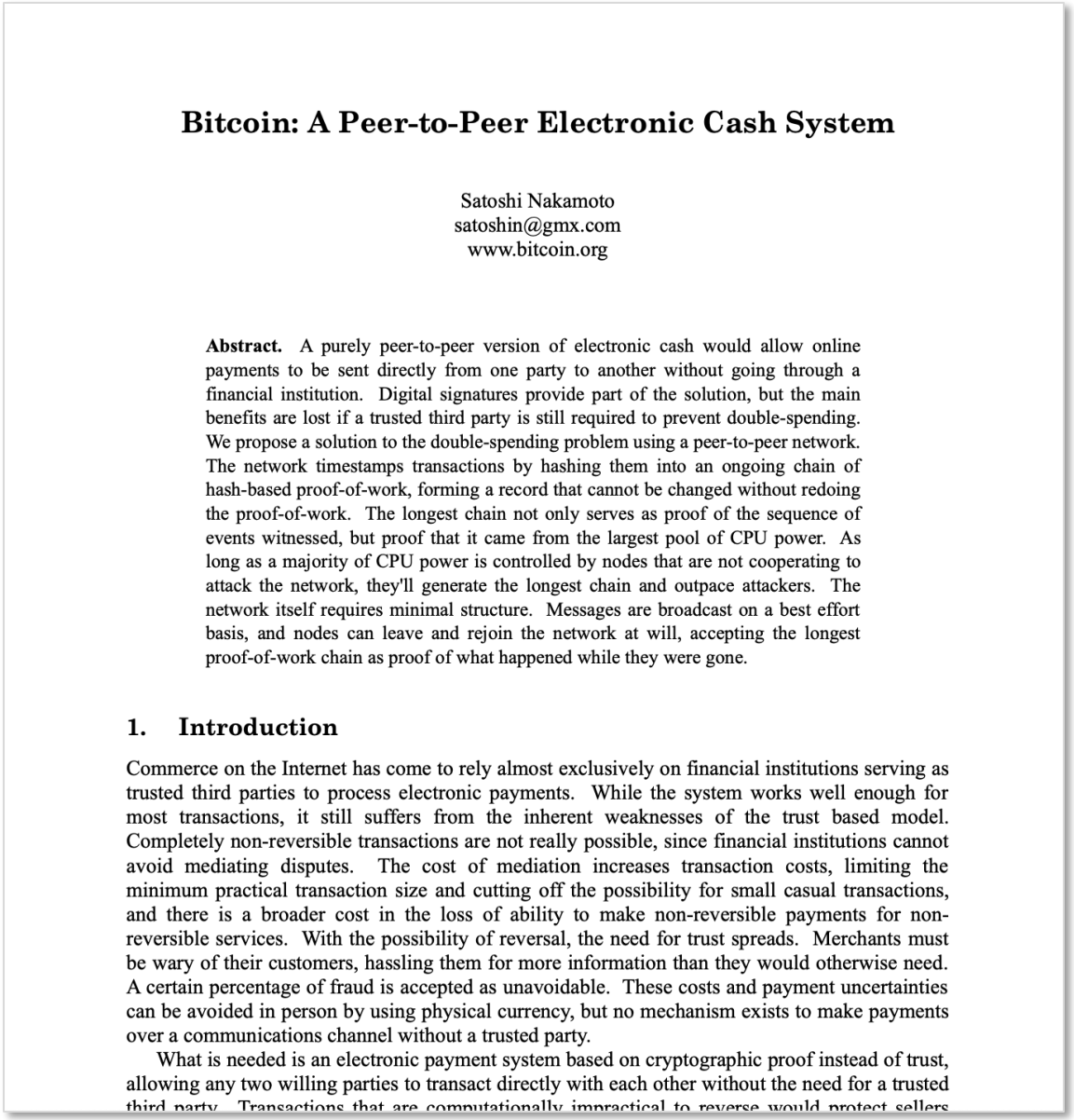
In the age of the Internet, "cypherpunks" tried to create an anonymous, autonomous, free and direct digital currency that worked without intermediaries. Many failed - but not Satoshi Nakamoto. In the middle of the subprime mortgage crisis, he was the first to publish the code for Bitcoin.

The genesis White Paper

Bitcoin: A Peer-to-Peer Electronic Cash System,
https://bitcoin.org/bitcoin.pdf, 2008

What did you read ?
What did you understand ?

Required reading



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.

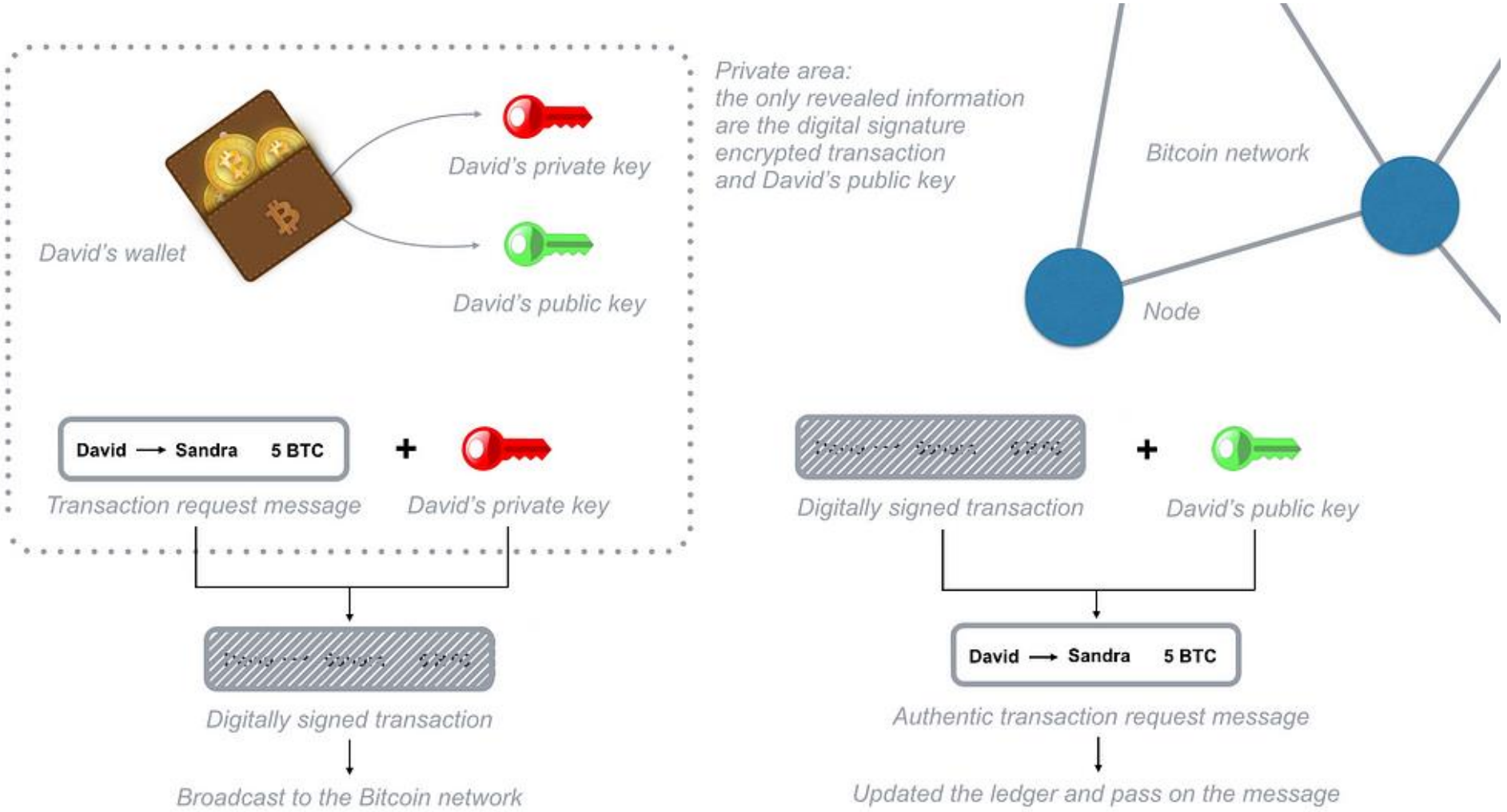
1. Introduction

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, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

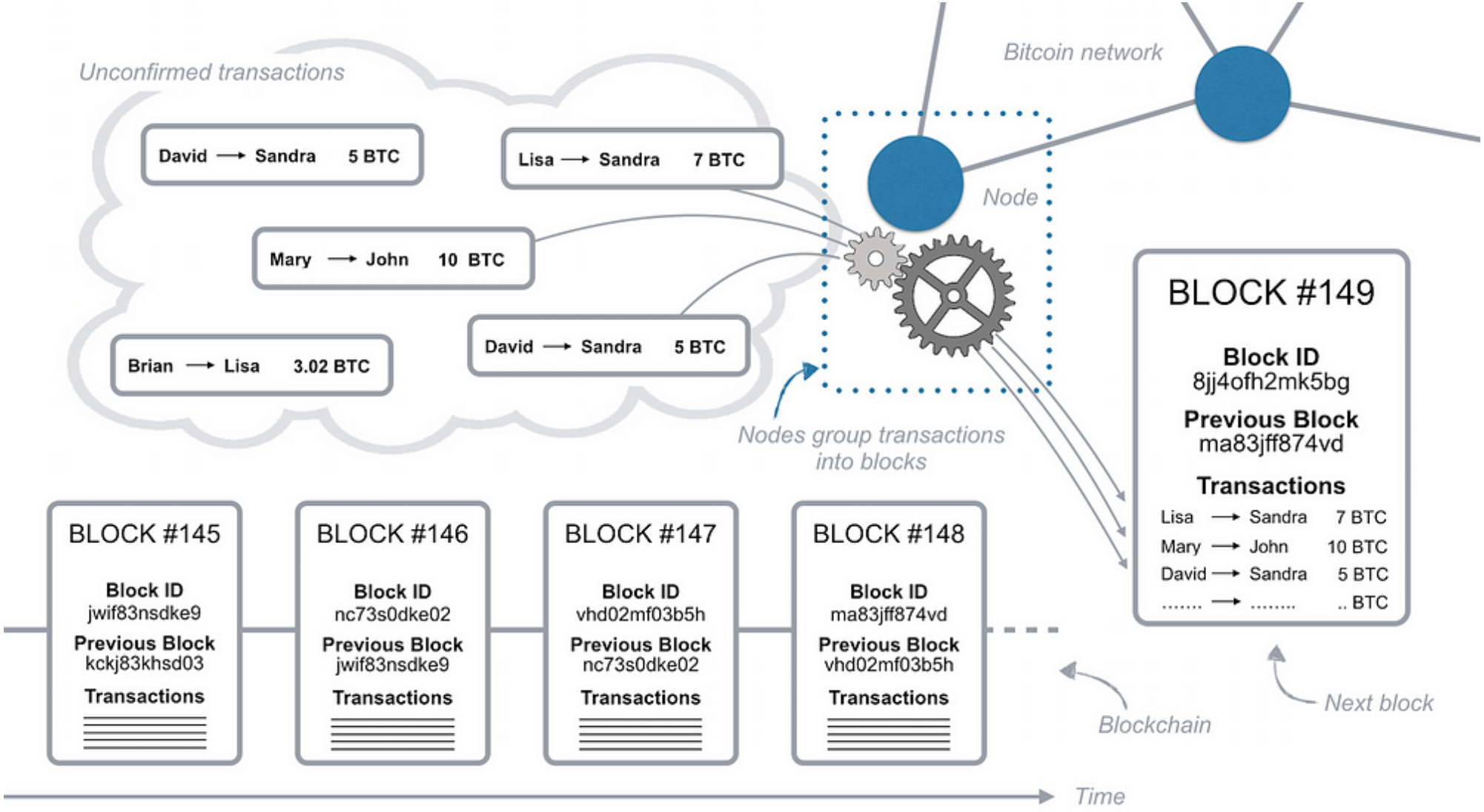
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers

1. How does Blockchain work?

1. Someone Wants to Send Bitcoin



The transaction is not yet confirmed



2. The Transaction is Broadcast to the Network

BITCOIN TRANSACTION REQUEST MESSAGE

"David sends 5 BTC to Sandra"

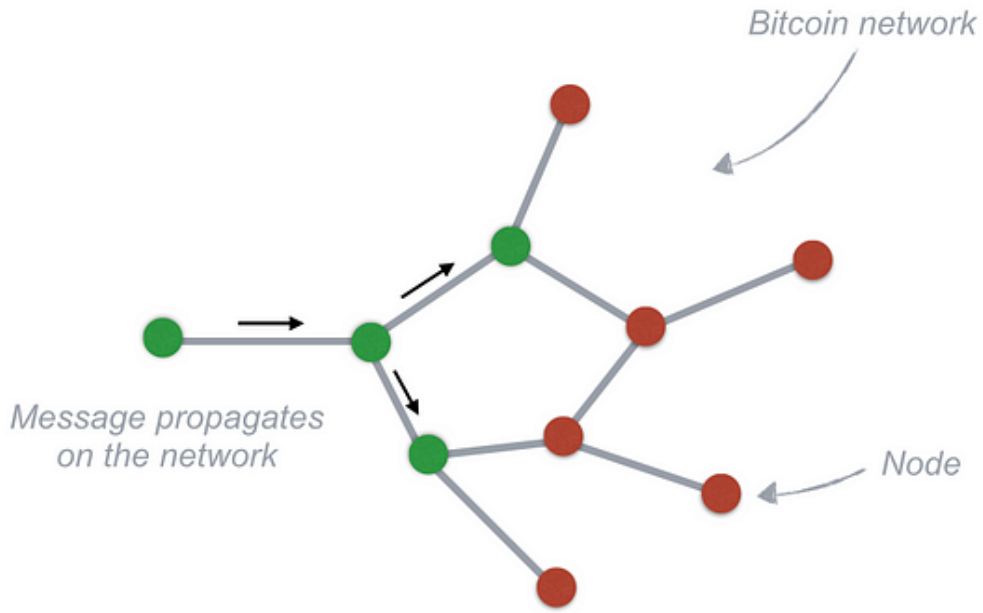
David → Sandra 5 BTC

LEDGER

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23

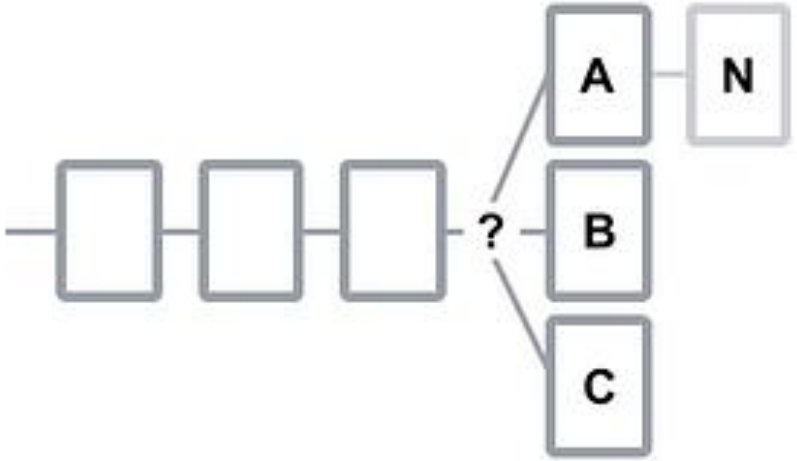
LEDGER

Account owner	Value
Mary	4
John	56
Sandra	88
Lisa	16
David	182
Brian	23

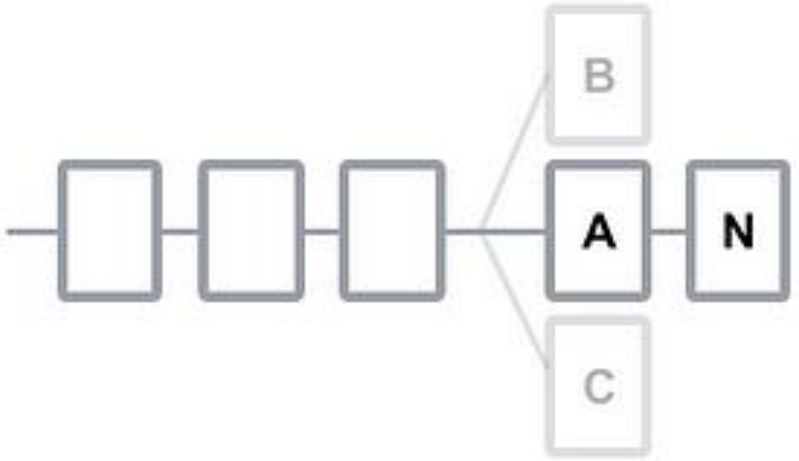


Each *node* receives the transaction request message, updates its own copy of the *ledger* and passes on the message to the nearby *nodes.*

3. Miners Get to Work (Mining Process)

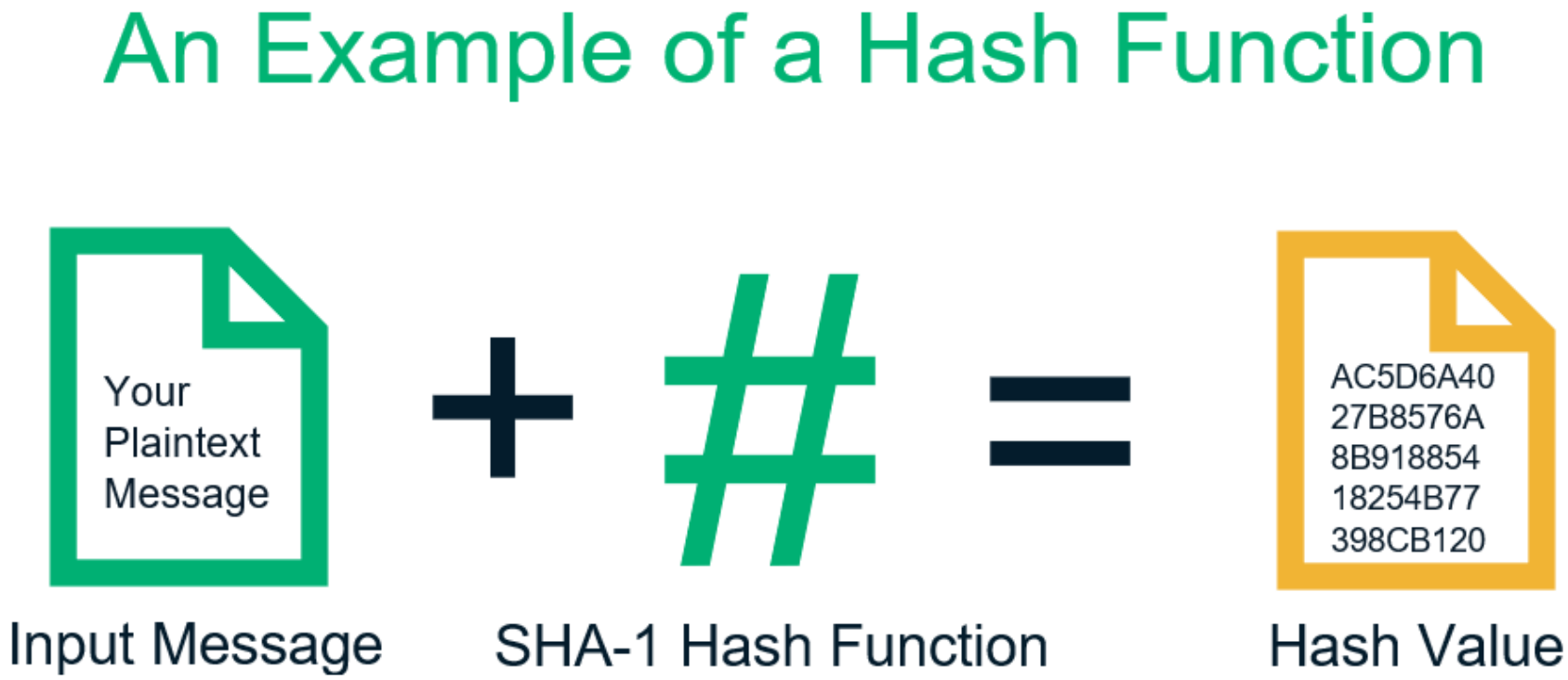


Each node than tries to add the new block (N) to the block they received first from the other nodes

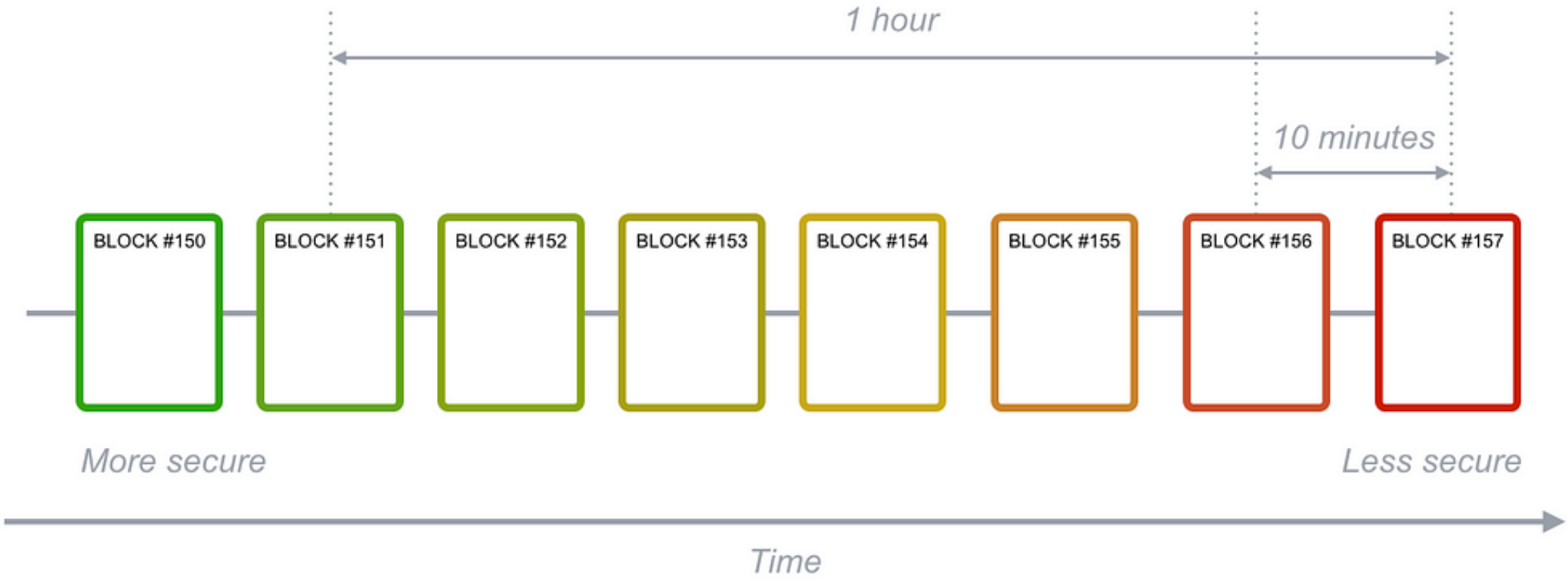


As soon as the new block (N) is added all the network adopt the longest chain possible (A+N) stabilising the whole network

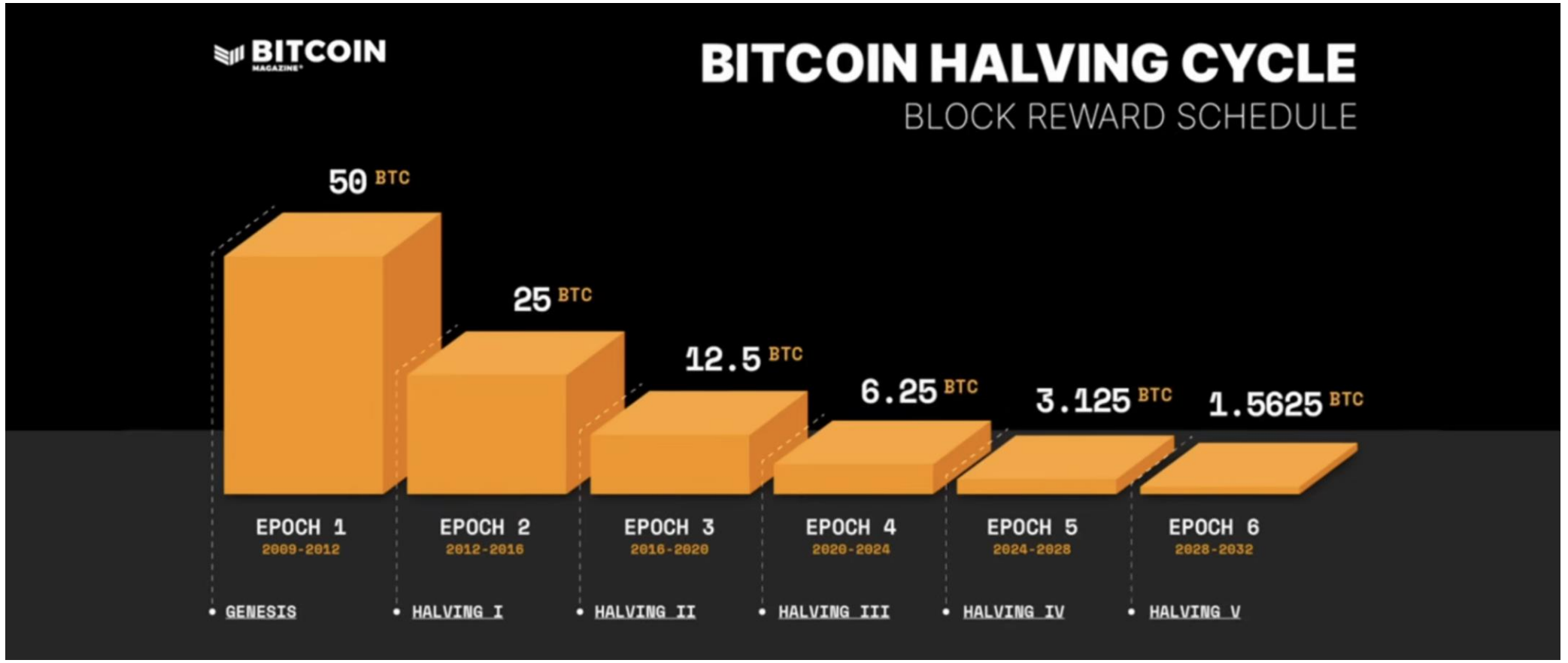
4. The Hash Function: The Secret Behind Mining



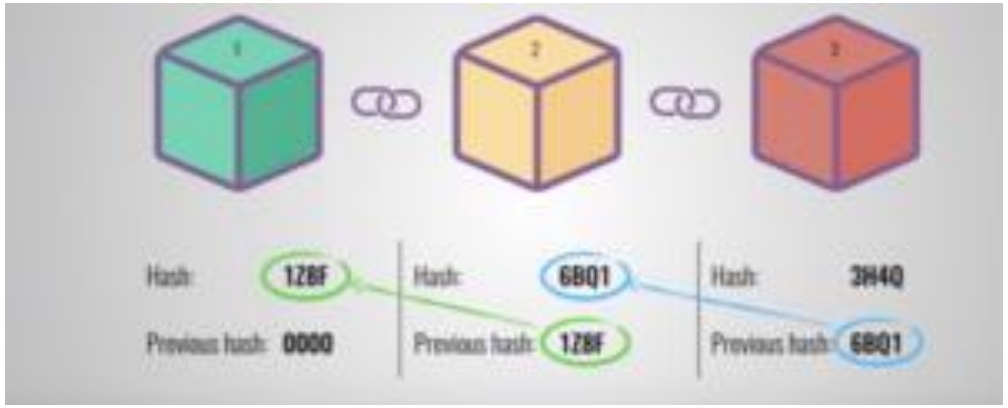
5. Adding a Block to the Blockchain

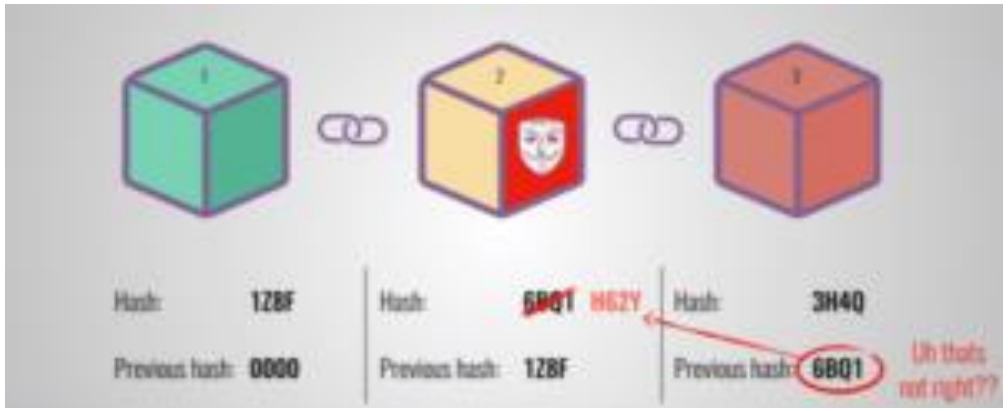


6. Miners Get Rewards



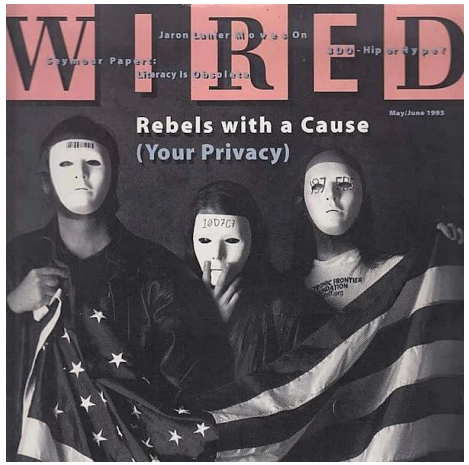
7. The Blockchain Keeps Growing





History

1990
Cypherpunk



A cypherpunk is one who advocates the widespread use of strong cryptography and privacy-enhancing technologies as a means of effecting social and political change.

1993
A Cypherpunk's Manifesto

David Chaum and DigiCash (1990s)

Adam Back and Hashcash (1997)

Wei Dai and B-Money (1998)

Nick Szabo and Bit Gold (1998-2005)

Hal Finney and Reusable POW (2004)

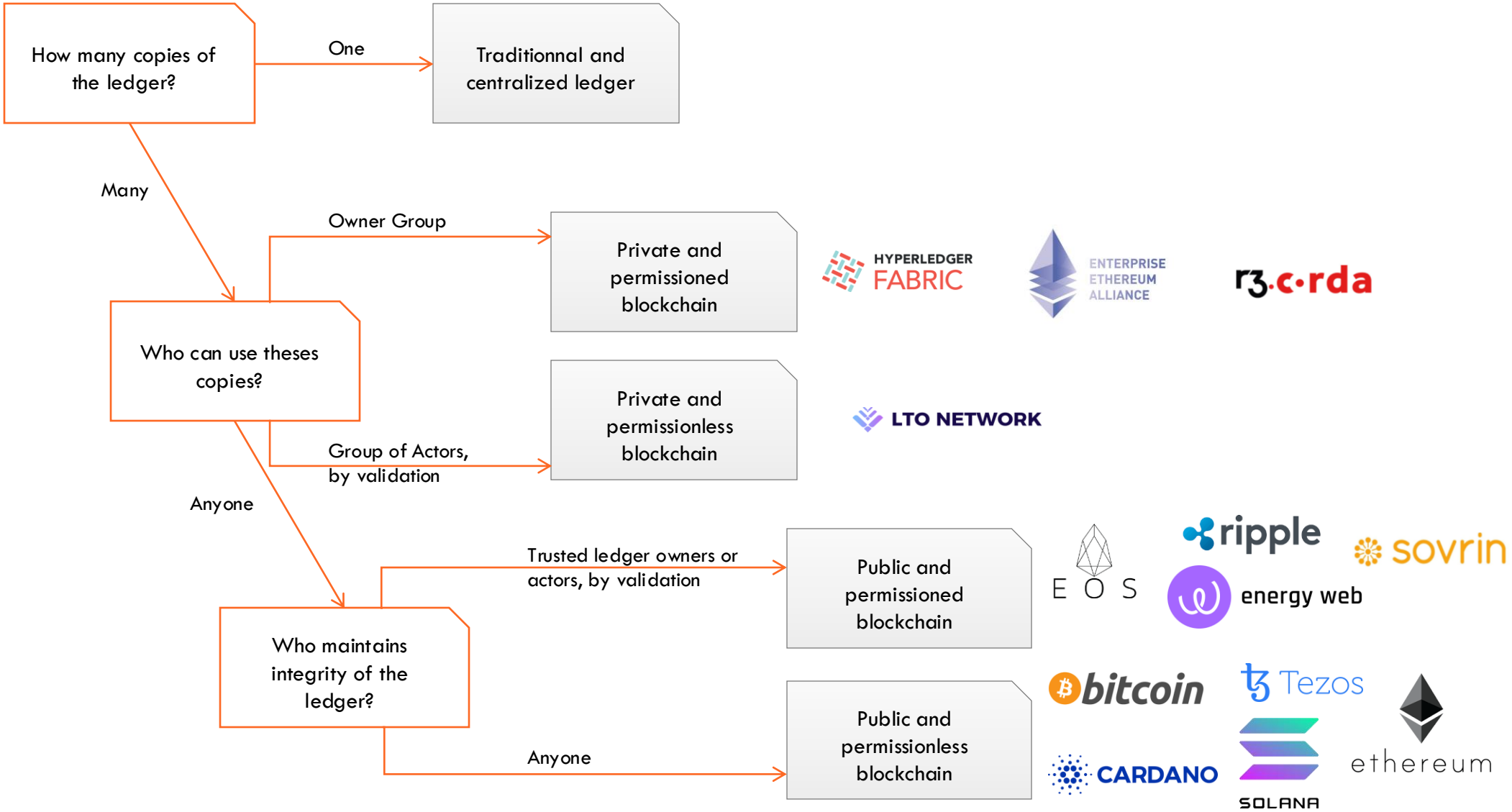
History

2009

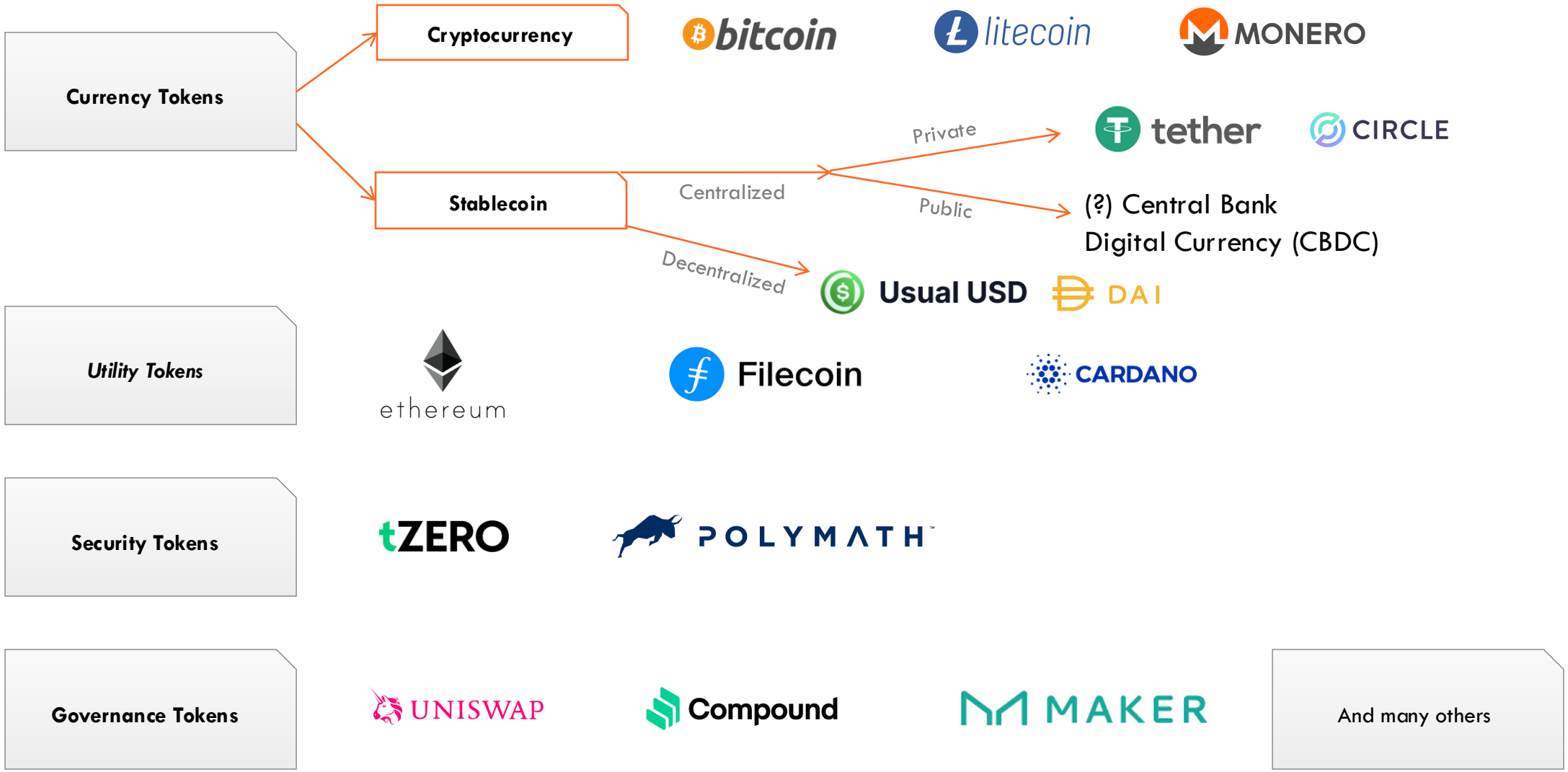
2015

2017

Public or private, permissioned or permissionless?



What type of token?



A token can serve multiple functions and, for example, be simultaneously a utility, security, and governance token

Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is **$2.65T**, a ▼ 0.29% decrease over the last day. Read More

Trending Coins

1	NEI	$0.008262	▲ 14.85%
2	TRUMP	$10.45	▲ 1.39%
3	PEPE	0.0_5$6707	▲ 1.53%
4	SNAI	$0.024	▲ 1.21%
5	BNB	$581.6	▲ 4.44%

Trending on DexScan

1	MERY/WCRO	$0.00002122	▼ 11.23%
2	STAR10/WBNB	$0.01469	▲ 31.85%
3	MATEZ/USDT	$17.78	▲ 7.47%
4	oGPU/WETH	$0.4149	▼ 1.76%
5	WEPE/WETH	$0.00005477	▲ 8.19%

Market Cap

$2.65T

▼ 0.29%

CMC100

$159.79

▼ 0.80%

Fear & Greed

21

Fear

Altcoin Season

15/100

Bitcoin Altcoin

All Crypto | NFTs | Categories | Token unlocks | Rehypo | Memes | SOL | DOT | BNB | USA | AI | RWA | Gaming | DePIN | DeFAI | AI Agents

Coins | DexScan | Top | Trending | New | Gainers | Most Visited | Filters | Columns

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$80,956.61	▼0.51%	▼1.34%	▼10.41%	$1,605,885,839,084	$30,185,828,851 372.65K BTC	19.83M BTC	

Custodial or non-custodial wallet?