

Smart contracts and blockchain



Mário Amorim Lopes

May 6th, 2021



instituto
new.economy

Always look on the crypto side of life

Today's agenda

- 14h - 16h **Smart contracts and blockchain**
Mário Amorim Lopes
- 16h - 16h30 **Coffee-break**
- 16h30 - 17h00 **Case-study: Fostering consumer bargaining and e-procurement through a decentralised marketplace**
Mário Amorim Lopes
- 17h - 18h **Governance and regulatory issues of cryptos and DeFis: challenges and opportunities**
Ian Gauci

Today's agenda

- 14h - 16h

Smart contracts and blockchain

Mário Amorim Lopes

1. The advent of decentralised finance
2. The origins of smart contracts
3. Comparing DeFi with TradFi
4. Some key DeFi projects

- 16h - 16h30

Coffee-break

- 16h30 - 17h00

Case-study: Fostering consumer bargaining and e-procurement through a decentralised marketplace

- 17h - 18h

Governance and regulatory issues of cryptos and DeFis: challenges and opportunities

1. The advent of decentralised finance

The ethos behind Bitcoin

**Bitcoin was created in 2008.
It is no coincidence.**



**While some
were on the street...**



Others were occupied working on a new technology

[Index](#) | [Next](#)

Cryptography Mailing List

Bitcoin P2P e-cash paper

2008-10-31 18:10:00 UTC - [Original Email](#) - [View in Thread](#)

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:

<http://www.bitcoin.org/bitcoin.pdf>

The main properties:

Double-spending is prevented with a peer-to-peer network.

No mint or other trusted parties.

Participants can be anonymous.

New coins are made from Hashcash style proof-of-work.

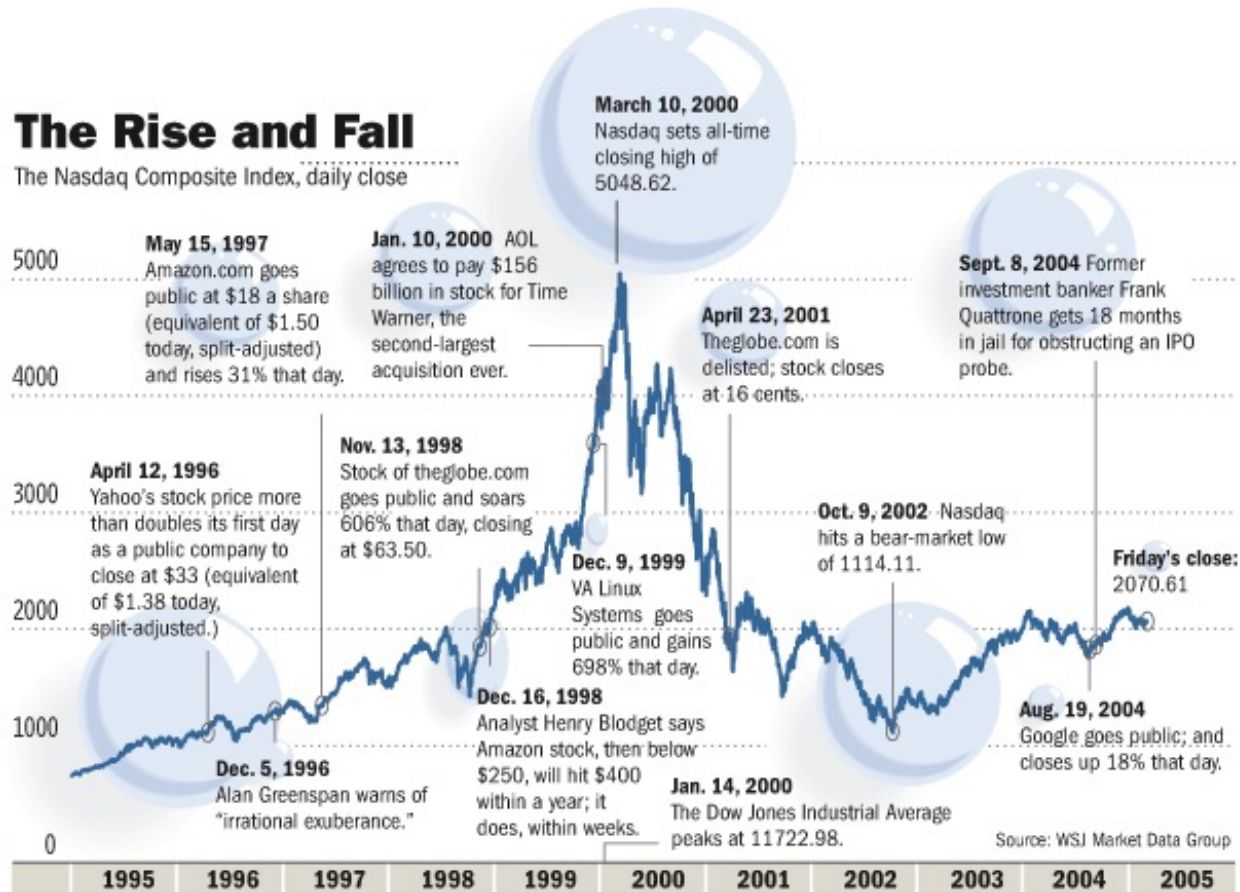
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?

The Rise and Fall

The Nasdaq Composite Index, daily close



“

To fight this recession the Fed needs...soaring household spending to offset moribund business investment.

[So] Alan Greenspan needs to create a housing bubble to replace the Nasdaq bubble.



Paul Krugman

Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



We agreed on the reduction despite our consensus that the economy probably did not need yet another cut [in the Fed funds rate].

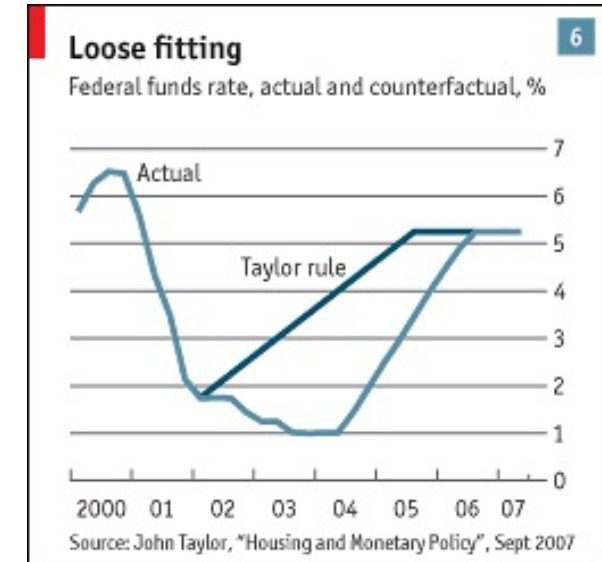
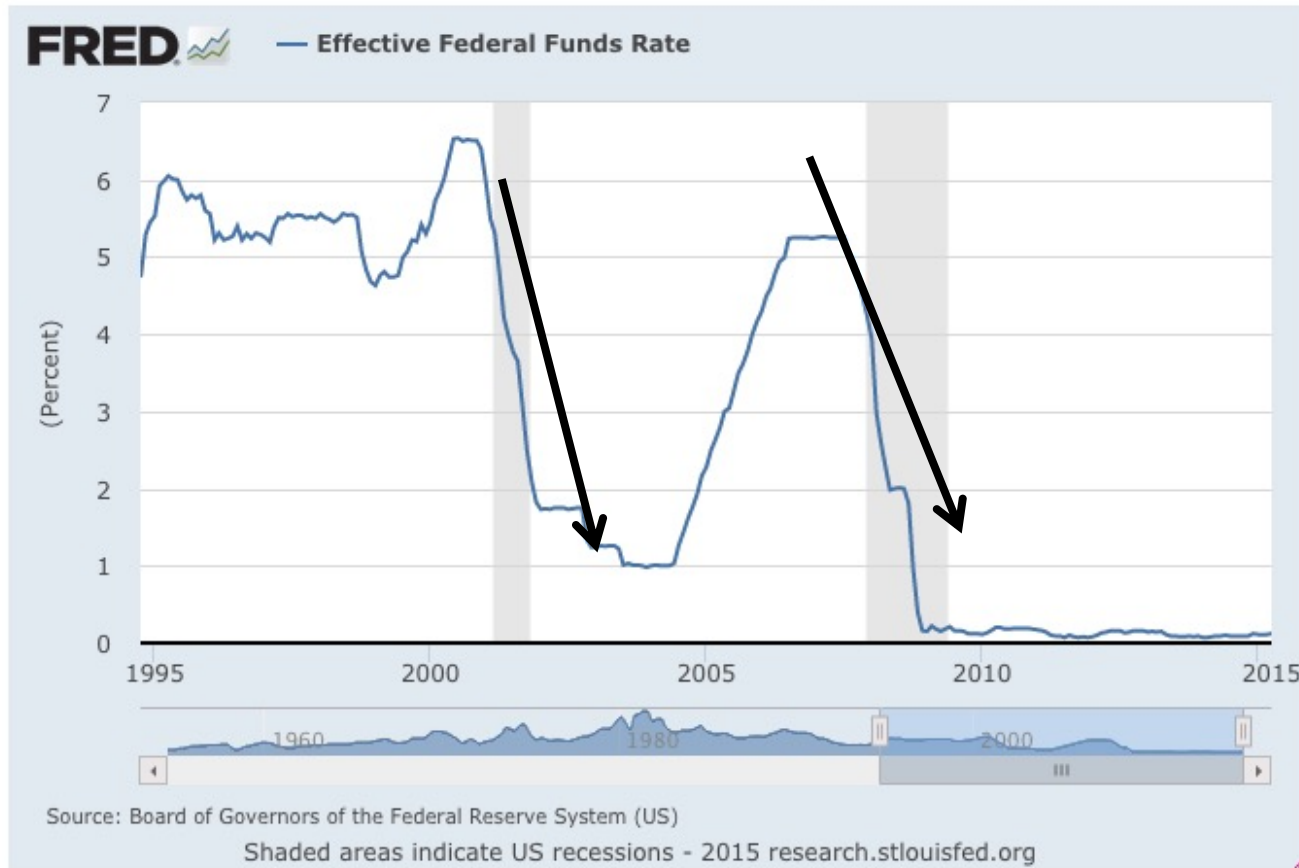
We wanted to shut down the possibility of corrosive deflation; we were willing to chance that by cutting rates we might foster a bubble, an inflationary boom of some sort, which we would substantially have to address.

Time would tell if it was the right decision, but it was a decision done right.

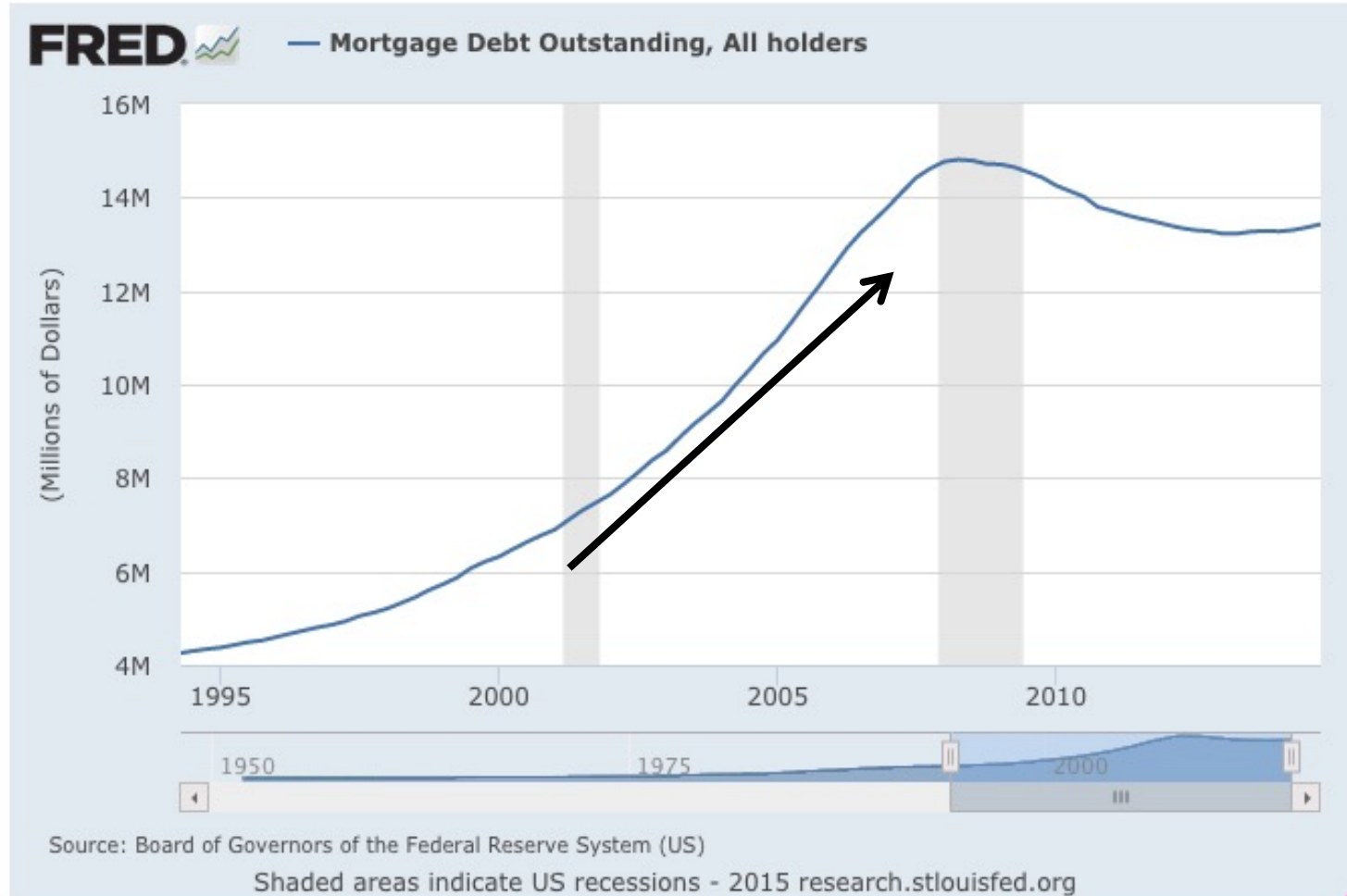


Alan Greenspan

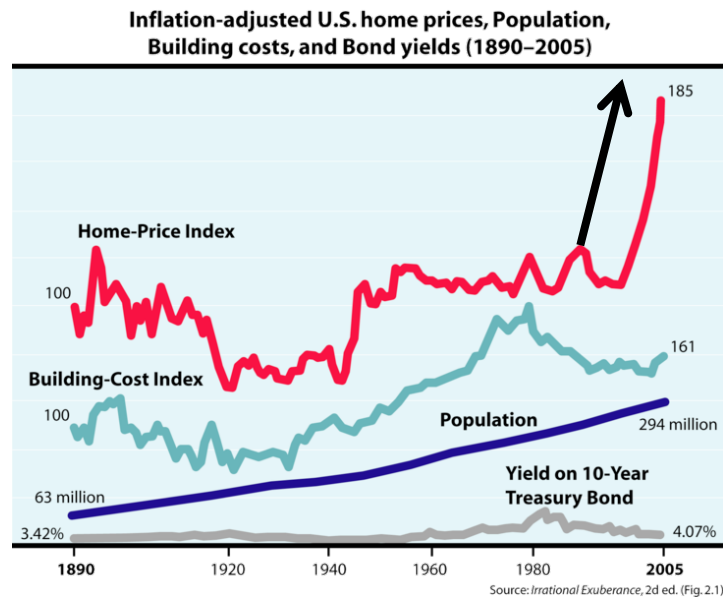
Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



It means we use the mighty muscle of the federal government in combination with state and local governments to encourage owning your own home.

George W. Bush

Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



If we can bend the housing finance system to transform the poor into home purchasers, [...] they can start to build equity wealth.

\$3 trillion in commitments Fannie Mae has made [...].

We have a dream too -- **that all Americans will have equal access to the American Dream of homeownership.**



Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



All the signs I look at show **the housing market is at or near the bottom.**

The U.S. economy is very healthy and robust.



Henry Paulson (April 2007)



Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



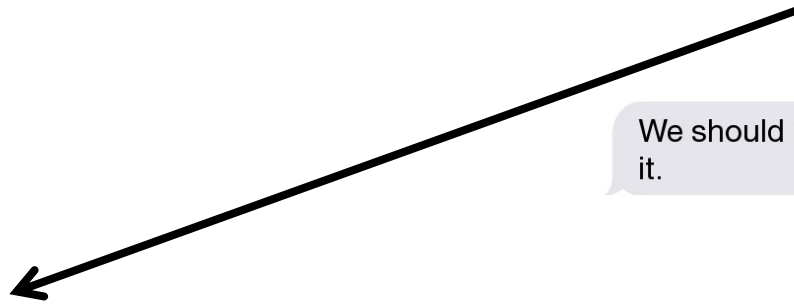
Markowitz 2 Asset Portfolio Variation

σ^2 = Variance
 σ = Standard Deviation
 ρ = Correlation of Two Assets

$$\sigma_{pf}^2 = w_a^2 \sigma_a^2 + w_b^2 \sigma_b^2 + w_a w_b \sigma_a \sigma_b \rho_{ab}$$

A screenshot of a text message conversation on a mobile phone. The status bar at the top shows signal strength, 3G, and 47% battery. The header includes a back arrow, "Messages", and "Contacts". The messages are as follows:

- Grey bubble: "By the way, that deal is ridiculous."
- Blue bubble: "I know, right, model definitely does not capture half the risk."
- Grey bubble: "We should not be rating it."
- Blue bubble: "We rate every deal. It could be structured by cows, and we would rate it."
- Grey bubble: "But there's a lot of risk associated with it—I personally don't feel comfy signing off as a committee member."

The bottom of the screen shows a camera icon, a text input field with "Text Message", and a "Send" button.

Bitcoin was born out of a general distrust in the legacy financial system. Was it justified?



Investors are worried about a hard landing.
I am less concerned because...

I believe that the Fed is our friend



Ed Yardeni



And so Bitcoin was born



RAW HEX VERSION BITCOIN GENESIS BLOCK

```

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 ....;f1yz{.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..ð.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠŸ°pUH'
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 ybàè.ad¶Iö¿?LŸ8Ä
0000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.â.Á.Þ\8M+ø..W
0000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 00 ŠLp+kñ._~....
  
```

2. The origins of smart contracts

The building blocks of the blockchain puzzle were being assembled long before it emerged

1990s

1991

Extropians mailing list started by Max More

1992

Cynthia Dwork and Moni Naor, "[Pricing via Processing or Combatting Junk Mail](#)" (16 Aug)

Eric Hughes launches the cypherpunks mailing list with support from John Gilmore and Hugh Daniel (21 Sep)

1993

Eric Hughes, "[A Cypherpunk's Manifesto](#)" (9 Mar)

"An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy."

1994

Cross-network electronic cash payment demonstration by David Chaum (DigiCash) at the first World Wide Web Conference (25 May)

1995

Markus Jakobsson, "[Ripping coins for a fair exchange](#)" (21 May)

1996

Nick Szabo, "[Smart Contracts: Building Blocks for Digital Markets](#)" published in Extropy 16

1997

[Hashcash](#) announcement by Adam Back on cypherpunks mailing list (28 Mar)

1998

Nick Szabo, "[Secure Property Titles with Owner Authority](#), first use of "bit gold"

Wei Dai announces [b-money](#), "a new protocol for monetary exchange and contract enforcement for pseudonyms" (26 Nov)

1999

Markus Jakobsson and Ari Juels, "[Proofs of Work and Bread Pudding Protocols](#)" (20 Sep)

Smart contracts are just contracts described and executed by computer code

New institutions, and new ways to formalize the relationships that make up these institutions, are now **made possible by the digital revolution**.

I call these new contracts "**smart**", because they are **far more functional** than their **inanimate paper-based ancestors**.

No use of artificial intelligence is implied.

A smart contract is a **set of promises**, specified **in digital form**, including protocols within which the parties **perform on these promises**.

In that popular article from 1996, Nick Szabo exemplified smart contracts beyond the traditional digital cash use case

“We can extend the **concept of smart contracts** to **property**. Smart property might be created by embedding smart contracts in physical objects.

These **embedded protocols** would automatically give **control of the keys** for operating the property to the party who rightfully owns that property, based on the **terms of the contract**.

For example, a **car might be rendered inoperable** unless the proper challenge-response protocol is completed with its rightful owner, **preventing theft**.

If a loan was taken out to buy that car, and the **owner failed to make payments**, the smart contract could automatically invoke a lien, which **returns control of the car keys to the bank**. This "smart lien" might be much **cheaper** and more **effective** than a **repo man**.

Also needed is a protocol to provably remove the lien when the loan has been paid off, as well as hardship and operational exceptions. For example, it would be rude to revoke operation of the car while it's doing 75 down the freeway.”

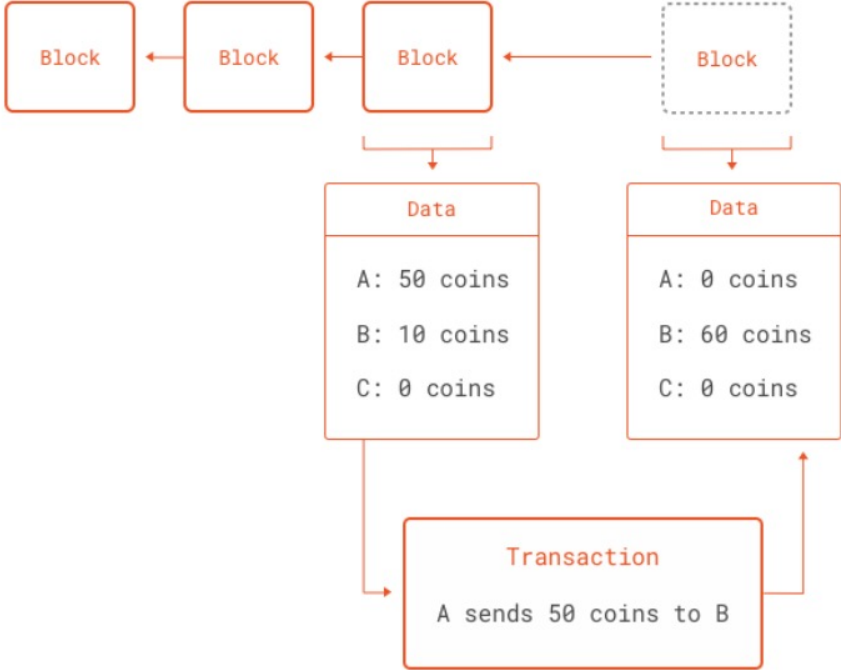
Ethereum's whitepaper, released in 2013, laid the groundwork for the first popular implementation of a blockchain focused on smart contracts

A Next-Generation Smart Contract and Decentralized Application Platform

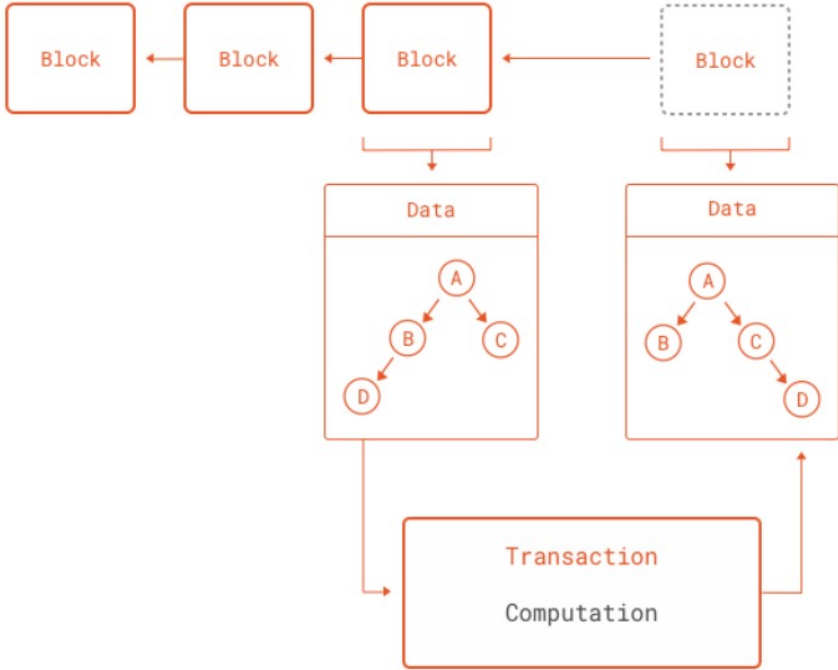
Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or [intrinsic value](#) and no centralized issuer or controller. However, another - arguably more important - part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcoin. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ([colored coins](#)), the ownership of an underlying physical device ([smart property](#)), non-fungible assets such as domain names ([Namecoin](#)), **as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules** ([smart contracts](#)) or even blockchain-based [decentralized autonomous organizations](#) (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

After all, transactions are basic computations. So, as blockchains scale, they can perform more complex and varied computations

From a distributed ledger



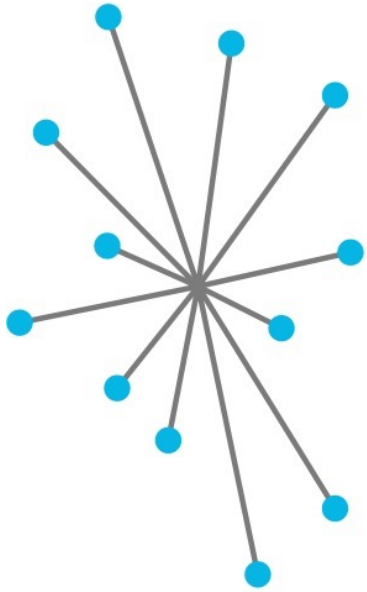
To distributed scripts



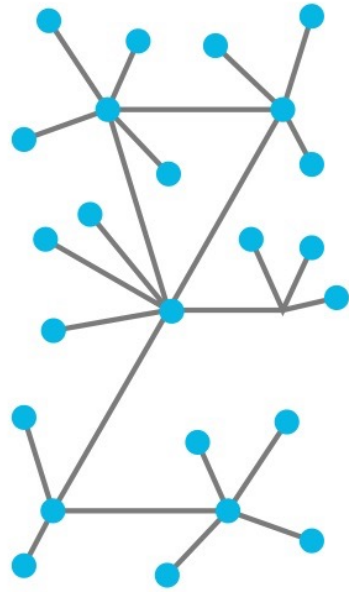
What makes the blockchain unique?

What makes the blockchain unique?

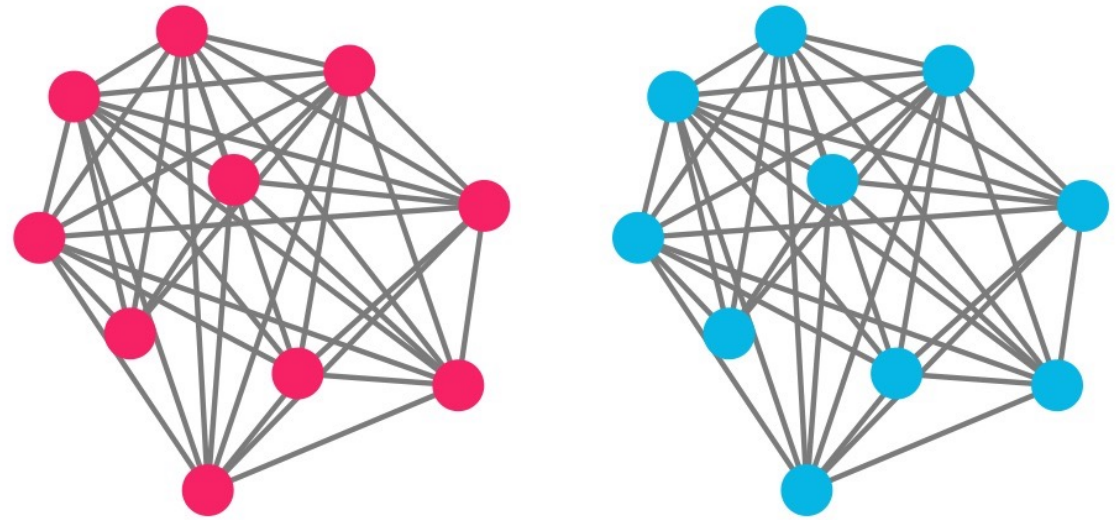
Centralized



Decentralized



Distributed Ledgers



What makes the blockchain unique?

1. Trustless
2. Decentralized (distributed, P2P)
3. Consensus-based
4. (Virtually) immutable
5. Smart contracts

Oh, and one more thing...

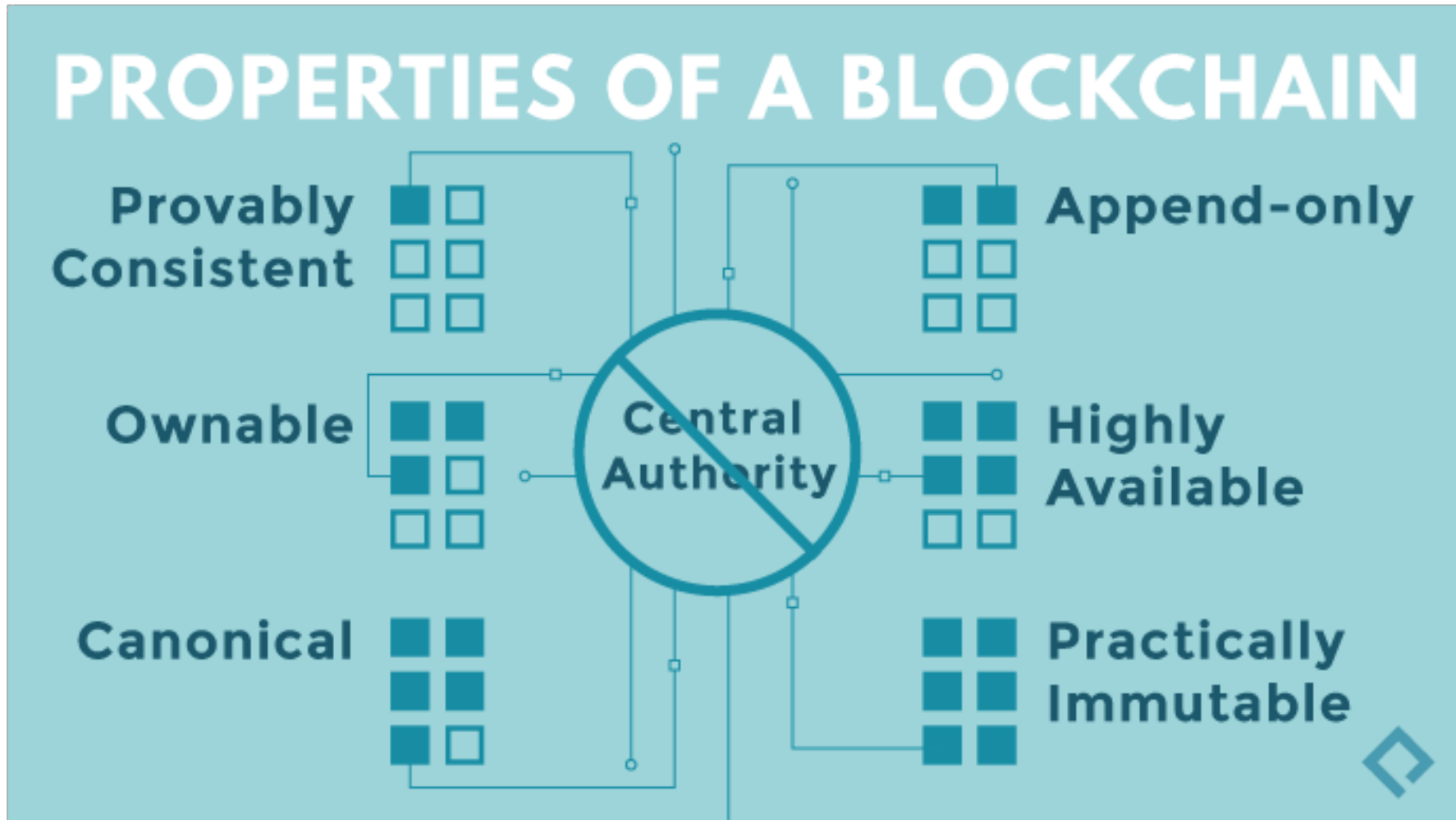
What makes the blockchain unique?



Robert Ryman – Ledger (in exhibition at Tate)



What makes the blockchain unique?



What makes the blockchain unique?

Characteristics of high-potential use cases



Shared repository

A **shared repository** of information is used by multiple parties



Multiple writers

More than one entity generates transactions that require modifications to the shared repository



Minimal trust

A level of **mistrust exists between entities** that generate transactions



Intermediaries

One (or multiple) intermediary or a central gatekeeper is present to enforce trust

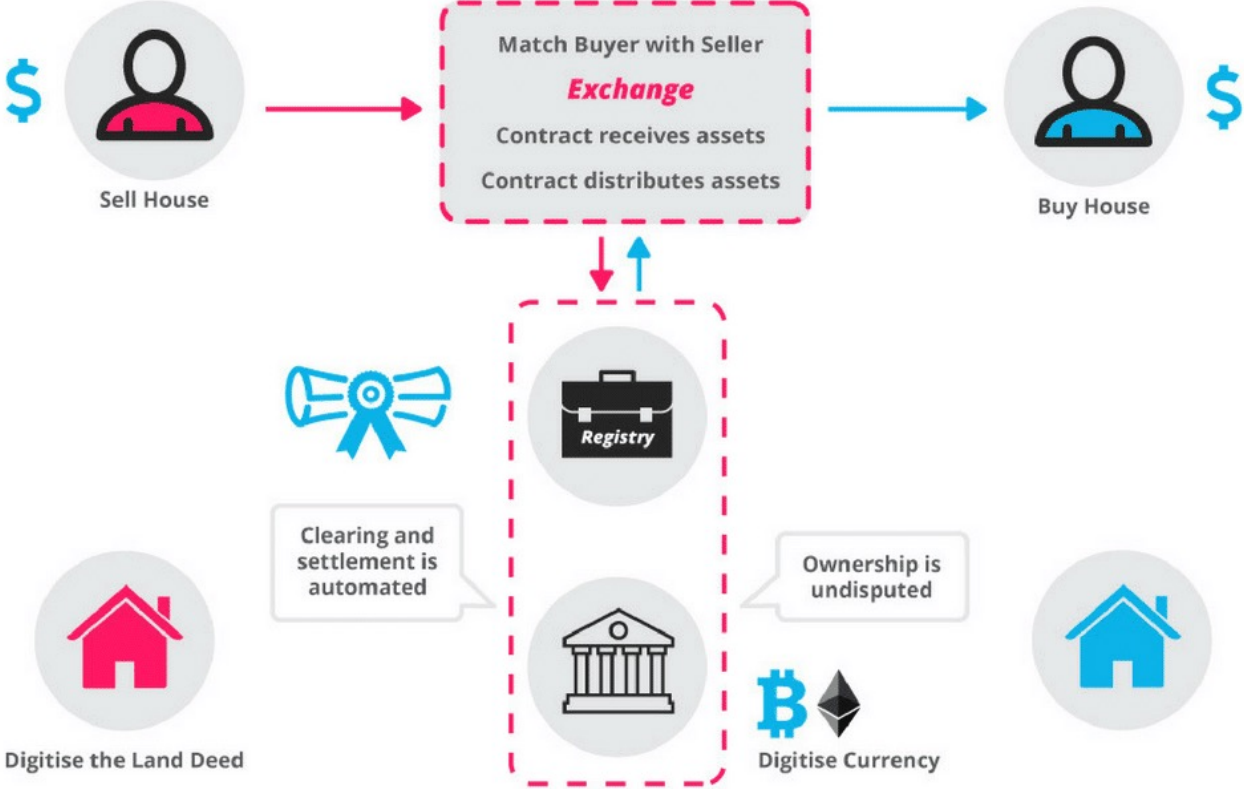


Transaction dependencies

Interaction **or dependency between transactions** is created by different entities

Will the lawyer of the future be a coder too?

How Smart Contracts Works



Smart contracts reduce transactional costs and enhance efficiency



Blockchain properties: from an end-user view

Thousands of use cases

Transportation
Online storage
Mesh networks
Healthcare

DAOs

Millions of uses

Smart contracts

Wagers
Bounties
Family trusts
Performance proofs
Escrows

Hundreds of millions of uses

Pegged services

Naming
Identity
Ownership
Voting
Membership

Billions of uses

Currencies

Transfers
Payments
Tips
Crowdfunding

Key blockchain use cases

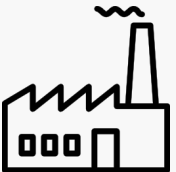
Sectoral applications of blockchains



Markets and Finance



Public Sector



Enterprise and Industry



Legal Industry



Energy



Healthcare



Distributed computation



PUBLIC SECTOR

One year ago: 117 Initiatives in 26 Countries



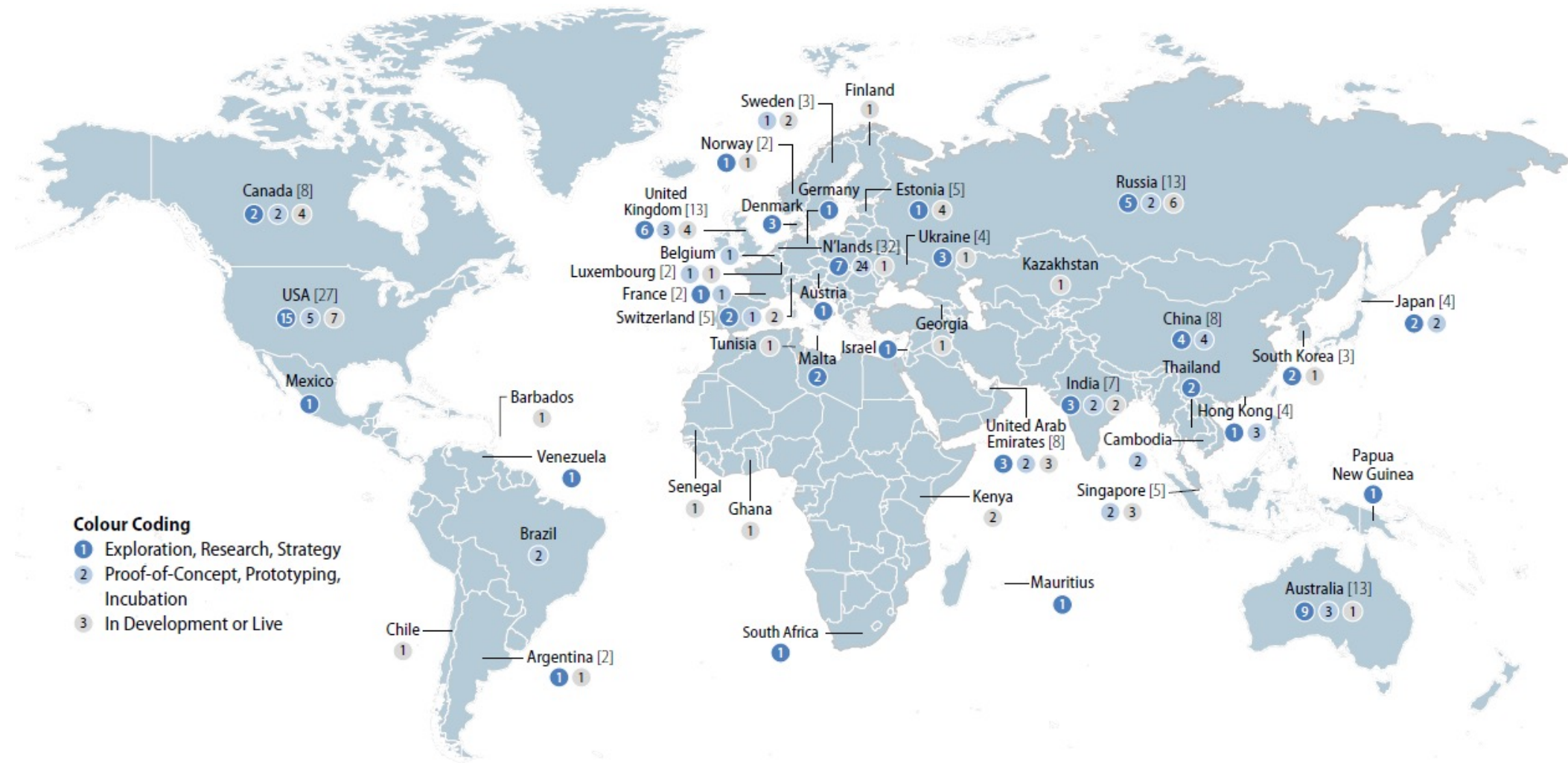
Top 10 most active public sector use cases*

- | | |
|------------------------------|-----------------------------|
| 1. Digital currency/payments | 7. Voting (proxy) |
| 2. Land registration | 8. Corporate registration |
| 3. Voting (elections) | 9. Taxation |
| 4. Identity management | 10. Entitlements management |
| 5. Supply chain traceability | * Measured by observing the |

Color coding key

- In progress
- Planned
- Announced

Now: 202 blockchain initiatives in 45 countries



Potential use cases in the Public Sector

Use Case	Description
Identity	Establishing and maintaining identities for citizens and residents (birth certificates, marriage licenses, visas, death records).
Personal records	Interoperable health records, insurance records, etc.
Land title registry	Details and historic records related to real estate and property transactions.
Supply chain management, inventorying	Tracking an asset from its creation, transportation, purchase, and inventorying.
Benefits, entitlements, and aid	Social security, medical benefits payments, domestic and international aid. Anticipatory/automated payments could be automated through Smart Contracts.
Contract and vendor management	Tracking and paying vendors, managing purchase commitments and transactions, and monitoring schedule performance. Can allow for perfect transparency of government expenditures.
Voting	Enabling new methods of digital voting, ensuring eligibility, accurate counting, and auditing (e.g., to avoid ballot-rigging).
Streamlining interagency processes	Blockchains and smart contracts can automate transaction handling and improve information sharing – allows each agency to better focus on their own mission and tech without as much need to consider others tech.

Example 1: Vehicle wallet (Denmark)

Problem

During a car's lifecycle it undergoes various phases and activities (tests, repair, loan, insurance and changes in ownership). When a car is sold from one person to another, there can be a lack of information from either the buyer or seller. On the seller's side, the car could have undergone an undesirable re-build or even be stolen. On the buyer's side, the buyer could never re-register the car, which could result in continuous taxes for the original seller.

Solution

Vehicle Wallet is a partnership between payment service provider and the Danish Tax Administration. It is a supply chain management tool where data concerning the car is saved in one distributed ledger and creates one agreed and shared record of the vehicle history as it is transferred across the supply chain. This reduces risks for buyers and sellers, and helps ensure Denmark receives all proper taxes.

Example 2: BenBen (Ghana)

Problem

For land property, Ghana lacked a systemic way to determining the legal existence of parcels and to track land ownership titles. This prevented authorities and property owners from having clear certainty and visibility over what belongs to whom, resulting in regular disputes. In addition, because previous processes were on paper, it could take over a year to register the sale/purchase of a property, which was a fraud risk for both sellers and buyers.

Solution

BenBen provides an Ethereum-run digital register system of all land registries across Ghana. It is able to certify land information through the cross-cutting of satellite imagery and on-the-ground verifications, working hand-in-hand with local stakeholders in the land market. It aggregates all the information such that financial institutions and the Lands Commission have real-time access to the data. Property transaction times have been reduced by 75% and court disputes have been reduced.

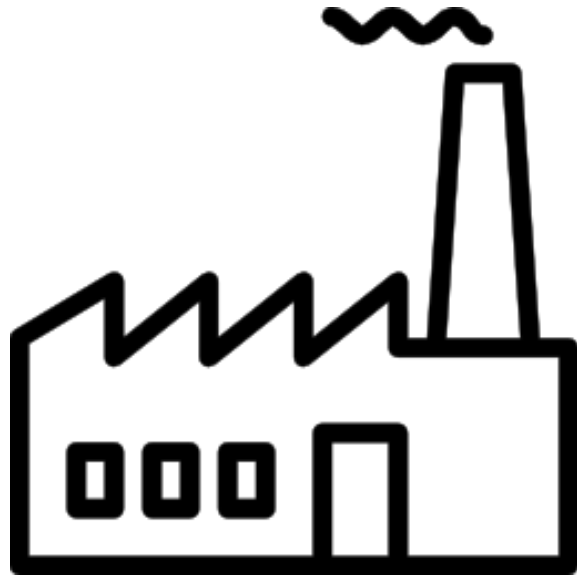
Example 3: Project Ubin (Singapore)

Problem

The Monetary Authority of Singapore (MAS) conducted a study that found that Inter-bank payments within Singapore and cross-border financial transactions were inefficient and slow.

Solution

MAS partnered with R3– a consortium of banks and regulators to create a prototype for a Blockchain-based digital Singaporean dollar to facilitate digital transactions. This would allow for incorruptibility of records through a decentralised trust system, but also 24-hour processing with no centralised – i.e. human-based – checks required. The partnership has successfully developed software prototypes of three different models for decentralised inter-bank payment that are now being explored. MAS has published the source code as open source software on GitHub.



ENTERPRISE AND INDUSTRY



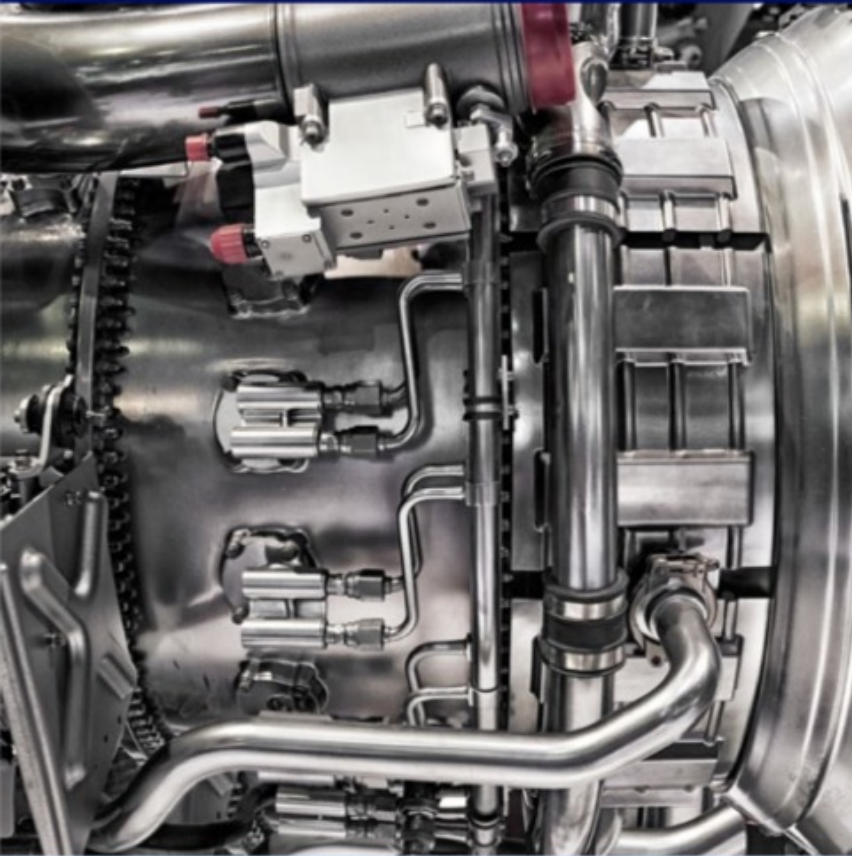
□ Challenges

Disparate record-keeping and reporting systems can lead to scattered, incomplete and unreliable manifests, bills of lading, certifications and more.

□ Opportunities

With blockchain-stored records, all relevant information can be simultaneously and securely available to sender, receiver, shipper and regulators.

- **The result:** IBM and Maersk have announced a joint effort to streamline shipping with an efficient, secure global trade digitization platform based on IBM Blockchain. The new venture will address needs for transparency, simplicity and open standards as goods move across borders and trading zones.



□ Challenges

Supply chain intelligence is knowing more than where goods are at any given moment. To find the source of flawed parts or component failures, being able to trace the origin and provenance of previously shipped goods is critical.

□ Opportunities

With blockchain records that reflect a product's geographic flow and how it was treated, you can examine sources, investigate industry certifications, track restricted or dangerous components, discover storage-condition anomalies and more.

- **The result:** A large aircraft manufacturer has adopted IBM Blockchain technology to track the origin, location and status of its components. This unlocks deeper insight into the quality and trustworthiness of each tracked part, providing documentation on certification, installation and inspection.



❑ Challenges

Even the best-planned supply chain can be thrown into chaos by natural disasters, unforeseen shortages, spikes in demand or a litany of smaller issues. With today's elongated supply chains, any delay or faulty delivery can impact production.

❑ Opportunities

Delays involving weather, labor disputes or error are inevitable; blockchain-optimized processes help to resolve real-world issues. Knowing that a shipment is incomplete or at risk can instantly trigger remediation actions like supplier substitutions or price adjustments — before a crisis emerges.

- ❑ **The result:** We're building an AI network that predicts the future instead of reacting to the past. In addition to ensuring food quality, blockchain data could soon feed an AI solution that does everything from tracking inventory and predicting future demand to monitoring freezer conditions and anticipating future repairs or replacements.



LEGAL INDUSTRY

Legal industry: do we still need notaries?

- **Notaries are key in witnessing and certifying (among other activities):**
 - Validity of signatures (it is signed by the right person)
 - Certifying the authenticity of documents (closing a contract, for instance)
- **Currently, these are labourious processes**

Legal industry: do we still need notaries?

Solution: A blockchain for storing contracts and proving existence

How it works:

- Documents are signed with a timestamp, proving it took place
- Remote identity verification may be enabled through remote videos
- A journal (the blockchain) keeps a record of all the contracts signed and revoked

Blocknotary

TIMESTAMP

Blockchain enabled timestamps

OPEN



INTERVIEW

Blockchain enabled video interviews for remote identity verification

OPEN



JOURNAL

Blockchain enabled notary journal

OPEN





HEALTHCARE

Health care: Electronic Health Records on the blockchain

- Medical records and patient information (Electronic Health Records) are scattered throughout the many institutions visited
- Access control is very limited and conspicuous in some health systems – any physician can access the patient's information
- Data exchange is also scant: private and public institutions usually don't share patient information
- The patient is not the owner de facto of the data
- A malicious user with access to the database could extract millions of records of patients, which is confidential and highly sensitive information

Health care: Electronic Health Records on the blockchain

- **Solution:** A permissioned (private) blockchain where both data (optional) and access control is stored.
- The blockchain provides distributed, sharable and transparent access to data
- Patients are the effective owners and can revoke access (or allow only for a given period)
- No single entity controls the data
- Information can be stored anonymously without giving away the patient ID or name
- Data can be stored off-chain, solving GDPR concerns and the right to erasure



[Team](#)

[Whitepaper](#)

[News](#)

[Partnership](#)

[Events](#)

[Careers](#)

[Contact](#)

[English](#) ▼

[MedTokens: Where to Buy](#)

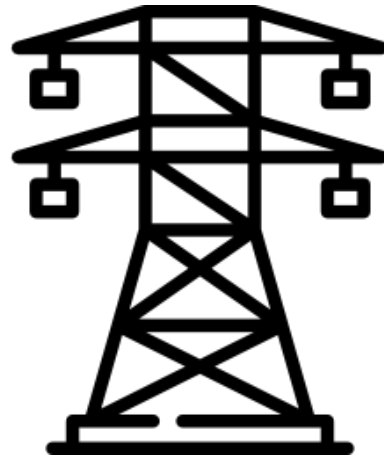


Own Your Health

Be part of Medicalchain's pilots

[Register as a Patient >](#)

[Register as a Practitioner >](#)



ENERGY



The Johansons

Meet the Johansons. They are a fictional family living in Portugal.

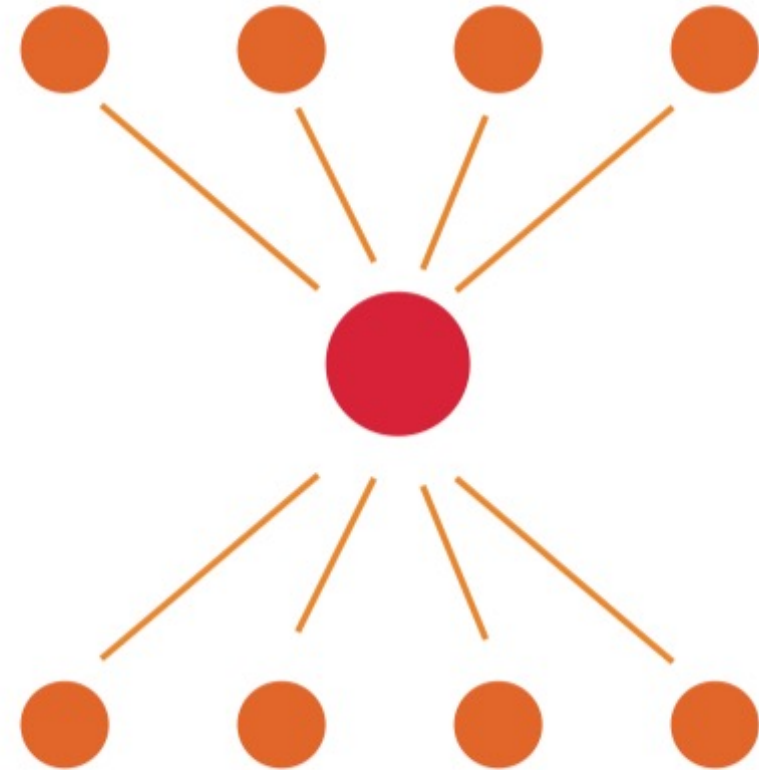
The Johansons sometimes produce more energy than their current needs, and so their meter spins in reverse.

Can the Johansons sell their surplus to needing neighbors?
Not currently.



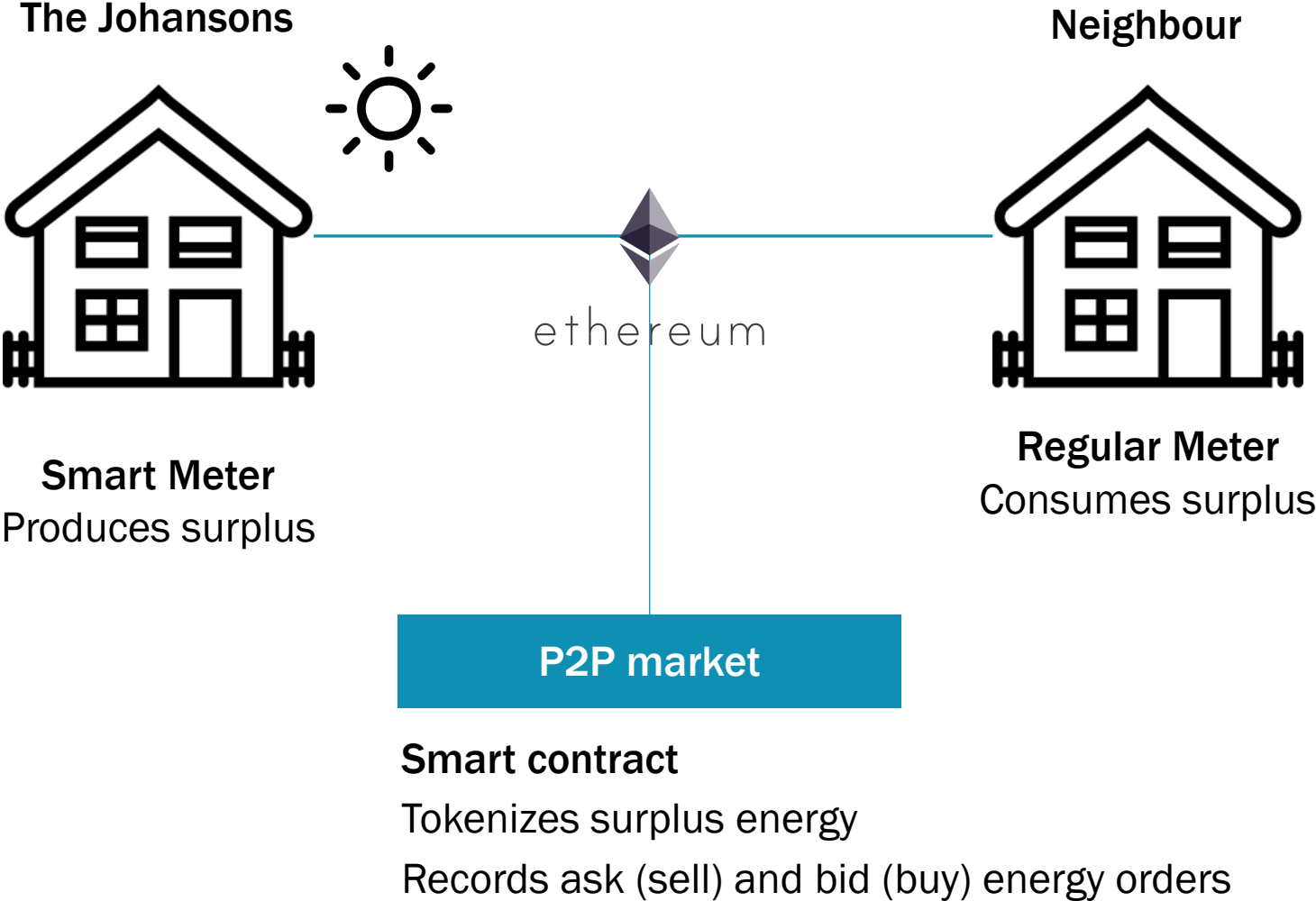
Smart energy grids

- The transactional model is highly dependent on a central authority (REN) in charge of balancing the grid



Smart energy grids

Solution: A P2P energy market with options/futures for prosumers



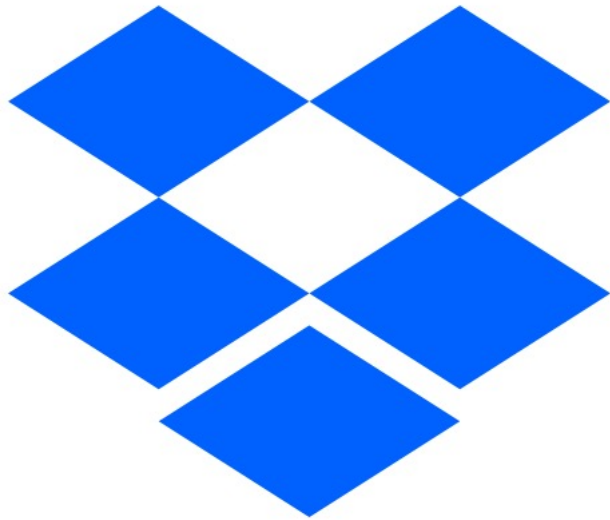


xGrid

Peer-to-Peer electricity trading across the regulated electricity network (the grid)



Distributed Computation



Dropbox

- All your files are handled and stored by one single entity
 - Do you trust that entity?
 - Is it secure by design?
 - Can NSA access your data?

Decentralised cloud storage

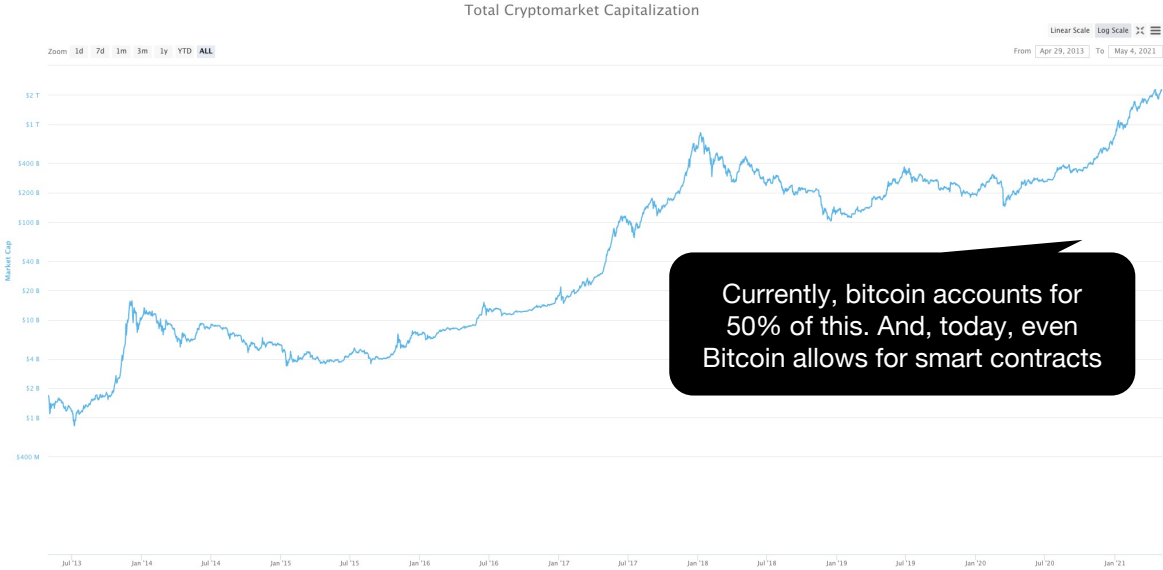
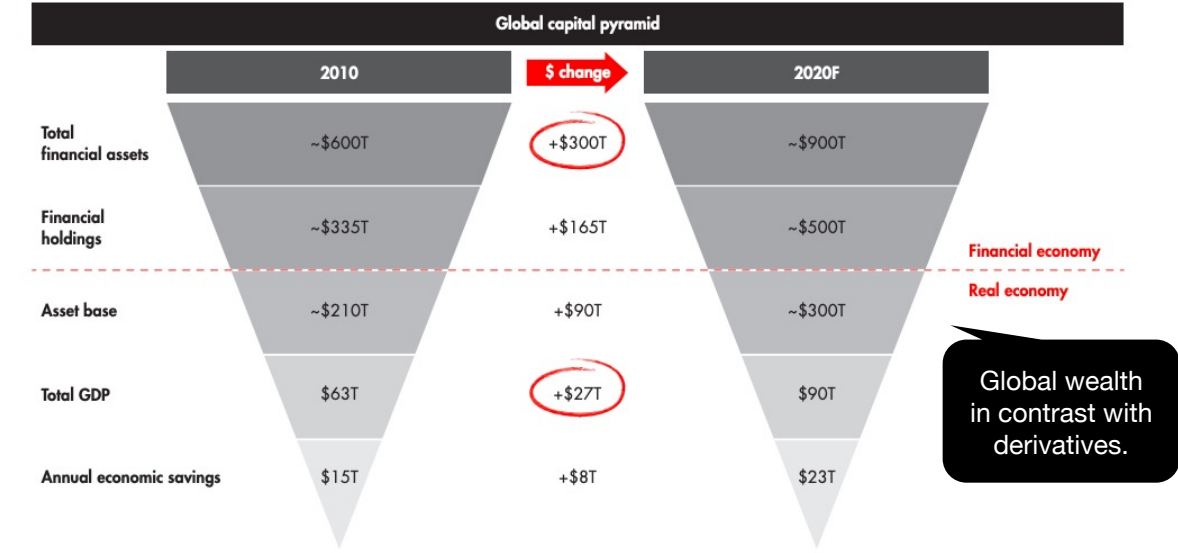
- Your files are split in thousands of parts, encrypted and sent to thousands of users
- No single user or entity can have access to your files
- Available slack in ordinary PCs can be used as storage

3. Comparing DeFi with TradFi

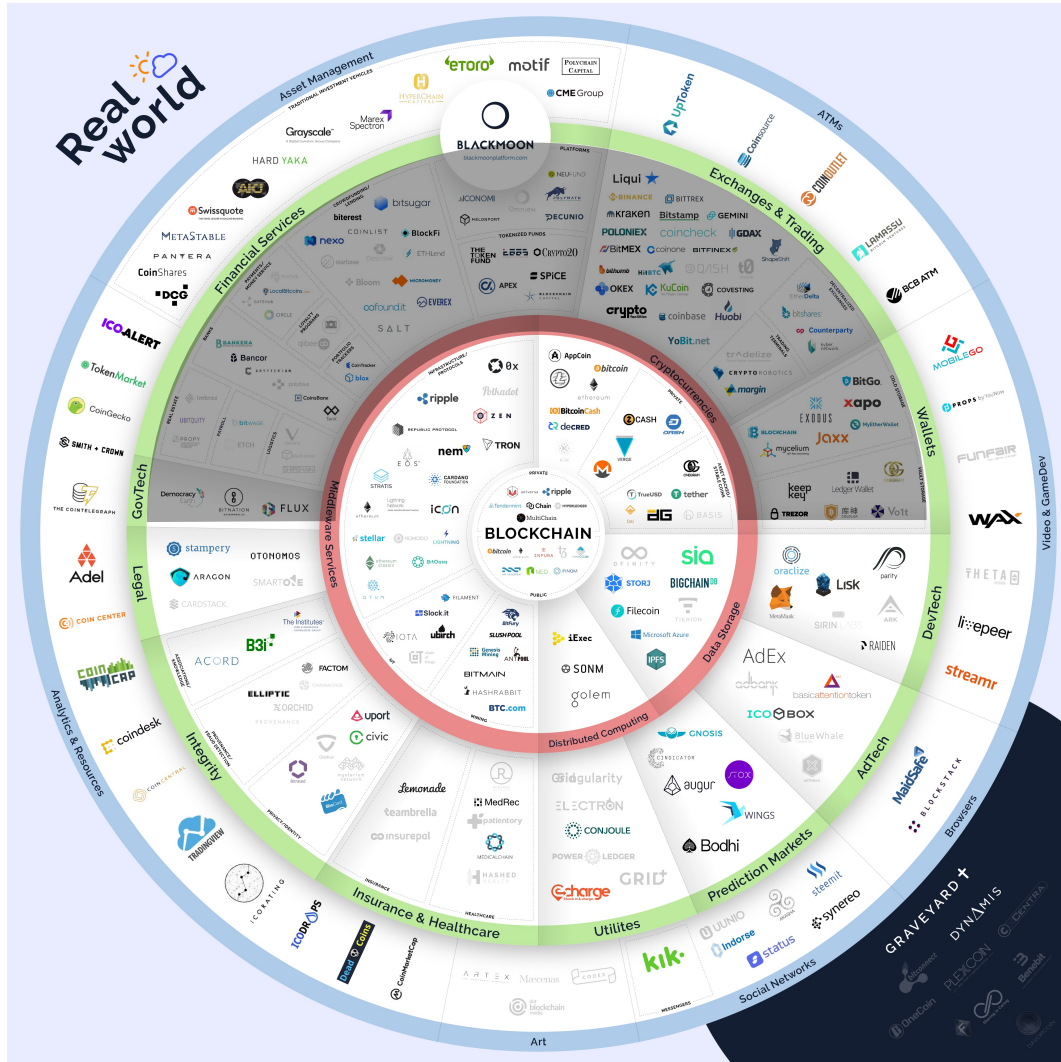
As contracts are the building blocks of our free markets, so did smart contracts become the building blocks of our digital, decentralised markets

Contracts are behind our \$900T traditional economy for centuries

And smart contract are the bedrock of this transparent \$2T decentralised economy



The applications of this decentralised economy touch many sectors, but most use cases and projects are related to finance



Syndicated Loans Business

<p>Clients</p>	<p>Faster Trade Settlement in 6 - 10 days per loan in the US</p>	<p>Investment Banks</p>	<p>Increased fee income US \$2 - \$7 billion per annum globally</p>
----------------	---	-------------------------	--

Mortgage Loan Origination

<p>Customers</p>	<p>Lower Processing Fees \$480 - \$960 savings per loan in the US</p>	<p>Banks</p>	<p>Lower operations costs US \$3 - \$11 billion per annum in the US and EU</p>
------------------	--	--------------	---

Motor Insurance Policy Servicing

<p>Customers</p>	<p>Lower Insurance Premiums \$45 - \$90 Savings per annum in the US and EU</p>	<p>Insurers</p>	<p>Lower claims settlement cost US \$21 billion per annum globally</p>
------------------	---	-----------------	---

That's because smart contracts can unlock value in financial services through various vectors

Anticipated Effects of Smart Contracts			Primary Source of Benefit		
			Automation	Self-execution & immutability	Distributed access & verification
Financial institutions	Operating cost (overhead, service)	↓	✓	✓	
	Legal and auditing fees	↓	✓	✓	✓
	Operational risk	↓	✓	✓	✓
	Counterparty risk	↓		✓	✓
	Data concentration risk	↓			✓
	Records replication	↓			✓
	Physical documentation	↓	✓		✓
	Coordination ease	↑			✓
	Verification ease	↑			✓
Customers	Service cost	↓	✓		✓
	Trust barrier	↓		✓	✓
	Uncertainty	↓		✓	✓
	Access	↑	✓		✓
	Timeliness	↑	✓	✓	✓
	Transparency	↑			✓

The overall goal is to disrupt traditional finance functions and correct the inefficiencies of legacy markets

Investable Themes in Decentralized Finance

BANKING, LENDING, PAYMENTS	WEALTH & ASSET MANAGEMENT	CAPITAL MARKETS	INSURANCE
<p>PAYMENTS</p> <p><u>REMITTANCES</u></p> <ul style="list-style-type: none"> •Cross-border; cut fees; consumers can send money the way they send data over the Internet <p><u>BANK TO BANK; B2B</u></p> <ul style="list-style-type: none"> •No borders or intermediaries; lower cost; re-platform ACH or SWIFT <p><u>MICROPAYMENTS</u></p> <ul style="list-style-type: none"> •Off-chain with net on-chain settlement; machine to machine payments or per view purchases for content <p><u>STABLE COINS</u></p> <ul style="list-style-type: none"> •Digital, collateralized representations of a dollar on blockchain <p>LENDING</p> <p><u>CRYPTO BACKED</u></p> <ul style="list-style-type: none"> •Smart contract based lending with digital assets serving as the collateral <p><u>SUPPLY CHAIN</u></p> <ul style="list-style-type: none"> •Supply chain finance and tracking <p>BANKING</p> <ul style="list-style-type: none"> •Full-stack neo banks built on crypto rails with an EM focus •ATMs and consumer off / on-ramps 	<p>CUSTODY</p> <ul style="list-style-type: none"> •Institutional grade solutions to store and retrieve digital assets; likely married with insurance <p>IDENTITY AND DATA</p> <ul style="list-style-type: none"> •Identity: Identification confirmed through third party - stored and shared at user's choice •Data ownership: Customer protection, data ownership, and monetization of financial data <p>INVESTING & INDEXING</p> <ul style="list-style-type: none"> •Platforms that allow users to select projects (discovery for crypto, or robo advisor) or create and manage baskets of crypto assets <p>TOKENIZATION PLATFORMS</p> <p><u>ORIGINATION</u></p> <ul style="list-style-type: none"> •Digitization of assets from commercial real estate to PE funds <p><u>SECONDARY</u></p> <ul style="list-style-type: none"> •Trading venues and liquidity networks related to STOs (security token offerings) <p><u>FULL STACK</u></p> <ul style="list-style-type: none"> •Full stack solutions that do both origination and secondary trading 	<p>PREDICTION MARKETS</p> <ul style="list-style-type: none"> •Smart contract automation and decentralized oracles <p>DERIVATIVES</p> <ul style="list-style-type: none"> •Smart contract automation; transparency; real-time margining <p>TRADE DATA & EXECUTION</p> <ul style="list-style-type: none"> •OMS / EMS, reference prices, inter-exchange connectivity, smart routing <p>TRADING VENUES</p> <ul style="list-style-type: none"> •Buy or sell cryptocurrencies or utility tokens <p>PROJECT & CHAIN DATA</p> <ul style="list-style-type: none"> •Project data: total token supply, inflation schedule, founder lock-ups & checks •FV: determine FV from on-chain TXs, rewards, and developer activity <p>ASSET EXCHANGE</p> <ul style="list-style-type: none"> •STO and utility token compliant liquidity pools and exchange <p>PRIVACY</p> <ul style="list-style-type: none"> •Zero knowledge protocols to enable private transactions and protect sensitive data <p>POST-TRADE SETTLEMENT</p> <ul style="list-style-type: none"> •Reduce settlement times and costs; eliminate much of middle and back offices at banks 	<p>PARAMETRIC</p> <ul style="list-style-type: none"> •70% of catastrophic loss (\$1.3tn) not covered; ability to create trustless, automated policies and claims payouts via smart contracts <p>STRUCTURE</p> <ul style="list-style-type: none"> •Open community or mutual insurance; surplus goes back to the pool <p>SECONDARY TRADING</p> <ul style="list-style-type: none"> •More seamless risk transfer; greater liquidity / marketplace provides fairer price for risk <p>TRADITIONAL CARRIERS / BROKERS / REINSURERS</p> <ul style="list-style-type: none"> •Lower paperwork and reconciliation costs; reduce fraud; easier sharing of risk or real-time sharing of risk books

Real Time Settlement

Tokenization means settlement in traditional markets goes from several business days to real time, eliminating counterparty credit risk & operational expenses, increasing market liquidity, and potentially eliminating the need for hedging when engaging in cross-border transactions. A recent study by Plutoneo estimates that €1.4T worth of European assets are expected to be tokenized by 2024.¹²

Greater Transparency & Documented Ownership

A migration to tokenized securities means greater transparency in legacy markets. A token owner's rights and legal responsibilities would be embedded into the token and an immutable record of ownership would exist on the underlying blockchain. The combination of an immutable record and real time settlement would require short sellers to actually borrow securities before selling short, avoiding the over-shorted situation of Gamestop and the possibility of steep losses.

Greater Liquidity

Tokenizing assets means fractional ownership is possible and assets can easily be traded in a secondary market. This could mean greater market participation and liquidity.

Greater Efficiency

Tokens representing an asset would be embedded with all the necessary info for validating and transferring ownership, recorded in real time on an immutable blockchain. This means costly and sluggish back-office operations could be eliminated, which would not only reduce industry expenses but also make processing and validating asset transfers more efficient.

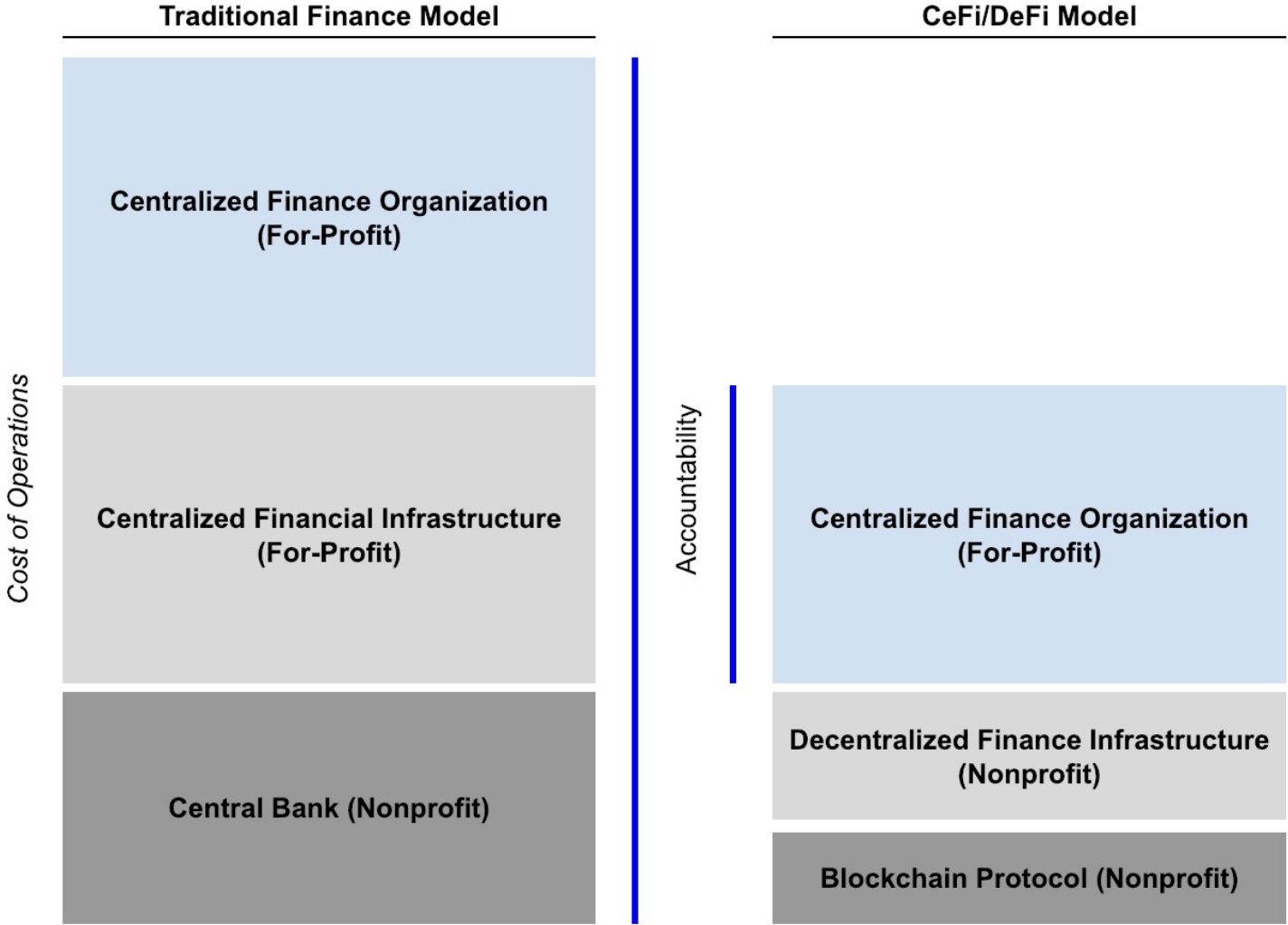
Autonomous Capital Management

Tokenized assets can have dividend payments, time revenue share pay-outs, vesting periods, and lock-ups embedded in the token and executed autonomously, saving both time and money for market participants and asset issuers.

New Markets

Tokenization means assets that couldn't otherwise be sold in the open public due to size or other factors that don't meet exchange listing requirements, are now marketable to market participants. This would open up new markets and allow for greater portfolio diversification.

All this while reducing the cost of financial services

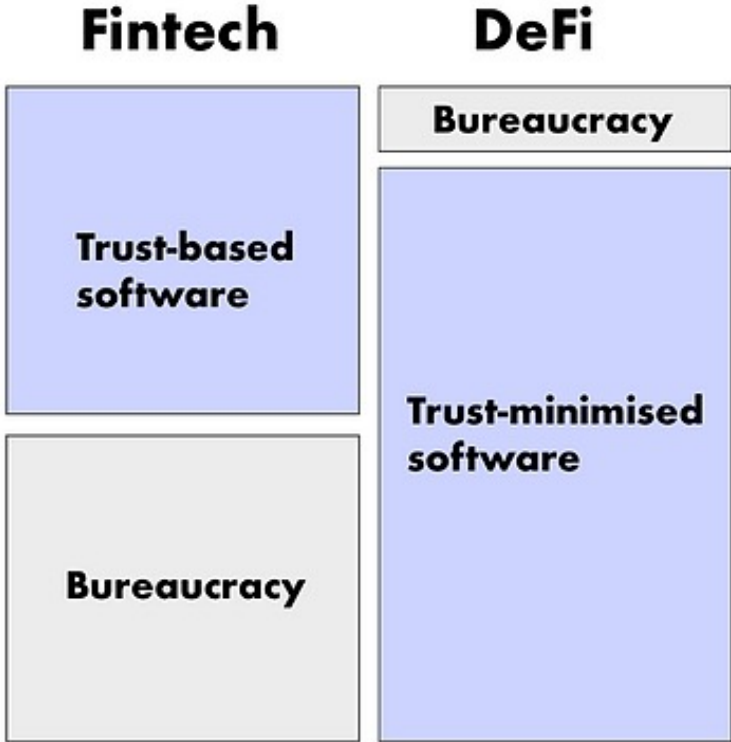


But while the fintech movement aims to reduce costs as well, DeFi is also focused on reducing bureaucracy with a major focus on decentralisation

	Traditional finance	Fintech	DeFi
Issuance of money	The State	The State	Proof of Work & Proof of Stake blockchains
Locus of trust	Government through the legal system	Companies	Ethereum Virtual Machine (smart contracts)
Transfer of money	ACH, wire transfer, cash	Digital transfer	Cryptocurrency and token transactions
Equity	Shares	Digital & fractional shares	Tokens
Money market	Short-term debt e.g. treasury bills	N/A	Compound · Aave · Maker
Primary market	IPOs	IPOs	ICOs/IEOs/Uniswap listings
Secondary market	Exchanges like NASDAQ	Robinhood	Uniswap · 0x · Kyber

ZERION

FinTechs are currently much better with UX/UI



Fintech is rooted in bureaucracy and trust, DeFi is free and trust minimised.

In brief, decentralised finance, or DeFi (pronounced as *defy*), is about replacing centralised, traditional finance with distributed, P2P finance

Laying the Foundations



Channels



13
SEP

Thursday, September 13, 2018

BUIDLing DeFi -- Workshop with Abacus, Dharma, and Set



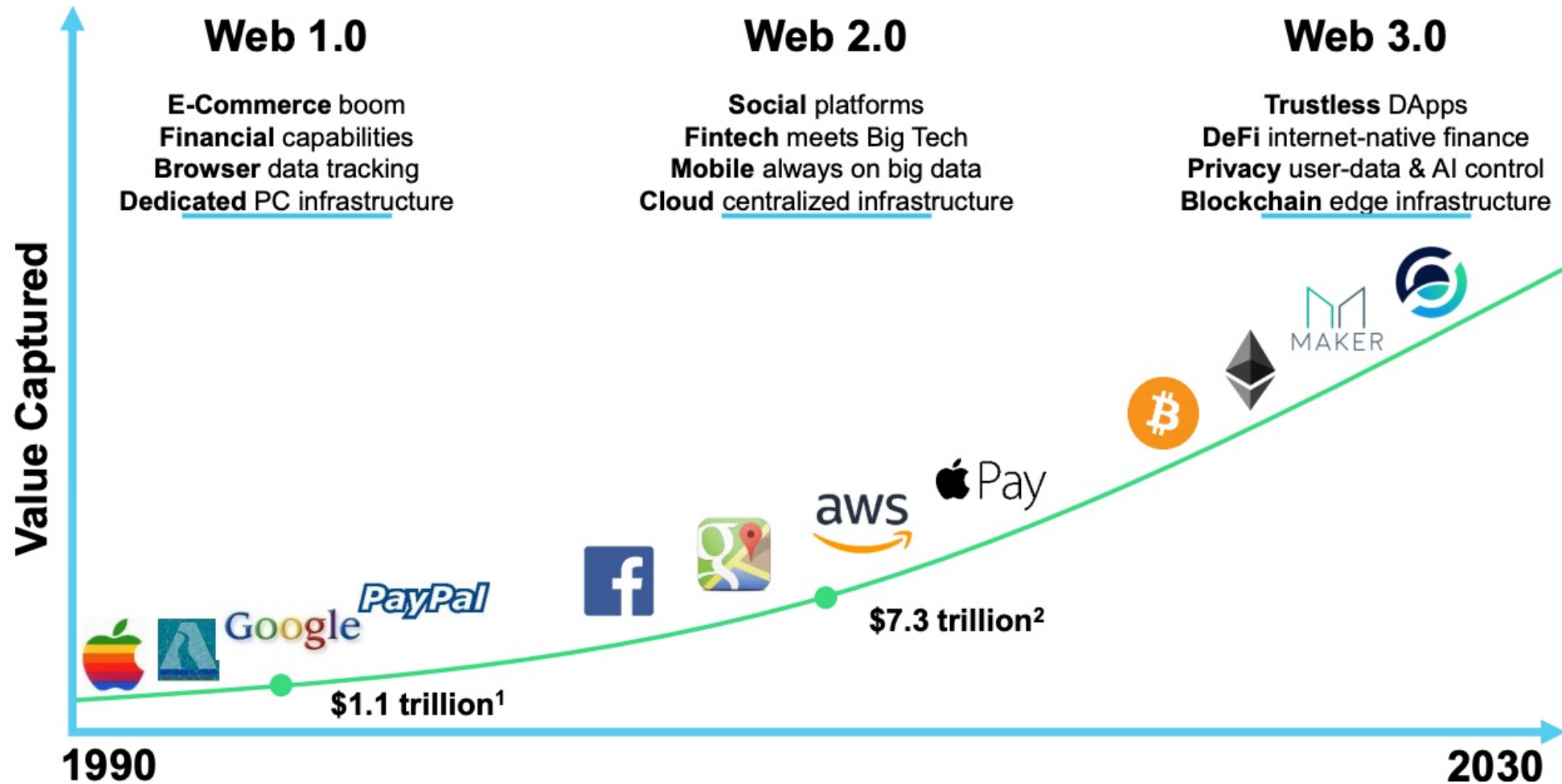
Hosted by Inje and 2 others
From DeFi - Decentralized Finance Workshops, SF
Public group

Details

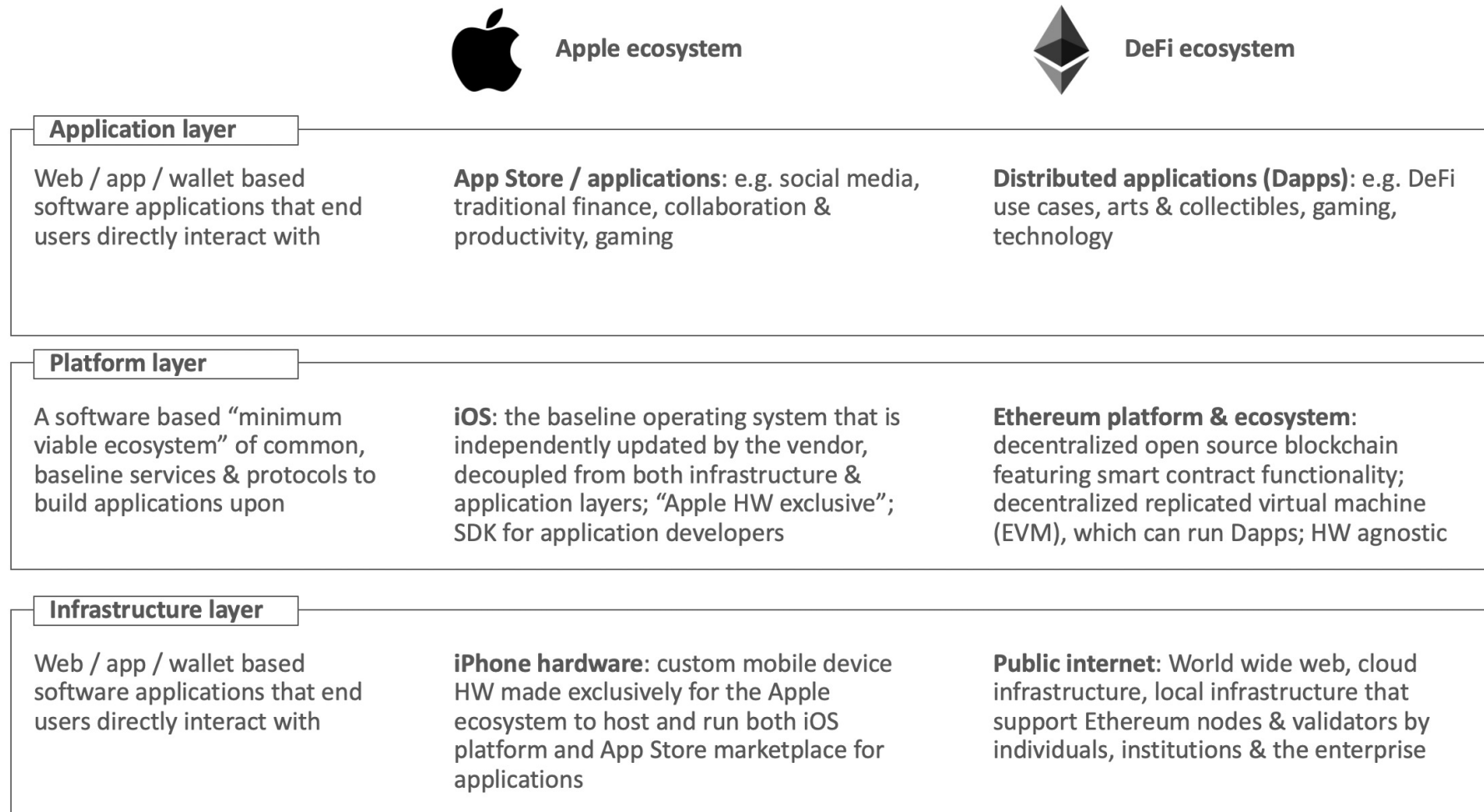
#DeFi is a community for intrepid developers, entrepreneurs, and enthusiasts of Decentralized Finance.

In this inaugural #DeFi meetup, we'll discuss what #DeFi is, do short deep dives into Abacus, Dharma, and Set, and then start building.

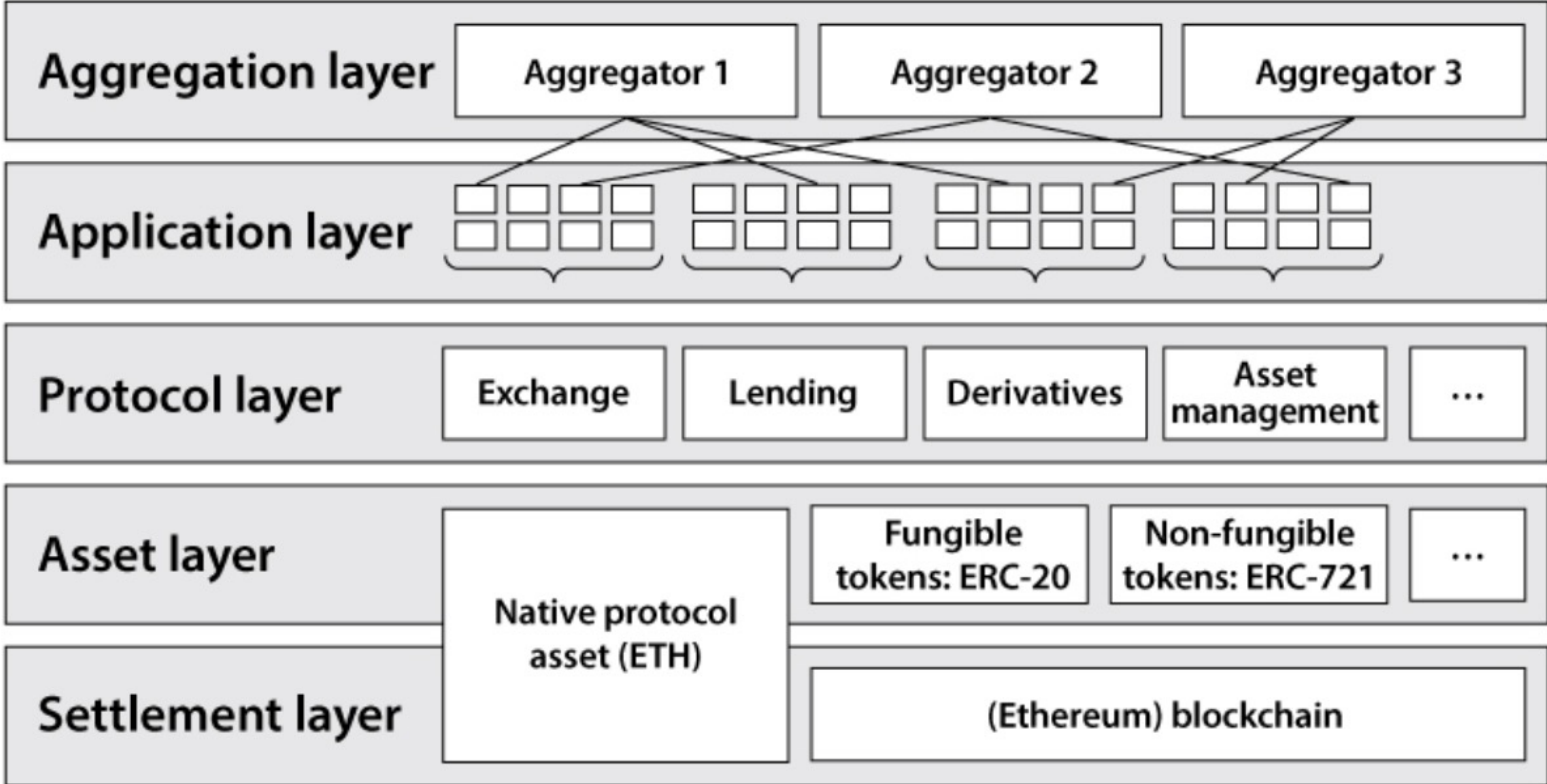
If we are to recap what DeFi is from another angle, we can say decentralised finance aims to power the next generation of the internet



In a final analogy, DeFi builds on top of key infrastructure and popular blockchain platforms to provide applications to users, like iPhone apps

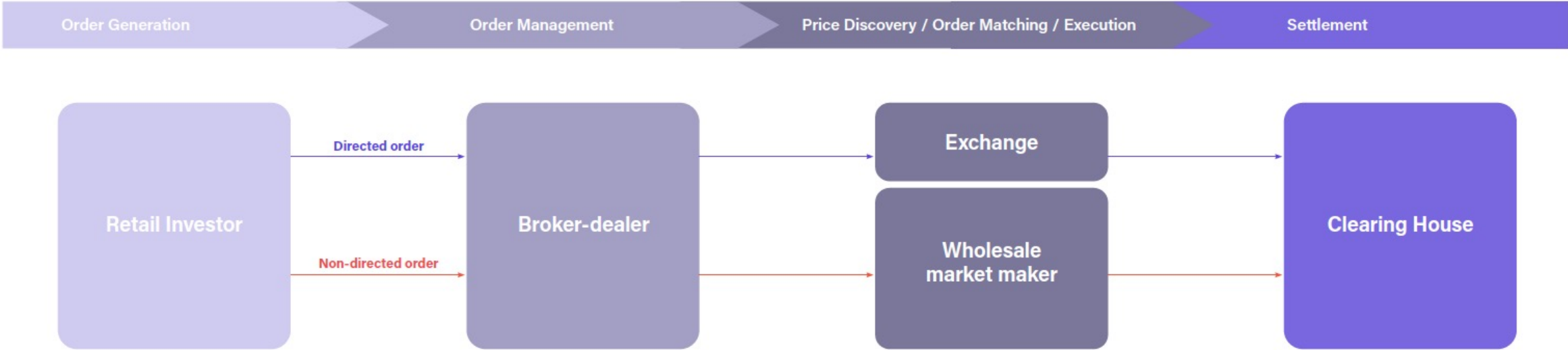


Now, let's look at a key interface to decentralised finance: decentralised exchanges, also known as DEXs



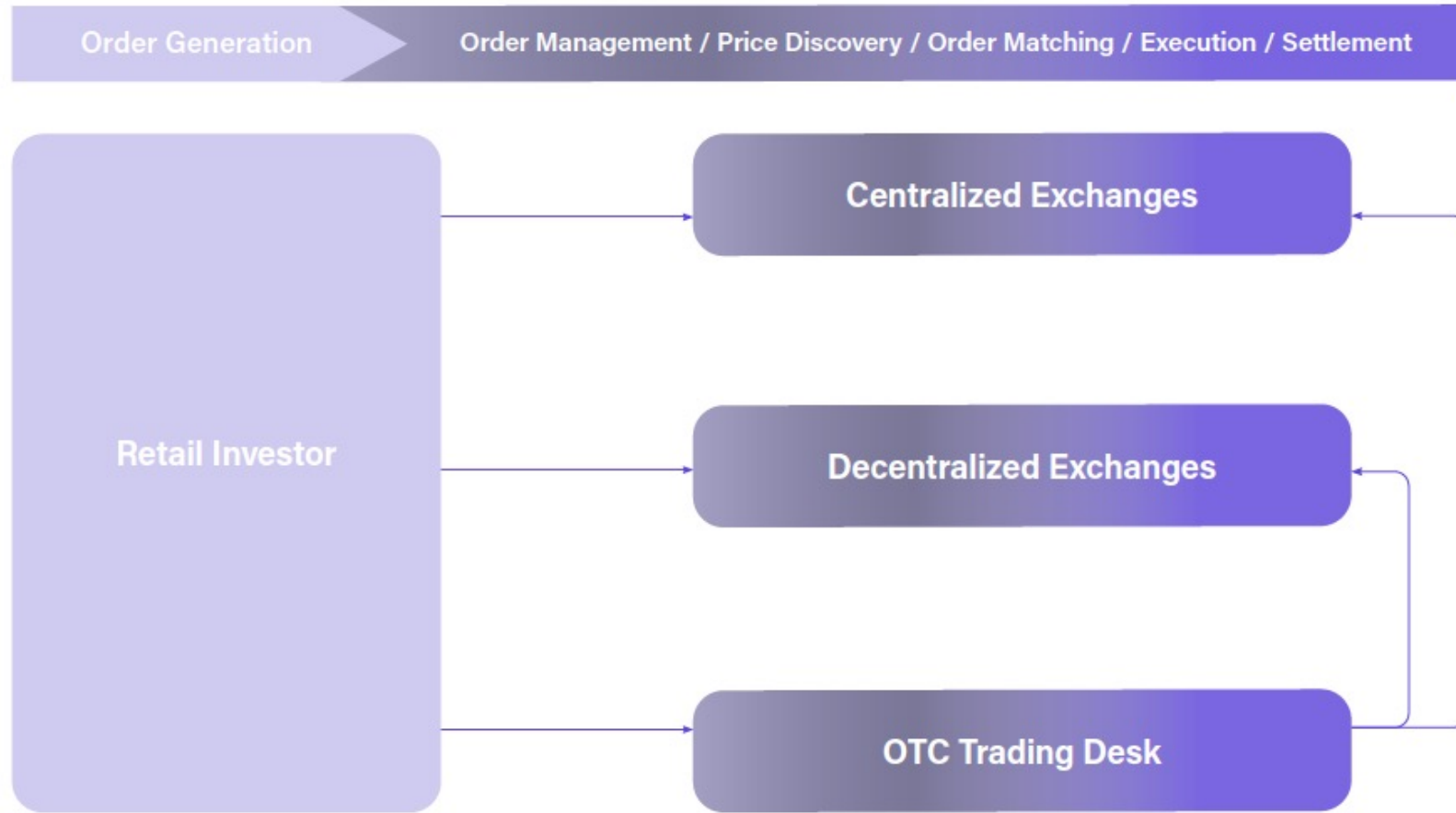
Naturally, DeFi doesn't share traditional finance's reliance on multiple intermediaries

Order flow in traditional markets

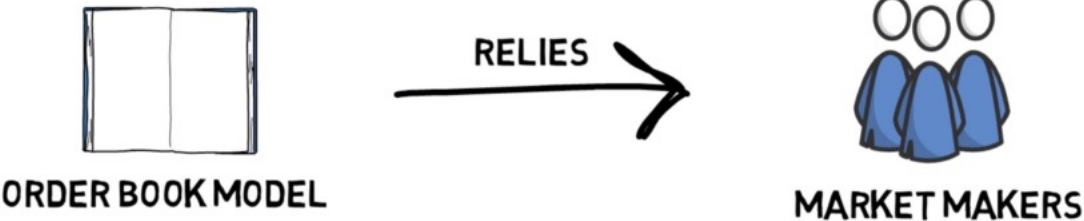


Nor does DeFi share the mainstream cryptosphere's dependence on centralised exchanges or OTC trading desks

Order flow in crypto markets



Alas, while DeFi was initially reliant on order books for on-chain trading, now most DEXs have relinquished that traditional pricing mechanism



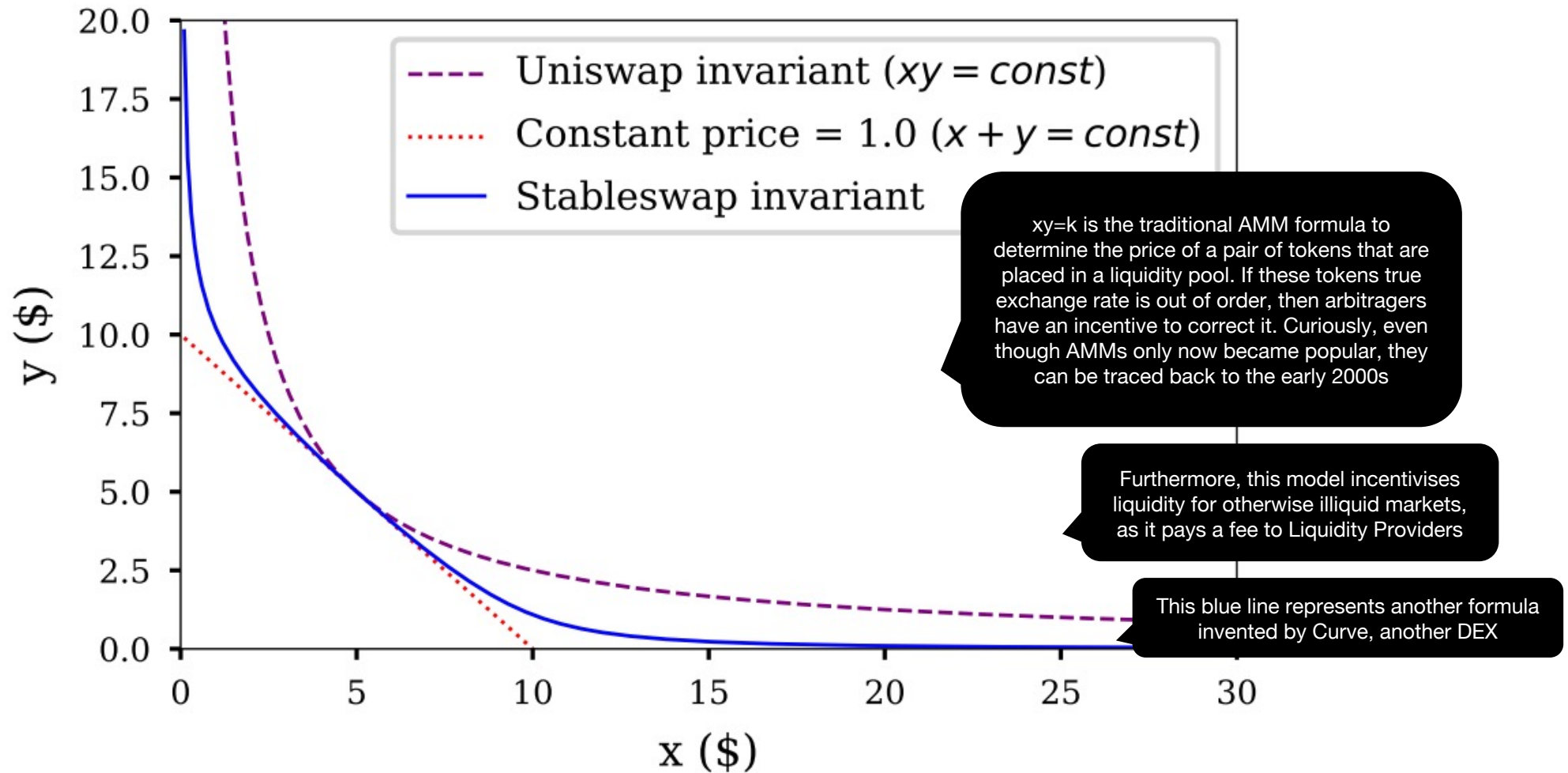
Because decentralised order books would require decentralised market makers to trade on-chain, which can be slow and expensive

Most Popular Decentralized Exchange Protocols

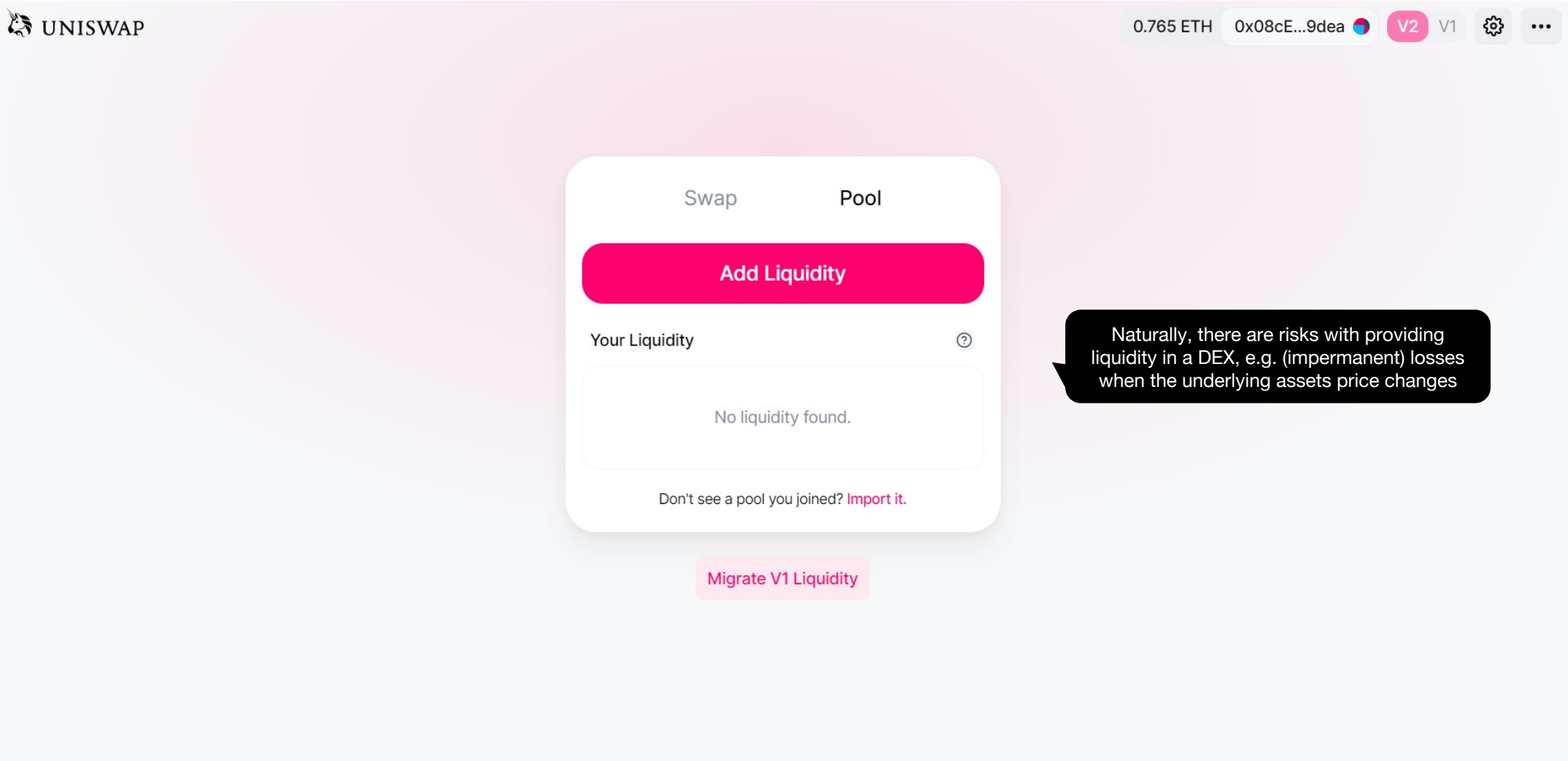
Protocol name	Protocol type	Price discovery
0x	Exchange	Off-chain order books
(Air)Swap	P2P / OTC	P2P negotiation
Bancor	CFMM	Smart contract
Balancer	CFMM	Smart contract
Curve	CFMM	Smart contract
Kyber Network	Reserve aggregator	Proposal by maker
UniSwap	CFMM	Smart contract

NOTE: CFMM, constant function market maker.

Instead, the cornerstone of decentralised trading are Automated Market Making algorithms – which power liquidity pool exchanges, like Uniswap



It may look complex, but providing liquidity is just a couple of buttons away. So many investors started doing it to earn a cut of a DEX's fees

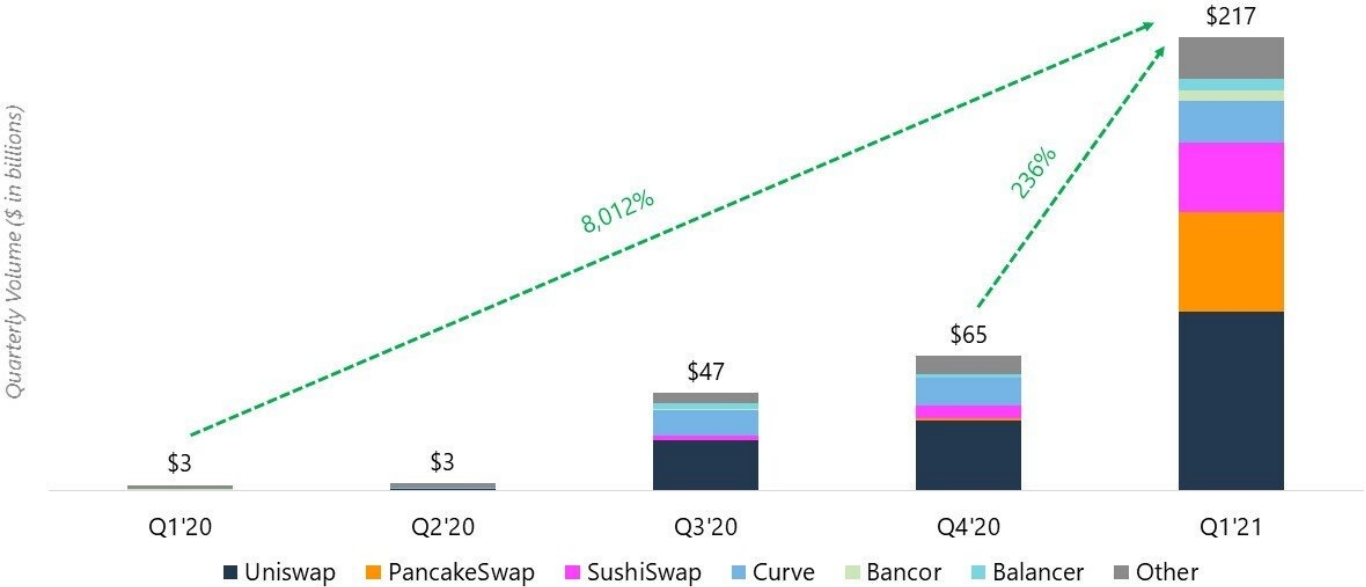


This convenience has prompted DEXs to grow rapidly, as developers, investors, and users explore new use cases for online value exchanges



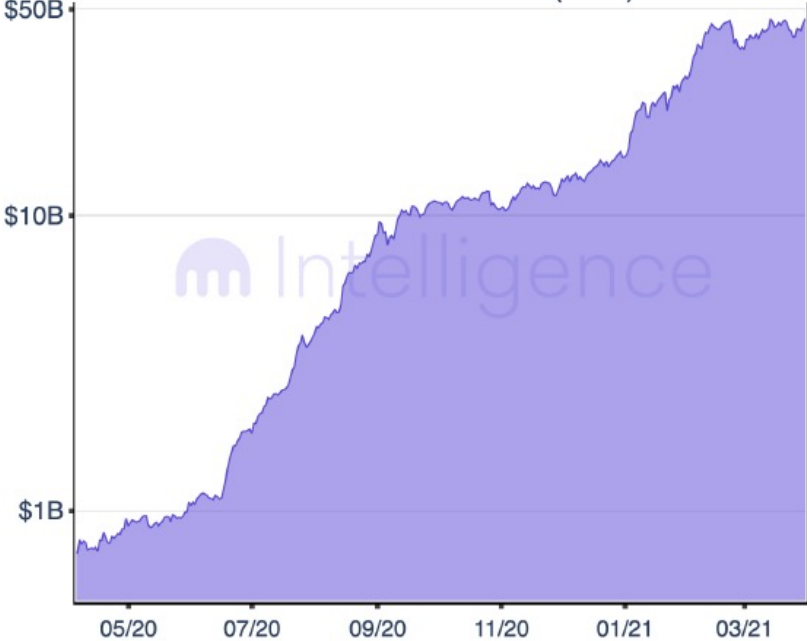
Quarterly DEX Volume

DEX volumes continue to soar as they eat into centralized exchanges share and the bull market heats up



Data as of: Apr. 1 2021
 Source: Messari, Dune Analytics, Coingecko

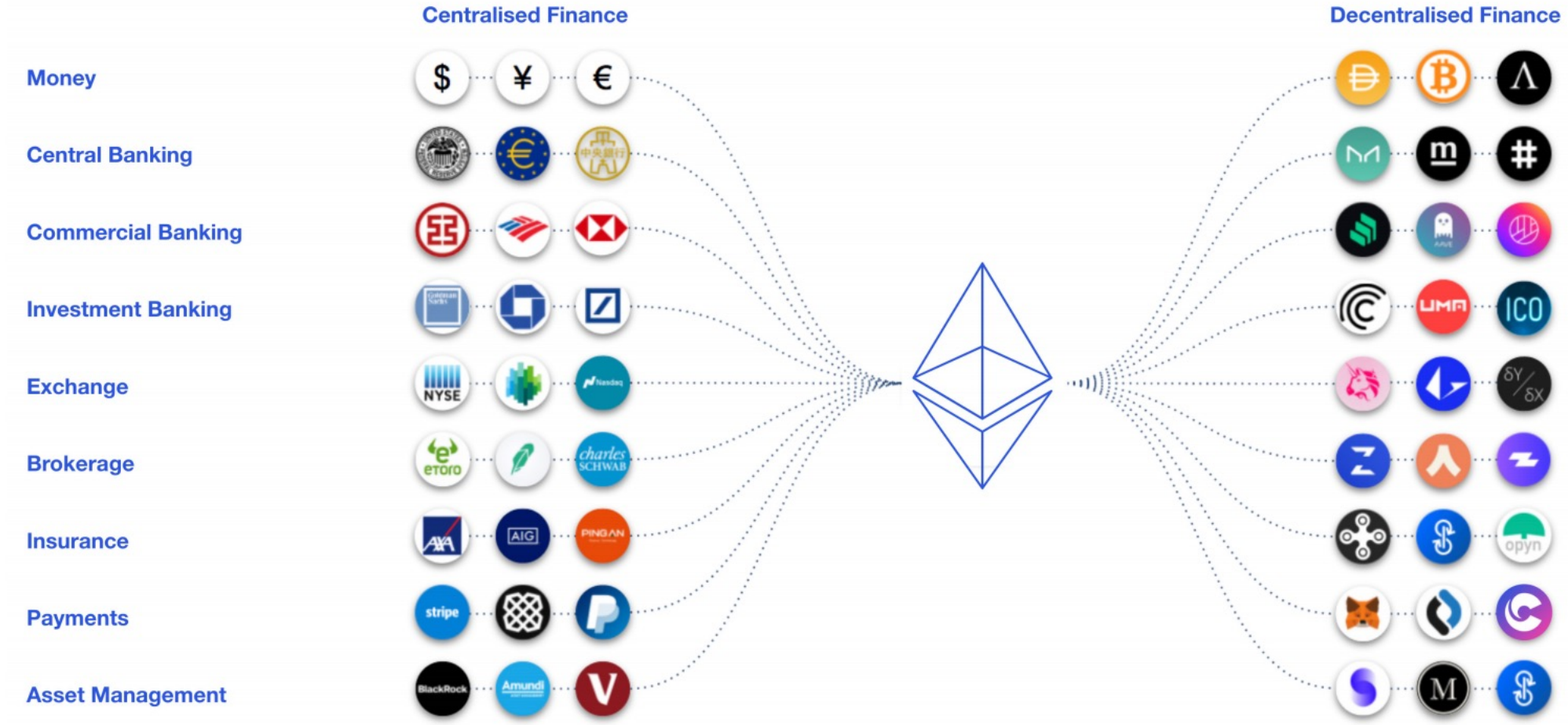
DeFi Total Value Locked (USD)



These use cases replicate TradFi applications in a decentralised manner: trade (or speculate), borrow for leverage and lend to generate yield

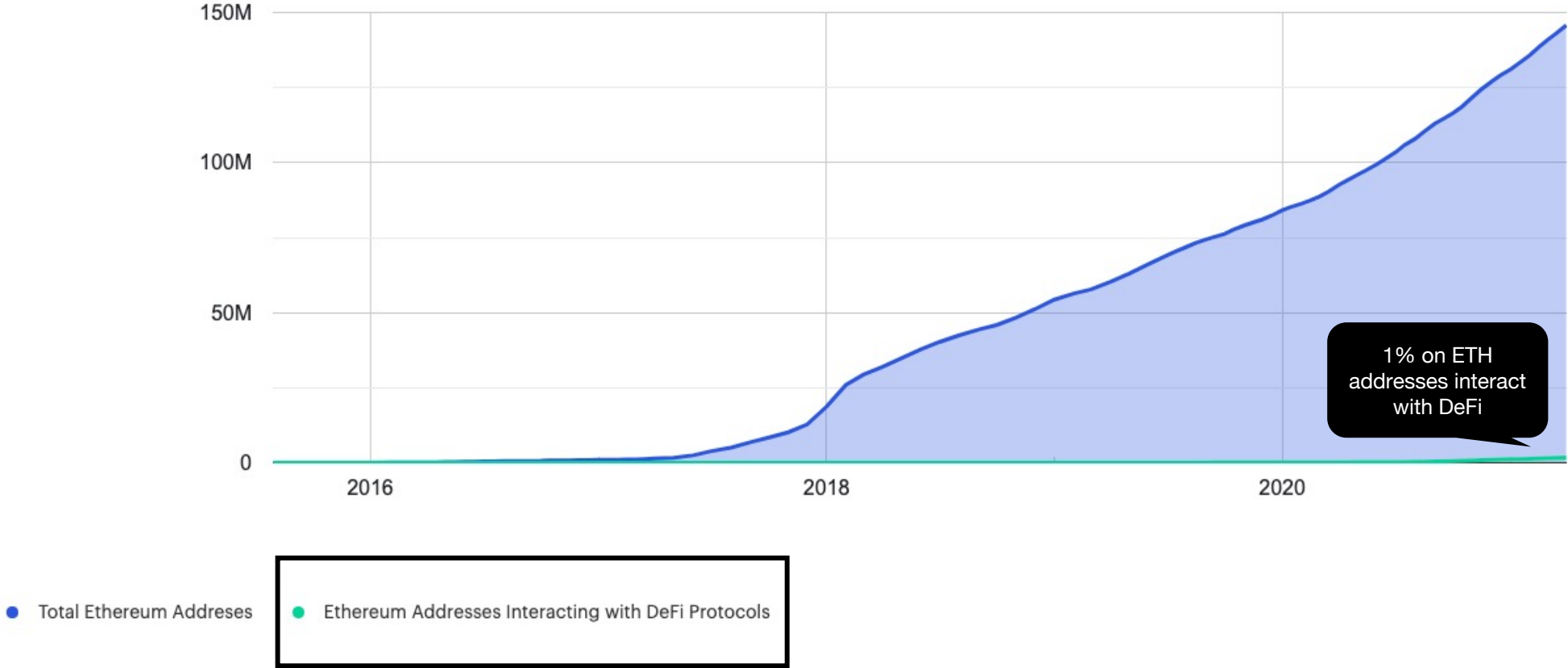


Overall, if you can think of an existing TradFi institution, there's likely a DeFi equivalent under development or even fully operational

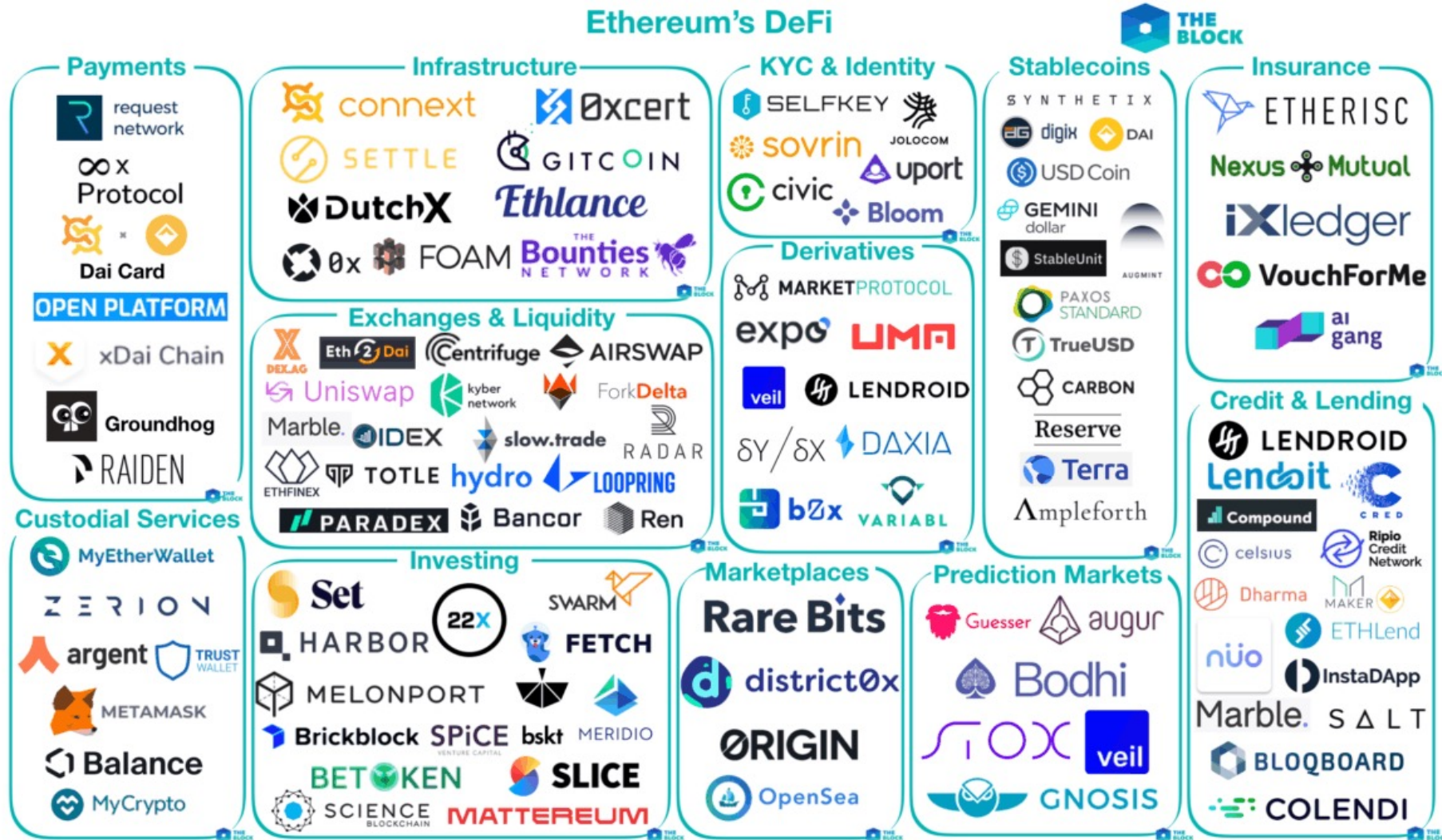


Still, this growth only represents a small fraction of blockchain users, even considering the most popular ecosystems, such as Ethereum

Ethereum Addresses Interacting with Defi Protocols



All-in-all, the DeFi space is growing exponentially with new devs and users contributing towards this open, global financial system



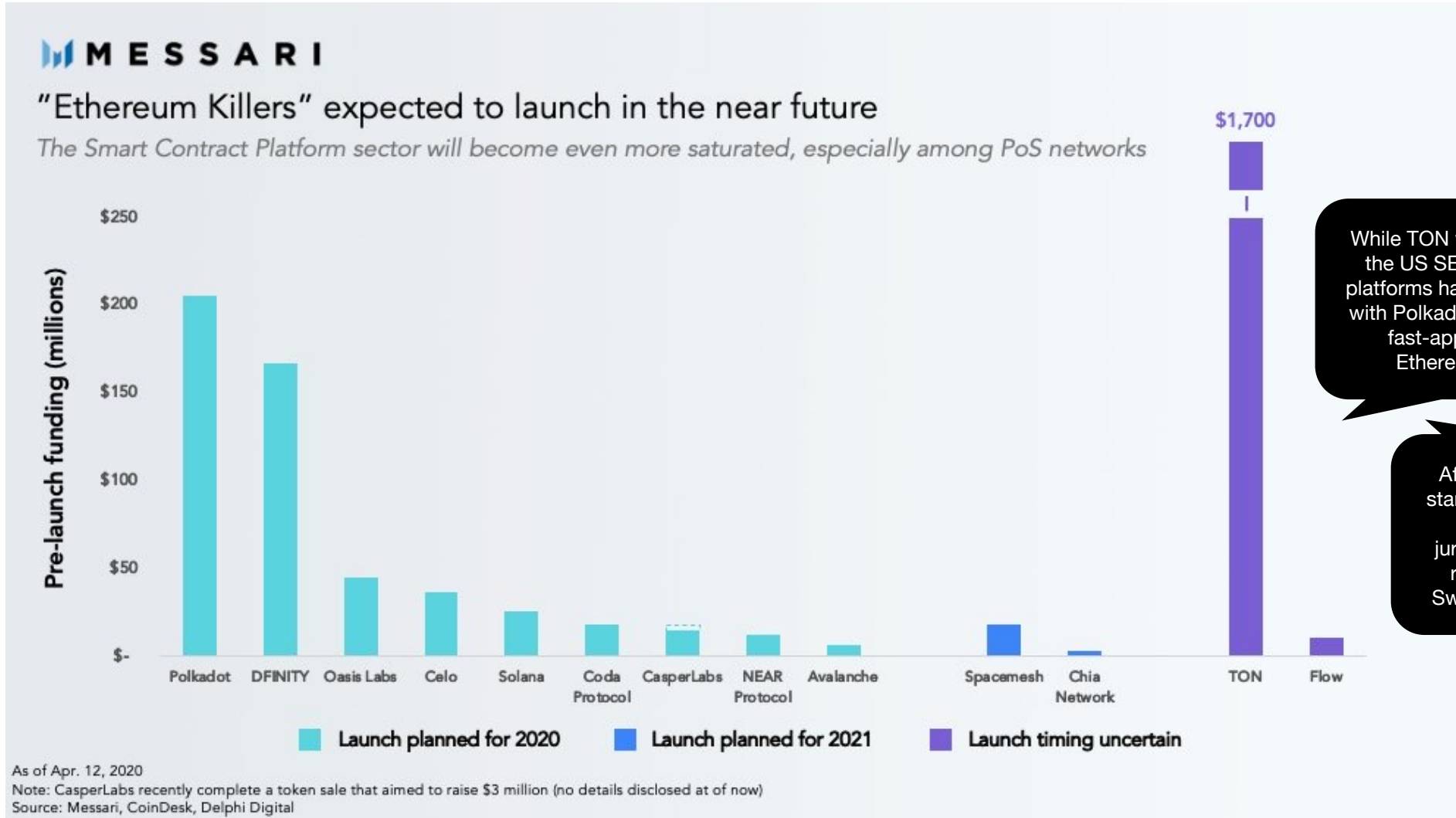
Naturally, not all these projects are aiming to capitalise on the bright side of smart contracts. Many are just riding the current bull cycle's narrative

2021 Outlook: 20 Reasons We're Remaining Bullish

We see several reasons to remain bullish on crypto during 2021

#	Category	Factor	Explanation
1	Bitcoin Cycle	Price	Fourth bull market cycle uptrend
2		Technical	Bitcoin above 200 DMA = bullish
3		Valuation	Valuations higher but not a bubble
4		Fundamentals	Increasing economic model estimates
5	Macro Trends	Monetary	Money supply growth & dry powder
6		USD trend	Expect dollar weakening & EM strength
7		Credit trend	Low rates & negative yielding debt
8		Equities trend	Strong S&P 500 & EM equity trend
9		Fiscal policy	Government stimulus expected
10		Geopolitical	Tension domestic & abroad
11		T.I.N.A.	There Is No Alternative
12	Capital Flows	Asset Class Size	Now large enough for institutions
13		Institutional interest	Crypto fund starts & AUM growing
14		Exchange traded fund flows	GBTC generated \$3B Q4 demand
15		Retail crypto on-ramp demand	PayPal & Coinbase demand surging
16		Corporate crypto buyers	Treasury & fundamental usage reasons
17		Consensus to bearish	Market pricing 10% chance BTC>\$100k
18	Coinbase equity IPO	Equity investors will be looking at crypto	
19	Institutional FOMO	Underperformance risk (Tesla)	
20	Regulatory	More clarity=lower discount rate	

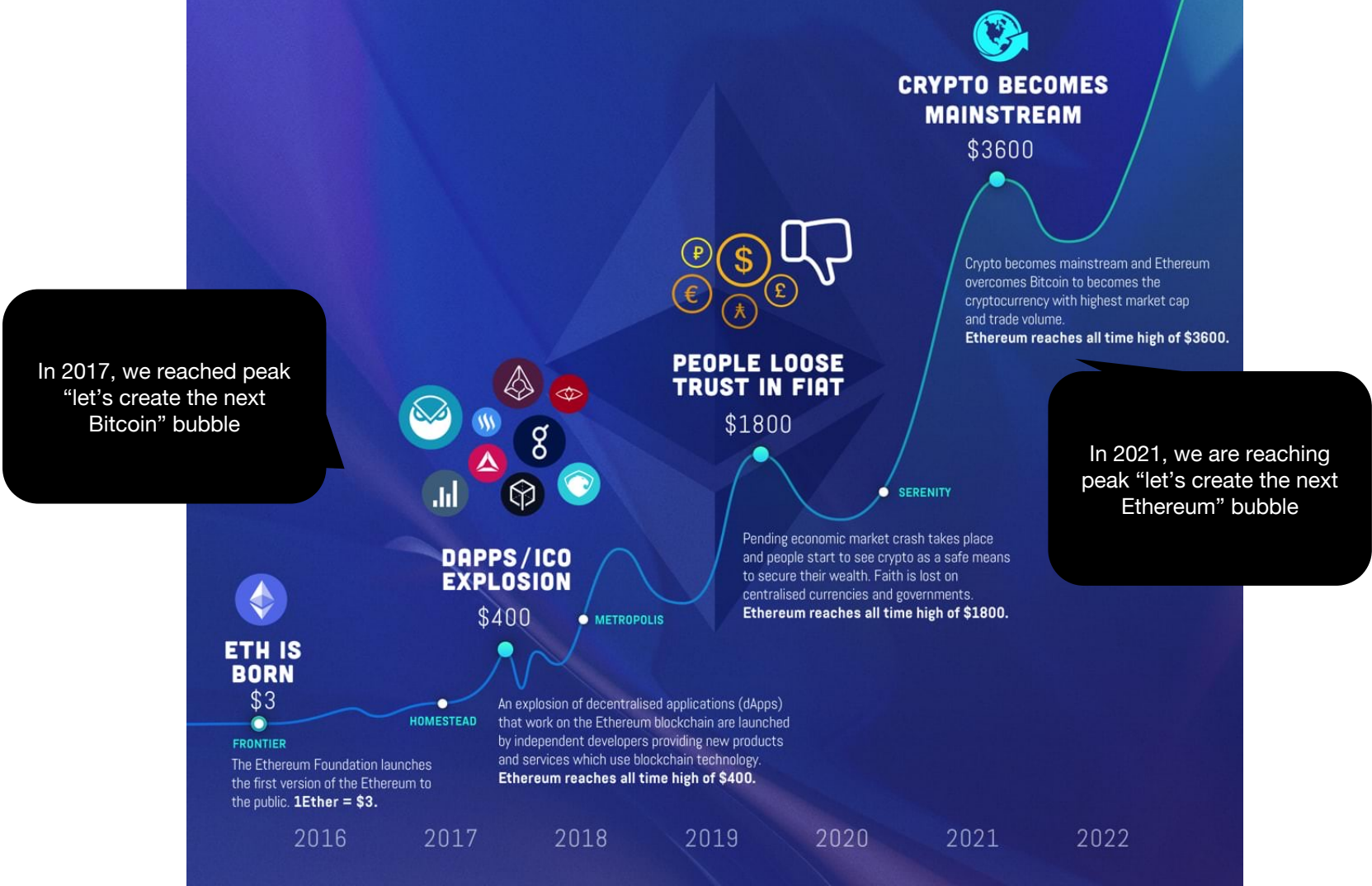
These new capital flows contribute to the fact Ethereum is not the only blockchain building the future of finance, as new projects are easily funded



Which brings us to conclude with

4. Some key DeFi projects

A primer on the ecosystem wars: recapping things so far, it all started when Ethereum was created with the vision of replacing Bitcoin



These “Ethereum killers” are all focused on being “Faster, Higher, Stronger” than the original smart contracts enabler

Polkadot

- Launched in 2020
- Nominated Proof of Stake
- Interoperable and scalable

Binance Smart Chain

- Launched in 2020
- Proof of Staked Authority
- Ethereum compatibility






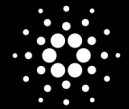

Solana

- Launched in 2020
- Delegated Proof of Stake
- Focus on high speed

Tezos

- Launched in 2017 (kind of)
- Liquid Proof of Stake
- Focus on governance

For example, Solana prizes itself for its high transaction speed, focused on building apps for the many. But Ethereum is also working on its scaling

by  SolMates	 Solana	 Ethereum	 Binance Smart Chain	 Polkadot	 Cardano	 Tron
Transaction per second	65,000	15	100	1000	270	1,000
Avg. Fee Per Transaction	\$0.0015	\$15	\$0.01	\$1	\$0.25	free
Transaction latency	0.4 sec	~5 min	75 sec	2 min	10 min	3 sec
Number of Validators	702	11,000+	21	297	2,376	27
Total Transactions to date	15 Billion	1.07 Billion	227 Million	1.7 Million	5.9 Million	1.7 Billion

Ethereum will transition to a Proof-of-Stake consensus algorithm sometime next year, which will improve speed and mitigate environmental criticism

(even though it's not true that Bitcoin mining wastes energy, as it mostly uses nonrival, renewable electricity)

Ethereum also derives most of its strengths from the multiple projects created on top of its protocol, especially within the DeFi sector

Lending

AAVE

- Open-source and non-custodial protocol to earn interest on deposits & borrow assets

MAKER

- Decentralized credit platform on Ethereum that supports Dai, a stablecoin whose value is pegged to USD and backed by digital assets as collateral

Compound

- Open-source money market protocol on Ethereum that lets users lend or borrow assets against collateral

Trading

UNISWAP

- Fully decentralized on-chain protocol for token exchanges on Ethereum that uses liquidity pools instead of order books

SYNTHETIX

- Decentralized platform on Ethereum for the creation of Synths: on-chain synthetic assets that track the value of real-world assets

UMA

- Decentralized protocol to enable the creation, maintenance, and settlement of financial contracts for any underlying assets

Interfaces / Infra

0x

- Protocol for P2P exchange of tokenized assets

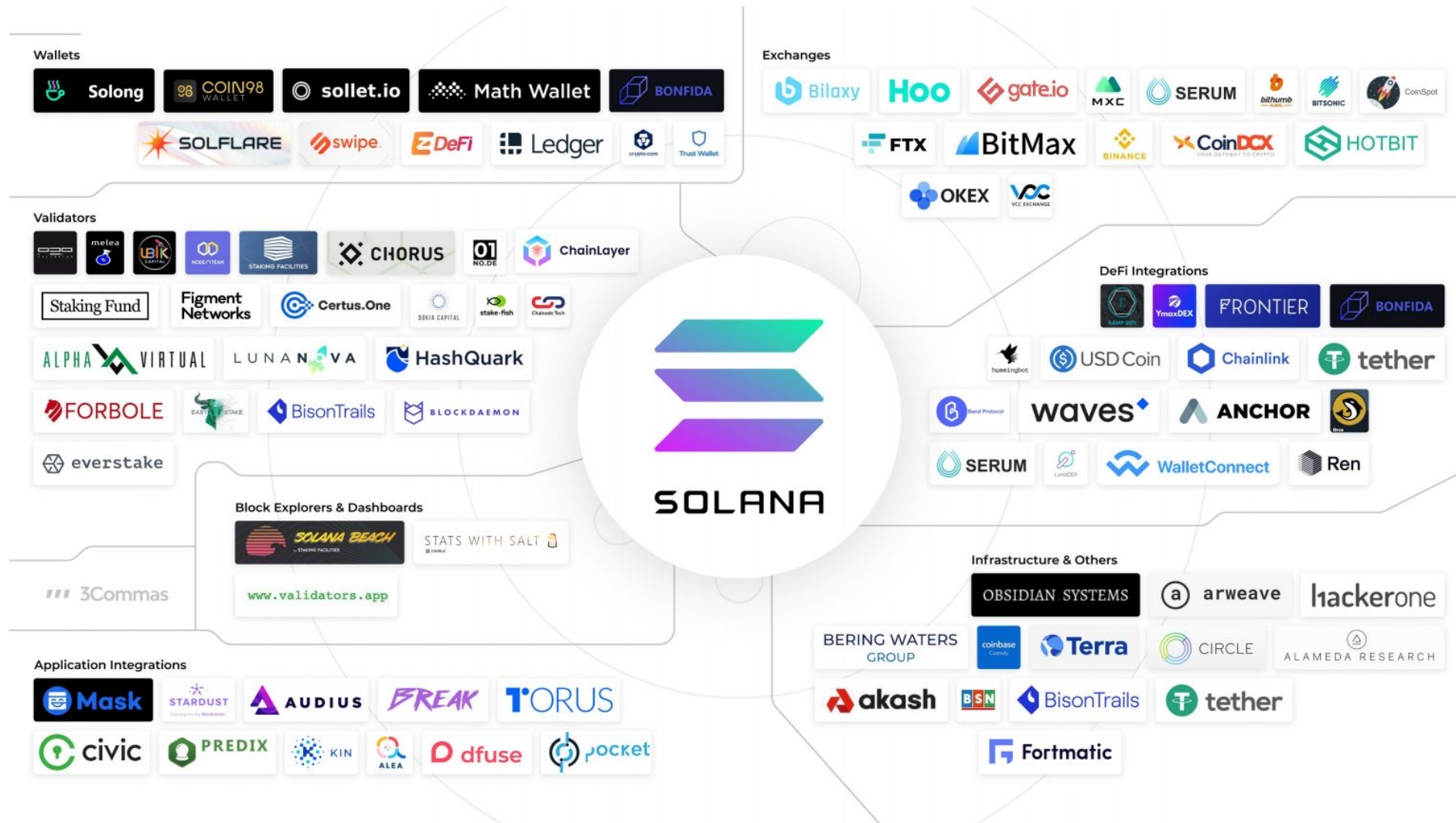
LOOPRING

- Open-source protocol for DEXs designed to provide matching-as-a-service

YEARN FINANCE NETWORK

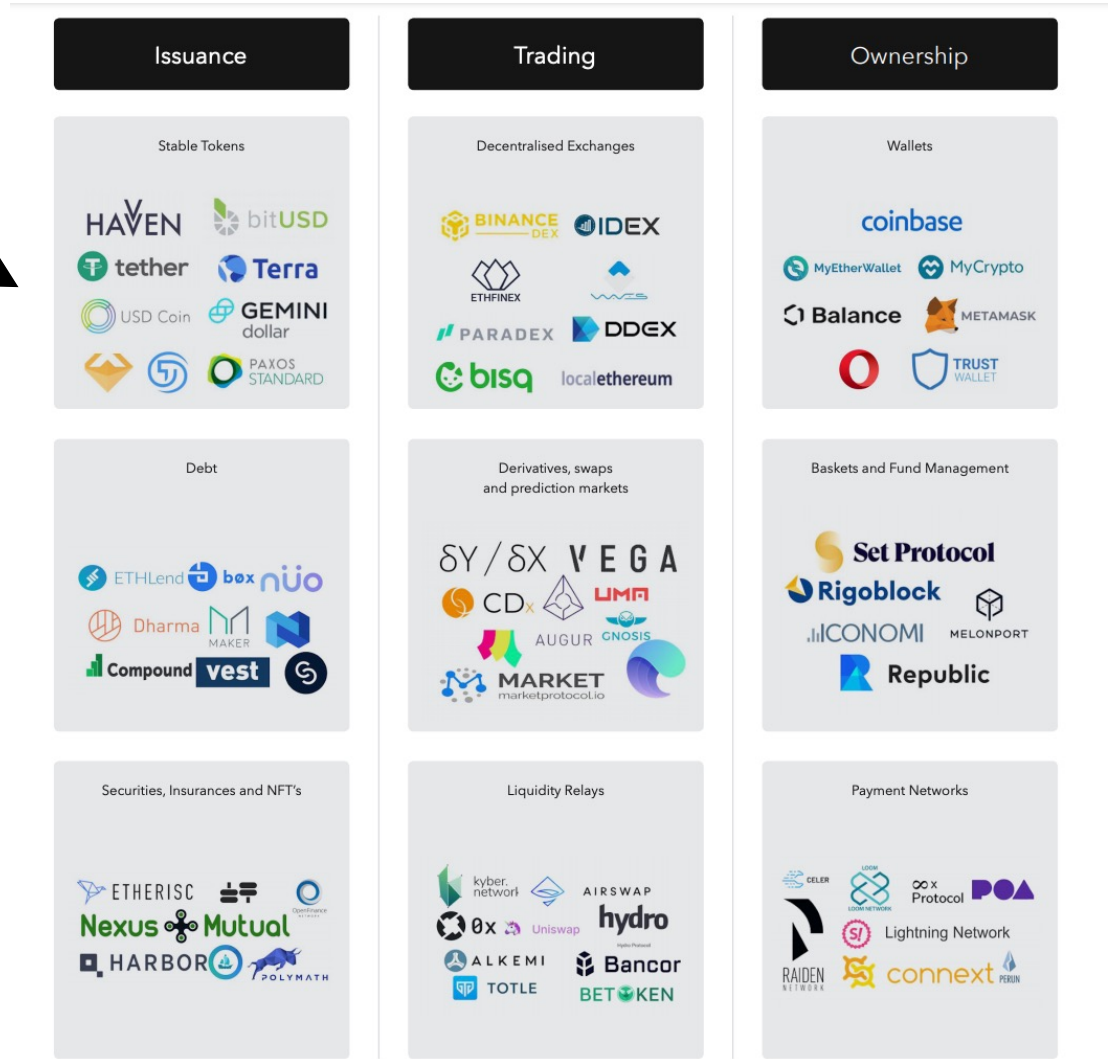
- Aggregator of community-led yield farming vaults, easy swapping tools and pooled insurance coverage

But, using Solana's example, more projects have been able to attract enough talent to start building potentially equivalent ecosystems

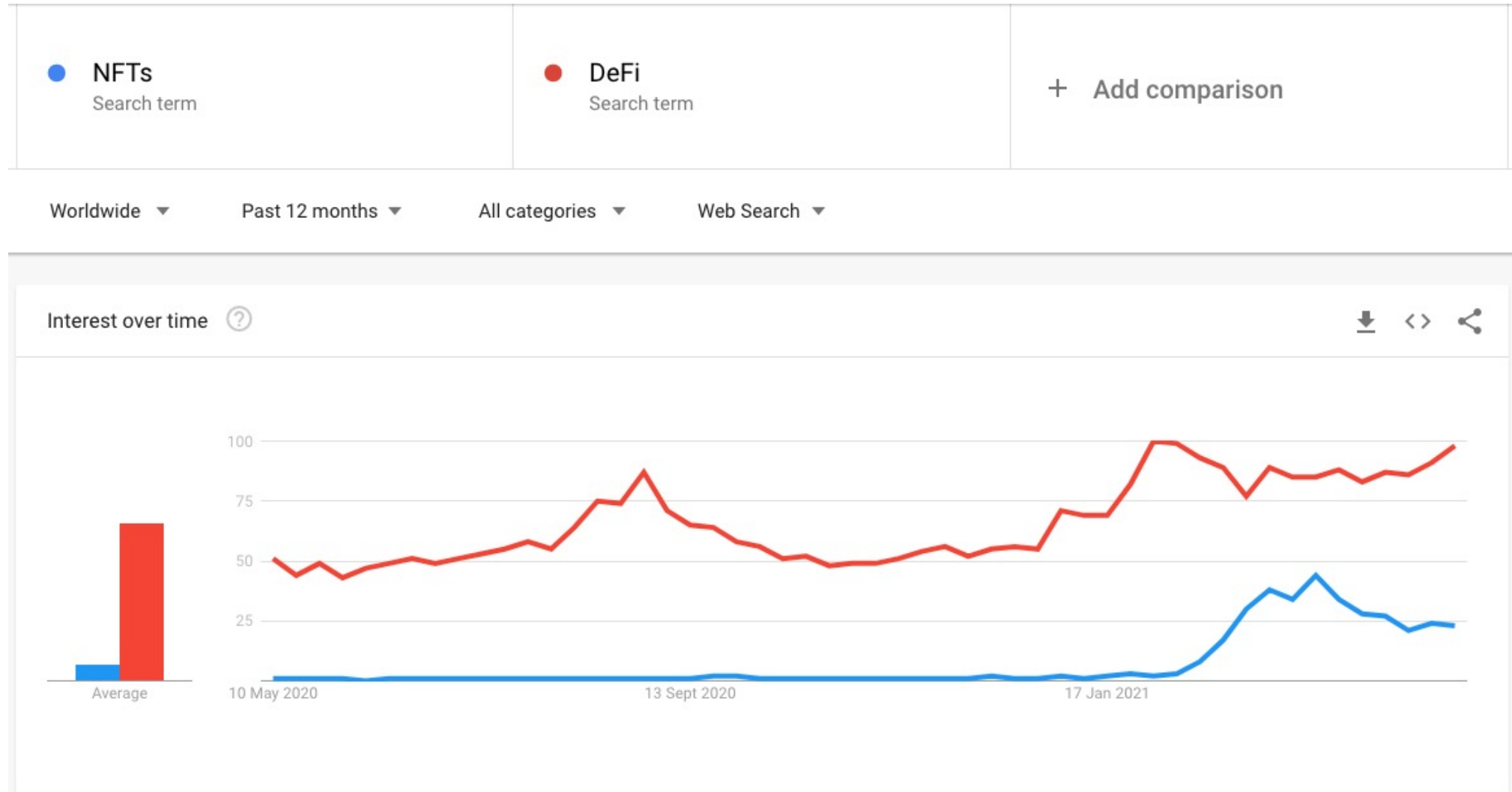


Overall, from a user's perspective, there are many alternatives they can choose from to meet their decentralised finance goals

Tether is not DeFi per se, but it's part of the larger ecosystem



Lastly, it seems the Non-Fungible Tokens hype, tangentially connected to DeFi, is fading a bit. But remember “every artist was first an amateur”!



Coffee?

Today's agenda

- 14h - 16h Smart contracts and blockchain
- 16h - 16h30 Coffee-break
- 16h30 - 17h30 **Case-study: Fostering consumer bargaining and e-procurement through a decentralised marketplace**
With Carnegie-Mellon University
- 17h - 18h Governance and regulatory issues of cryptos and DeFis: challenges and opportunities

Today's agenda

- 14h - 16h Smart contracts and blockchain
- 16h - 16h30 Coffee-break
- 16h30 - 17h30 Case-study: Fostering consumer bargaining and e-procurement through a decentralised marketplace

- 17h - 18h

Governance and regulatory issues of cryptos and DeFis: challenges and opportunities

Ian Gauci