Blockchain : The future of money

burnmark

@Sanjeevk_k

How Old is the Concept of Blockchain?

Blockchain Story: How Old is the Idea?

Blockchain Story: Example 1 (stone money)

Blockchain Story: Example 2 (Warehouse)

Cryptocurrency and Money Functions

- Three most important functions that money played are **medium of exchange, unit of account and store of value**
- **Medium of exchange**

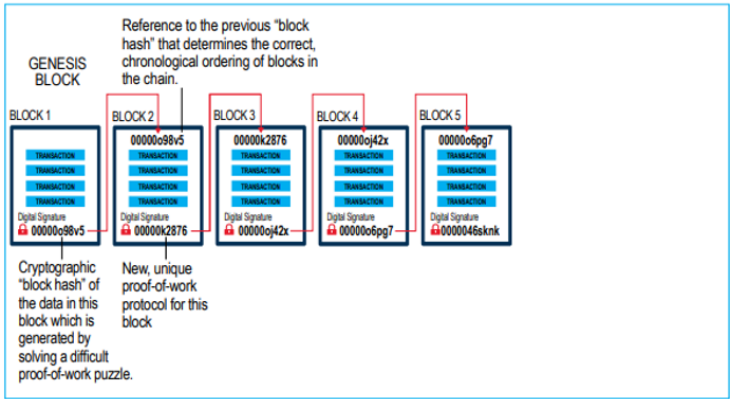
List of Companies Who Accepts Bitcoins

- KFC Canada
- Playboy
- Microsoft
- Subway
- Virgin Galactic
- Mint
- Yacht-base
- Intuit
- Grooveshark
- PizzaForCoins
- Whole Foods
- WannaCry
- OkCupid
- Expedia
- Wikipedia
- Zynga
- …

Cryptocurrency and Money Functions

- **Unit of account**
  - Unit of account is a basic measure of economic value
  - An economy would benefit from a stable unit of account, because if the price for a currency changes rapidly and frequently, it would be hard for business owners to carry out daily operation.
  - Bitcoin is a failure in terms of being a stable unit of account.
- **Store of value**
  - Gold and fiat money are most common store of value in modern times partly **due to their stable price** and the backing from governments respectively
  - Would not be considered as a stable store of value, but with the **rising public confidence** and more adoption of bitcoin, the store of value function could play more important role

Blockchain


GENESIS BLOCK
Reference to the previous "block hash" that determines the correct, chronological ordering of blocks in the chain.
BLOCK 1
BLOCK 2
BLOCK 3
BLOCK 4
BLOCK 5
TRANSACTION
Digital Signature
00000c98v5
00000k2876
00000oj42x
00000o6pg7
0000046sknk
Cryptographic "block hash" of the data in this block which is generated by solving a difficult proof-of-work puzzle.
New, unique proof-of-work protocol for this block

Background on the blockchain frenzy

AS OF MID-DECEMBER 2016…

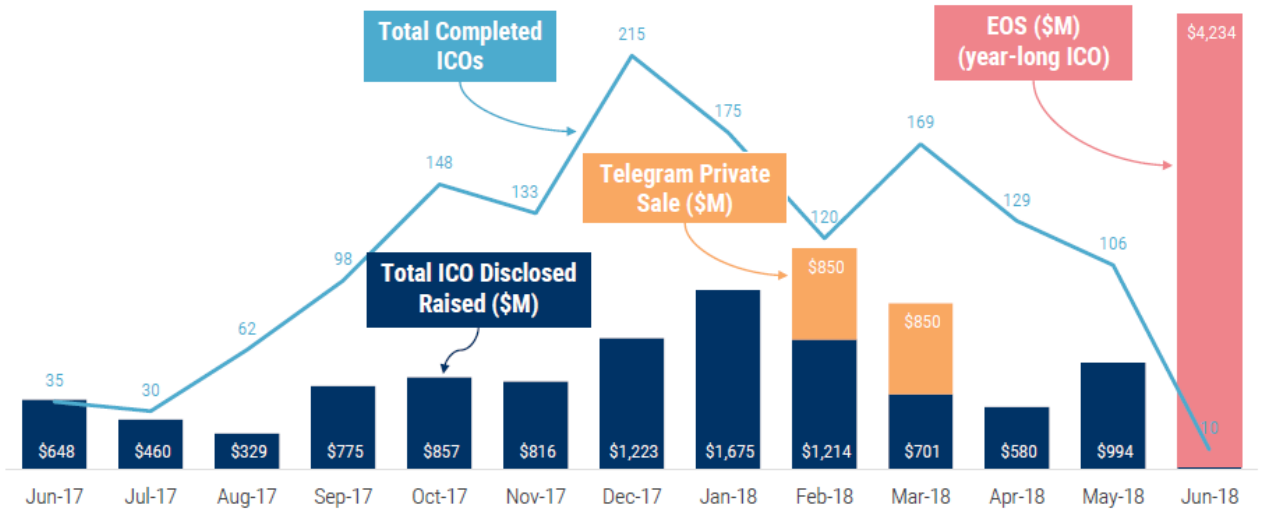
The market cap of all cryptocurrencies totaled **$15B**

In the beginning, there was Bitcoin

Bitcoin is an **online currency** that can be sent and received **peer-to-peer** by anyone in the world. With Bitcoin, **computers** – not humans – control the transfer and creation of money.

Completed ICOs raised about $18B in one year

Disclosed funding of completed ICOs (and Telegram's private sale). June 2017 – June 2018 (YTD)



AS OF MID-DECEMBER 2017…

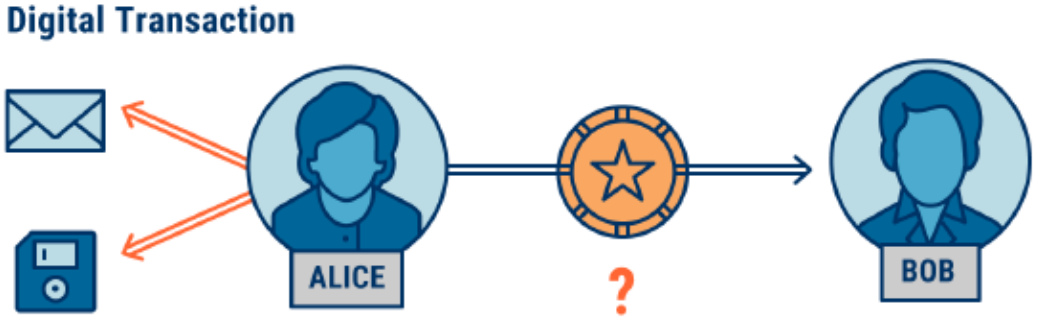
The market cap of all cryptocurrencies totaled **$500B** an increase of **3,200%**

Banks & financial services players exploring blockchain opportunities

A typical physical transaction

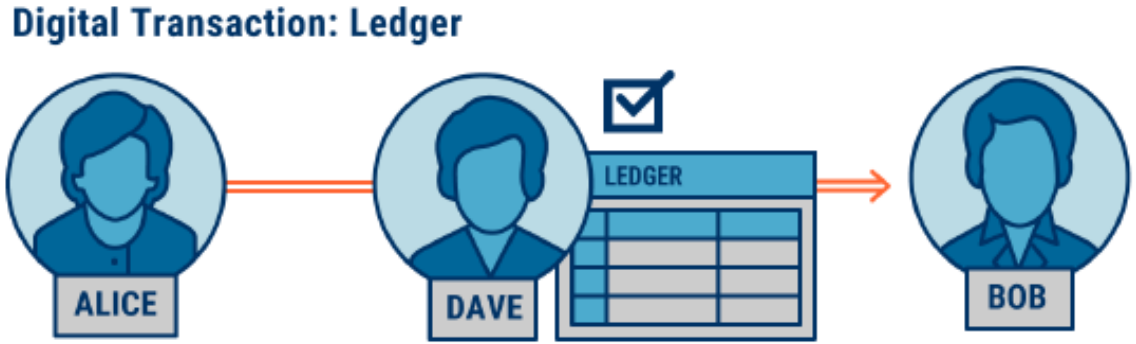
- Alice hands Bob a physical currency note worth 10$
- Bob has $10 more and Alice has 10$ less
- The transaction is complete

A typical digital transaction



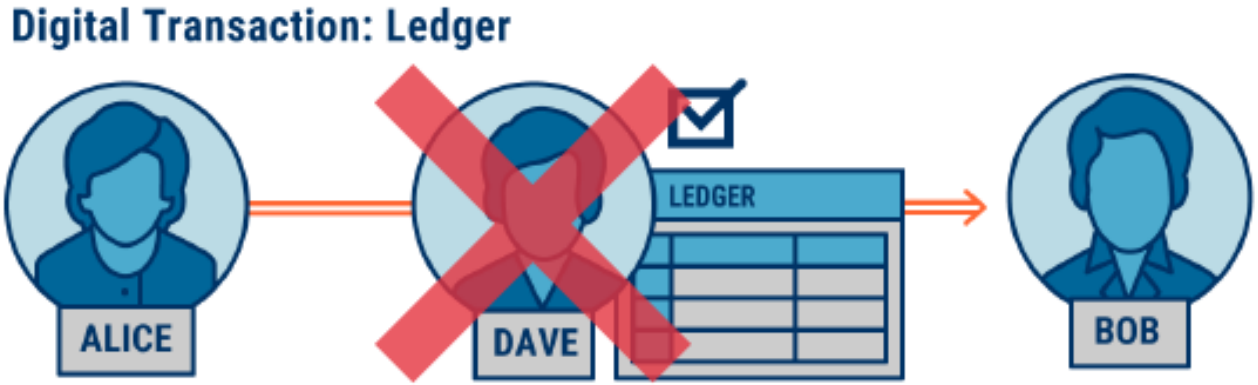
- Alice sends Bob a digital currency note worth 10$
- The transaction is complete
- Who is the unique owner

Let’s use a middleman



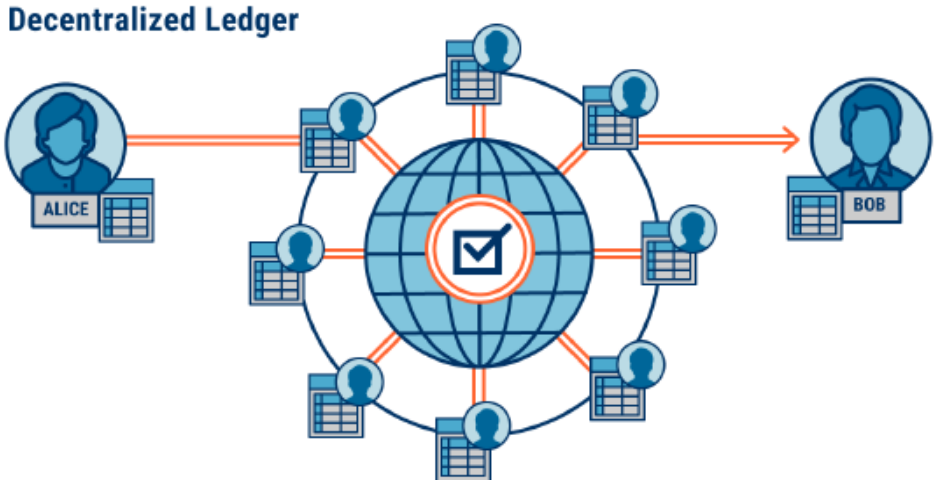
- A trusted third party will record the digital transaction in a database.
- This database —or ledger —will track a single asset: digital arcade tokens.
- This ledger is now the “source of truth.”

What if we can’t trust the middleman?



- What if Dave decides to charge a fee that neither Alice or Bob want to pay?
- What if Alice bribes Dave to erase her transaction?

What if we gave this database to trusted friends?

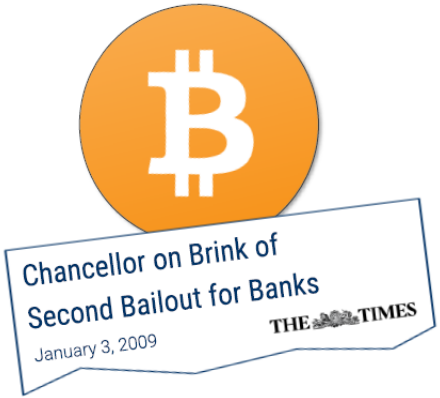


- Because the ledger is digital, all copies of the ledger could sync together.
- If a majority of participants agree that the transaction is valid (e.g. confirm that Alice owns the token and wants to send it), it gets added to this **decentralized ledger**.

DECENTRALIZATION MAKES SENSE

When everyone holds a copy of the ledger, **it's harder to cheat**; there is no single point of failure.

So What's Bitcoin?

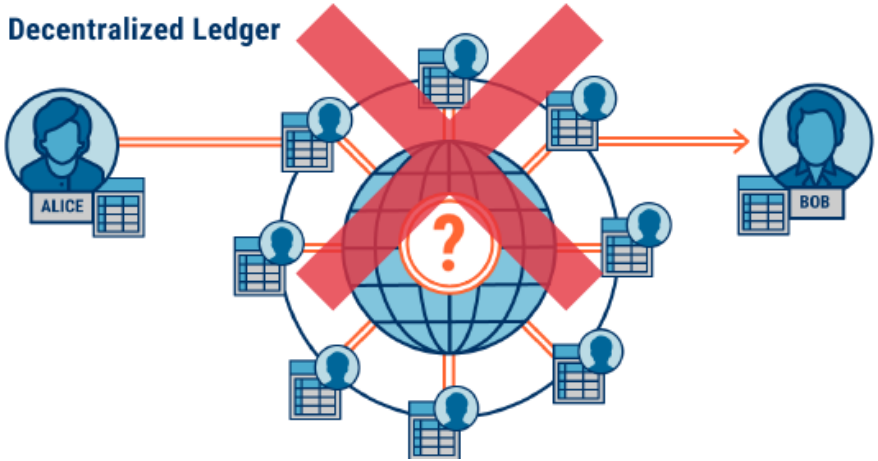


1. Bitcoin is a **decentralized**, public ledger. Due to its unique architecture, this ledger is known as a "**blockchain**." Bitcoin was the first to use blockchain technology.

2. This ledger's unit of account is "**bitcoin**." Bitcoin's rules state that there will only ever be 21 million bitcoin.

3. Bitcoin establishes **consensus** among untrusted nodes with a clever incentive structure, involving "miners."

What if we gave this database to everyone?



- Our “arcade token” ledger only allowed “trusted friends”to participate.
- In contrast, **Bitcoin is entirely public, and anyone can participate**.

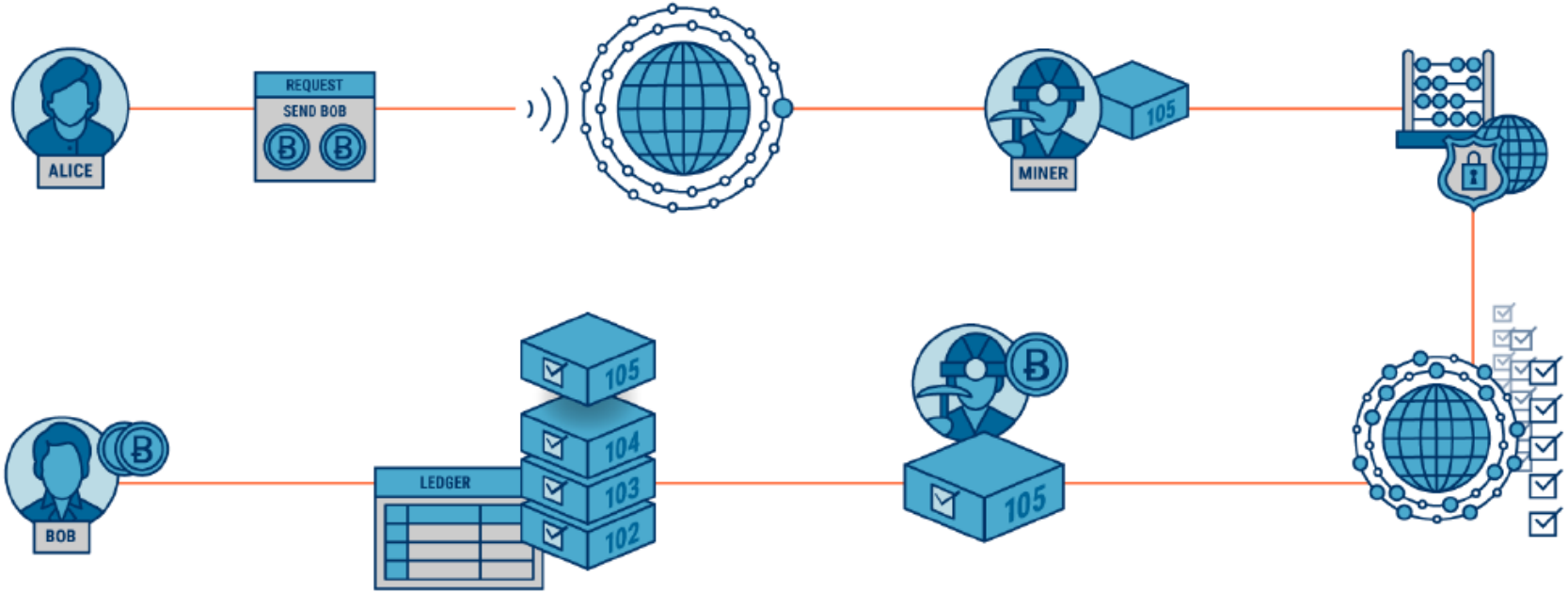
DECENTRALIZATION IS DIFFICULT

How does Bitcoin get untrusted participants to **come to a consensus** on the state of the ledger?

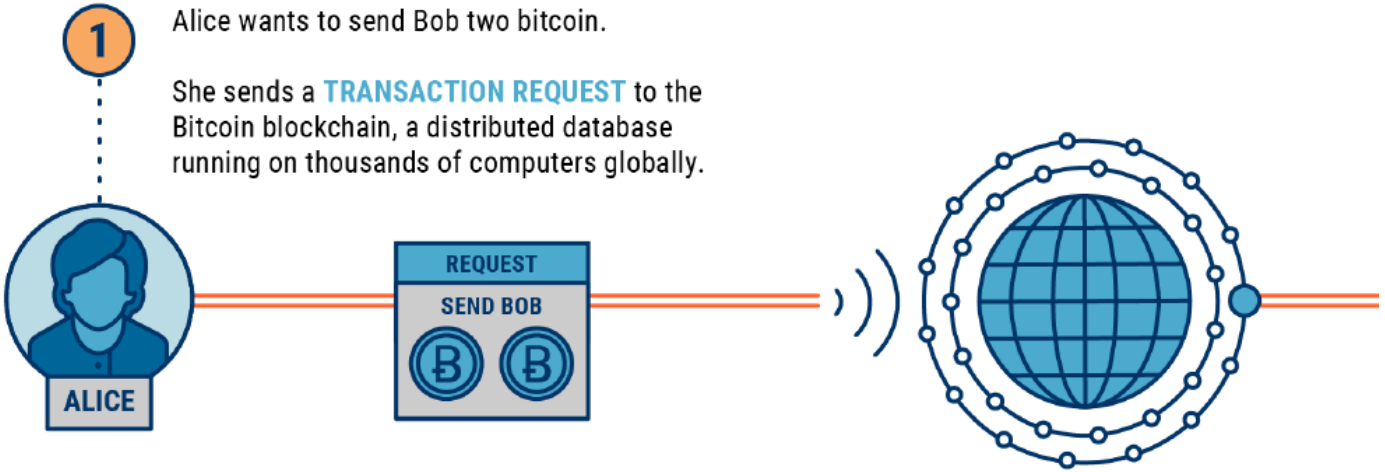
Bitcoin is secured through clever incentives

1. **CARROT:** Monetarily reward participants ("miners") for maintaining and securing the ledger
2. **STICK:** Monetarily punish bad actors for attacking the ledger

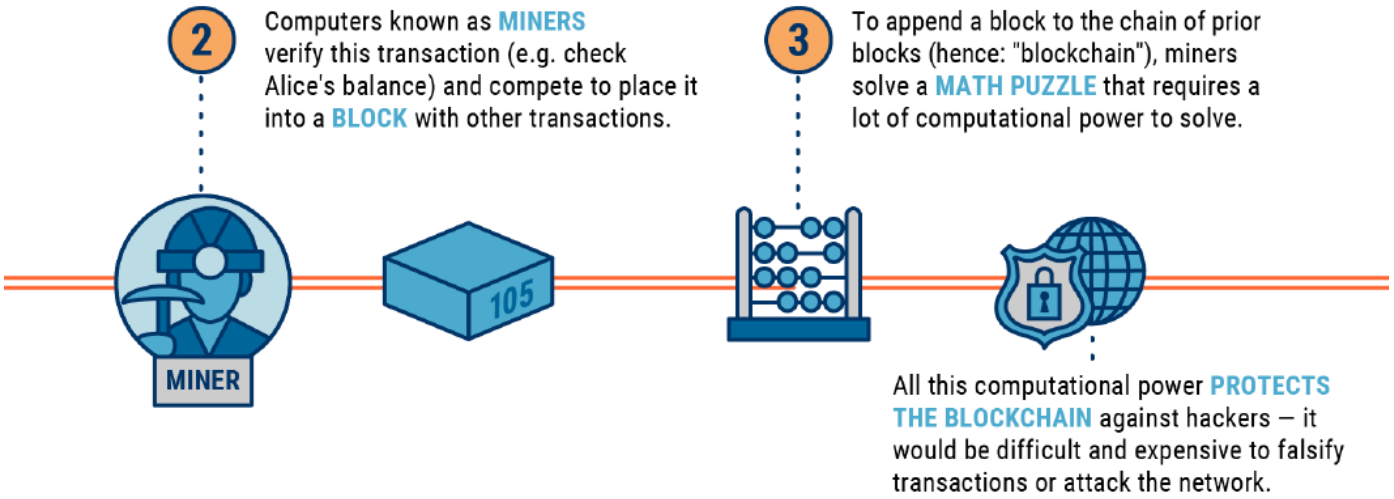
HOW BLOCKCHAIN POWERS BITCOIN



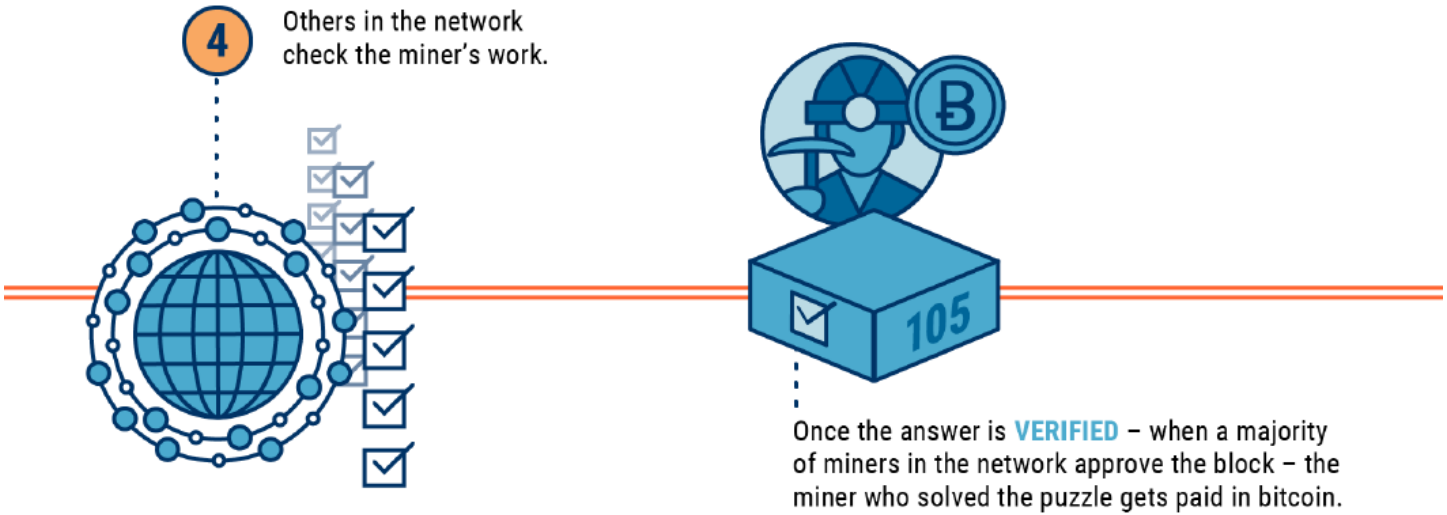
Understanding a bitcoin transaction



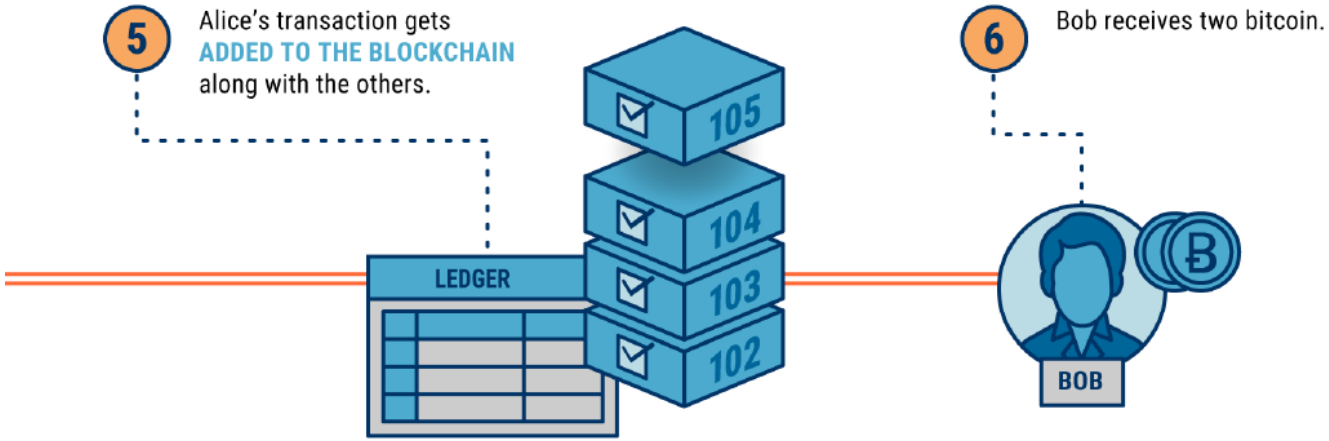
Understanding a bitcoin transaction



Understanding a bitcoin transaction



Understanding a bitcoin transaction

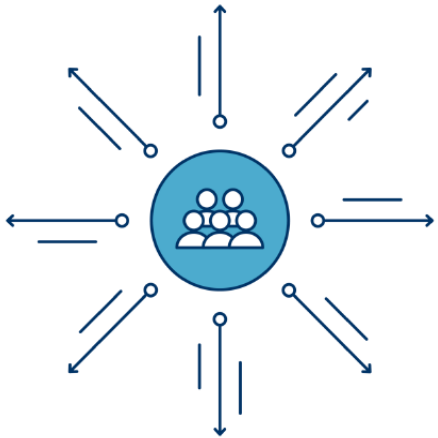


Wait… what is Bitcoin?

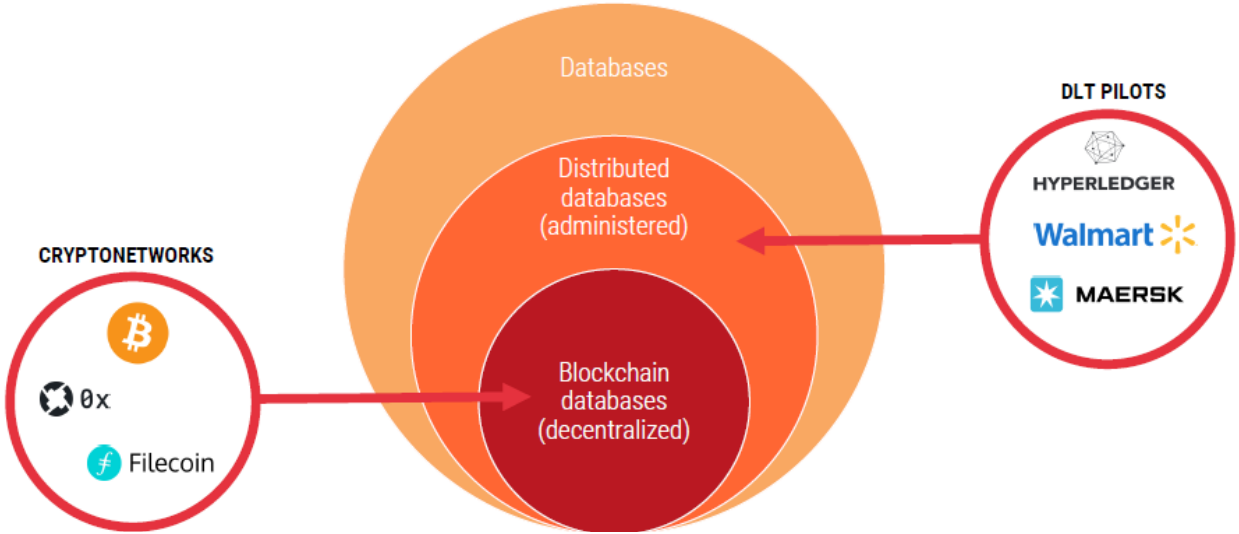
WHY IS BITCOIN WORTH SO MUCH MONEY?

Bitcoin is the first decentralized, censor-proof, portable, secure, durable, and **scarce** digital asset.

2. What is blockchain technology?



Blockchain allows **untrusted parties** to reach **consensus** on a shared digital history, **without a middleman**.


Databases
Distributed databases (administered)
Blockchain databases (decentralized)
CRYPTONETWORKS
0x
Filecoin
DLT PILOTS
HYPERLEDGER
Walmart
MAERSK

Blockchain will do for transactions what the internet did for information.

ENABLING TRUST

New technology is creating radical transparency – and uprooting how we interact, transact, and grow

NEW REVENUE STREAMS

More than a new technology, blockchain is rewriting how we do business

REMOVING BARRIERS

IBM Blockchain creates certainty, advances knowledge, brings together industries, and improves business process

REINVENTING BUSINESS

Blockchain is shifting from one way of doing business to *the* way – creating new business solutions where there were none

Blockchain in Finance

- **Payments:** By eliminating the need to rely on intermediaries to approve transactions between consumers, blockchain technology could facilitate faster payments at lower fees than banks.
- **Clearance and Settlement Systems**: Blockchain technology and distributed ledgers can reduce operational costs and bring us closer to real-time transactions between financial institutions.
- **Fundraising:** By providing blockchain companies with immediate access to liquidity through initial coin offerings (ICOs), the blockchain is creating a new, cryptoeconomic model of funding that unbundles access to capital from traditional financial services.
- **Securities:** By tokenizing traditional securities such as stocks, bonds, and alternative assets, the blockchain is upending the structure of capital markets.
- **Loans and Credit:** By removing the need for gatekeepers in the loan and credit industry, the blockchain can make it more secure to borrow money and provide lower interest rates.

	'Public' (open) Blockchains	Permissioned Blockchains
Central party	No central owner or administrator	Has some degree of external administration or control
Access	Anyone can join	Only pre-selected participants can join the network
Level of Trust	Network members are not required to trust each other	Higher degree of trust among members required (as collaboration among members could alter the ledger)
Openness	Ledger is open & transparent - shared between all network members	Different degrees of openness and transparency of the ledger are possible
Security	Security through wide distribution in a large scale network	Security through access control combined with DLT in smaller scale networks
Speed	Slower transaction processing restricts transaction volume	Faster transaction processing allows for higher transaction volume
Identity	User identity anonymous or protected by pseudonyms	Identity verification typically required by owner/administrator
Consensus	Difficult proof-of-work required as consensus mechanism	Variety of consensus mechanisms possible (typically less difficult & less costly than proof-of-work in permissionless blockchains)
Asset	Typically: native cryptocurrencies. But implementations are possible where a token is used which can represent any asset.	Any asset
Legal ownership	Legal concerns over lack of ownership as no legal entity owns or controls the ledger	Greater legal clarity over ownership as owner/administrator is typically a legal entity
Examples	Bitcoin, Ethereum	R3's Corda, Hyperledger Fabric

Examples of DLs	
Bitcoin	• Open/Permissionless • First and largest public blockchain • Records transactions of cryptocurrency Bitcoin • View transactions live here: https://blockchain.info/
Ethereum	• Open/Permissionless • Most popular blockchain for smart contracts (see section 8). Ethereum allows for a scripting language to exist on top of a blockchain, which enables construction of smart contracts. • The DAO used Ethereum (see Annex)
Ripple	• Permissioned • Focused on commercial cross-border and inter-bank payments • Offers alternative to correspondent banking • Raised $55 million in Series B funding in Q3 2016
Fabric (Hyperledger Project)	• Permissioned • Open-source • Focused on helping financial institutions mitigate settlement risk and lower reconciliation costs • Collaboration between the Linux Foundation and over 80 financial and technological companies including IBM, DTCC, JP Morgan, Accenture, CISCO
Corda (R3 CEV)	• Permissioned • Created by R3, a consortium of over 70 financial institutions • Open-source • Focus on financial applications

WHAT ARE ALTCOINS?

- Since Bitcoin launched in 2008, thousands of other cryptocurrencies and altcoins (“alternative coins”) have emerged.
- Because Bitcoin’s code is open-source, anyone can use Bitcoin’s code to create an altcoin. Many of them seek to improve on Bitcoin or expand its capabilities.
- **IS BITCOIN A BUBBLE?**
- Value of one bitcoin has gone from around $300 in 2015 to above $11,000
- If you had invested $100 in bitcoin in 2011 that bitcoin would be worth well over $2.5M today

WHAT'S THE CATCH?

What are some of the major **challenges** facing blockchain technology?

Blockchain technology faces technical obstacles

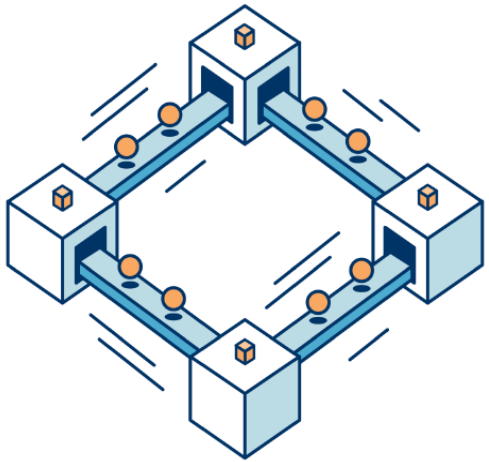
What does it take to scale?

LEDGER STORAGE SIZE

TRANSACTION SPEED

MINERS TOO POWERFUL

3. What is Ethereum?



If Bitcoin is a decentralized ledger for **payments**, then Ethereum is a decentralized computer for **applications**.

Can we do more with Blockchain?

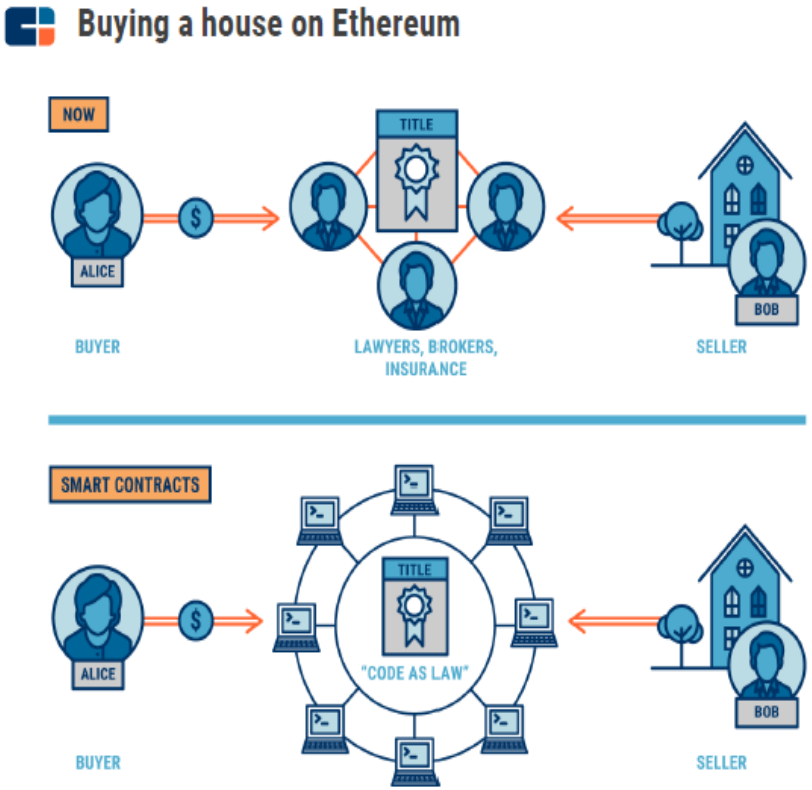
- What if Alice wants to add a **condition** to her payment?
- Perhaps Alice and Bob enter into a wager —how can they program and enforce that wager on the blockchain?

WHAT IS A SMART CONTRACT?

- Alice and Bob enter into a bet.
- Alice thinks that the temperature tomorrow morning will reach 70 degrees.
- Bob thinks that it will stay lower.
- They wager 10 bitcoin on the outcome.
- Ethereum, offers a decentralized solution. Alice and Bob could agree to use some basic code — a contract of sorts — to alert the system to what the temperature ended up being and pay out based on who was correct
- If the temperature goes higher than 70 degrees, the code pays Alice, otherwise, it pays Bob
- Alice and Bob could then place this code (their bet) on Ethereum's blockchain.

Ethereum does more with ‘smart contracts’

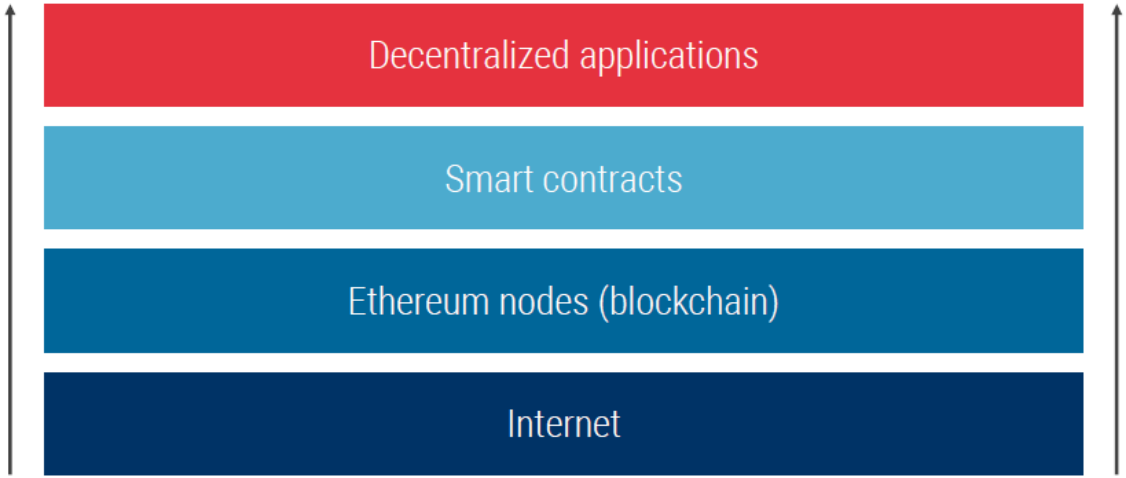
- A smart contract is self-executing and self-enforcing **code**.
- Unlike traditional centralized applications, this code is stored on the blockchain and **validated by all participants**.
- This enables counterparties to build **decentralized applications**.



2ND GENERATION BLOCKCHAIN

Ethereum is a blockchain that runs **smart contracts**, which allows developers to build complex **decentralized applications**.

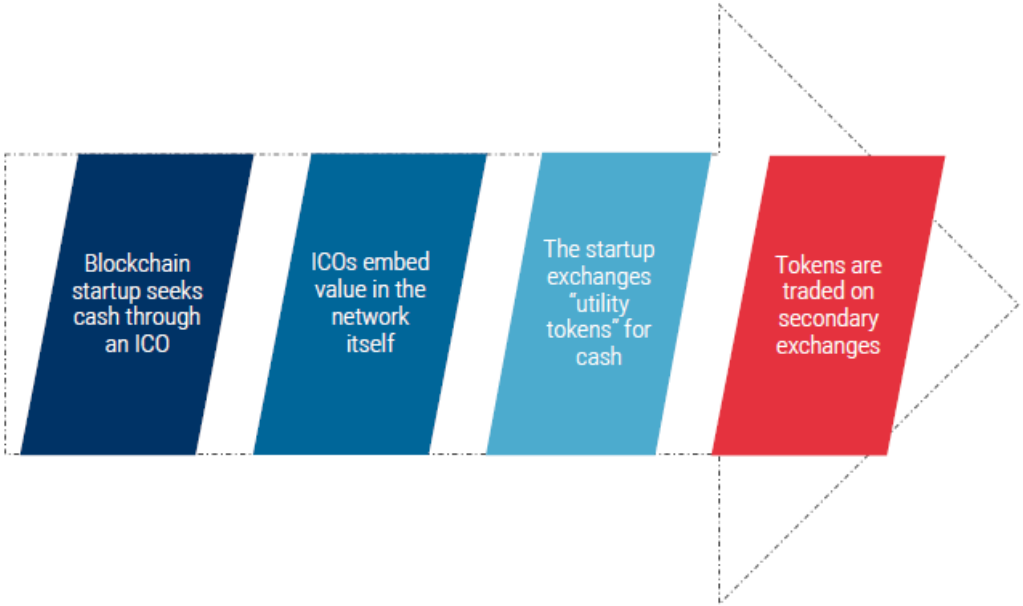
The Ethereum development stack



4. What are initial coin offerings?

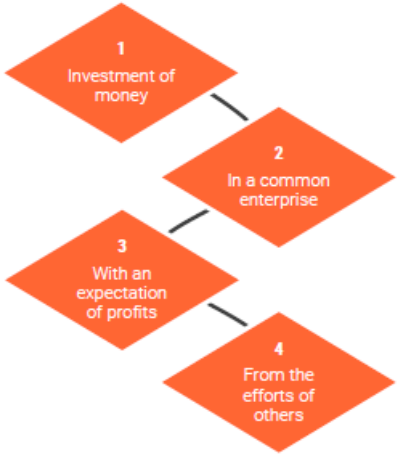
An initial coin offering (ICO) is when a company sells **tokens** to the public. Just like bitcoin or ether, these tokens provide **utility within the network**.

How do ICOs work?



Is your token a security?

The Howey Test



Tokens challenge the status quo

5. Let’s review

Key takeaways

BITCOIN

Bitcoin is the first decentralized, censor-proof, portable, secure, durable, and **scarce** digital asset.

BLOCKCHAIN

Blockchain is the technology behind bitcoin, that allows untrusted parties to reach **consensus** on a shared digital history, without a middleman.

ETHEREUM

Ethereum is a blockchain that runs **smart contracts**, which allows developers to build complex decentralized applications.

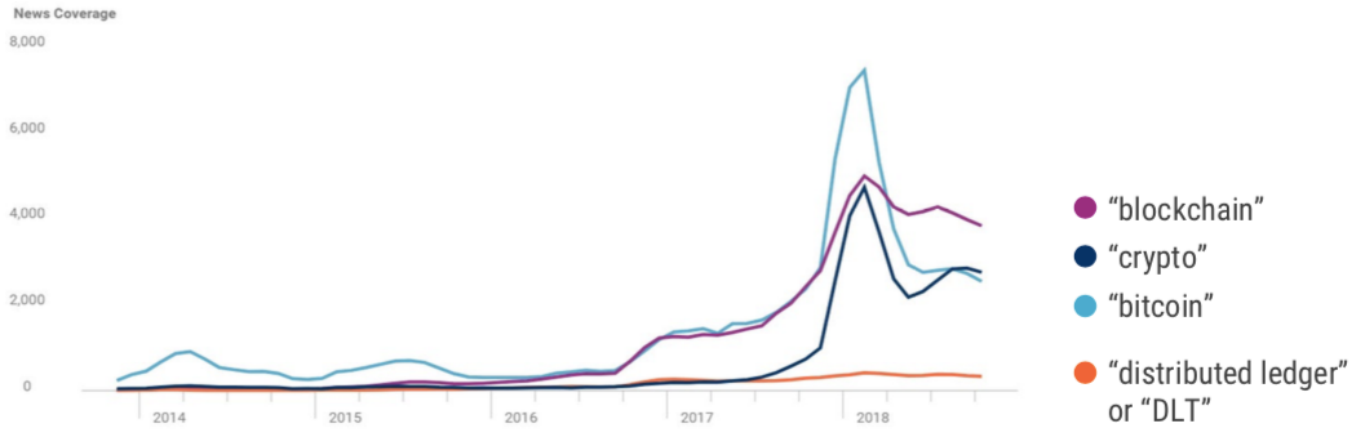
ICOs

An ICO is when a company sells **tokens** to the public. Similar to bitcoin or ether, these tokens provide utility within their decentralized application.

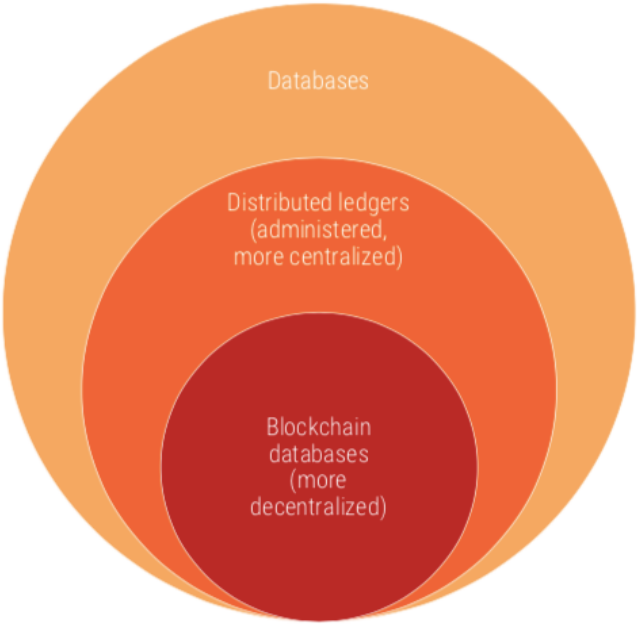
Blockchain Terminologies

Diverse terms highlight the sector's nomenclature

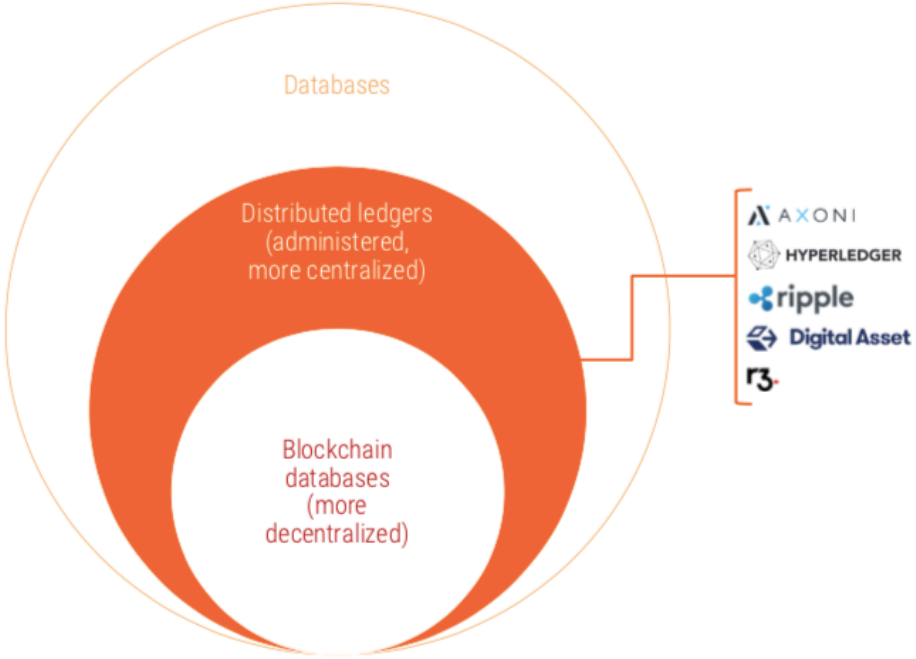
News coverage of blockchain-related terms. Q4'13 – Q4'18 YTD (11/26/2018).



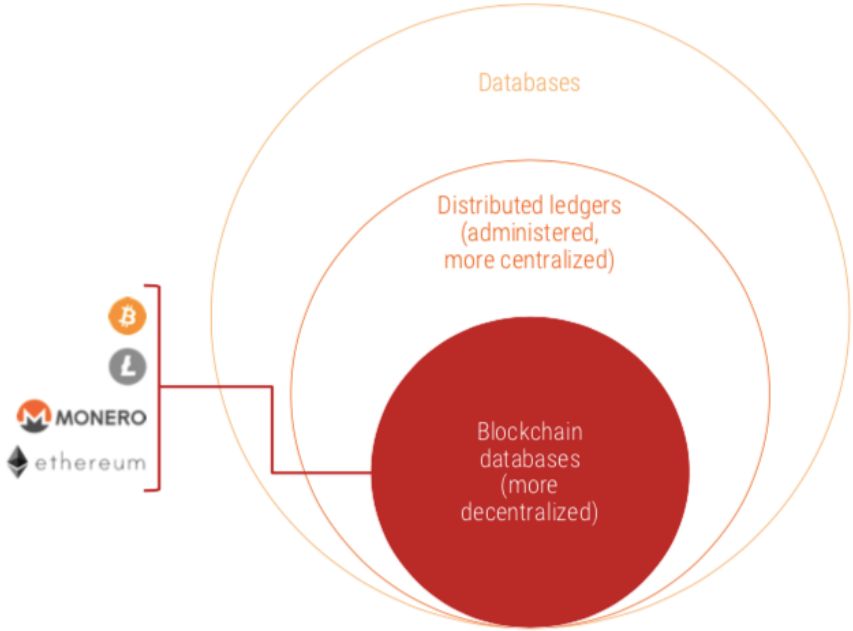
‘Blockchain’ is different things to different users



Corporates are looking at less centralized DLT

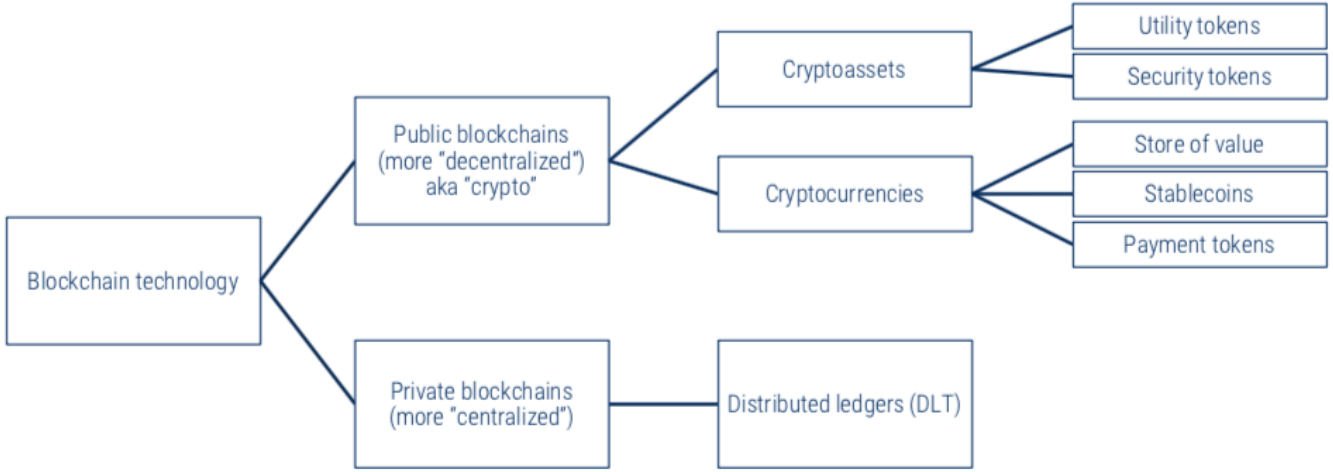


Public blockchains are rethinking money, web 3.0

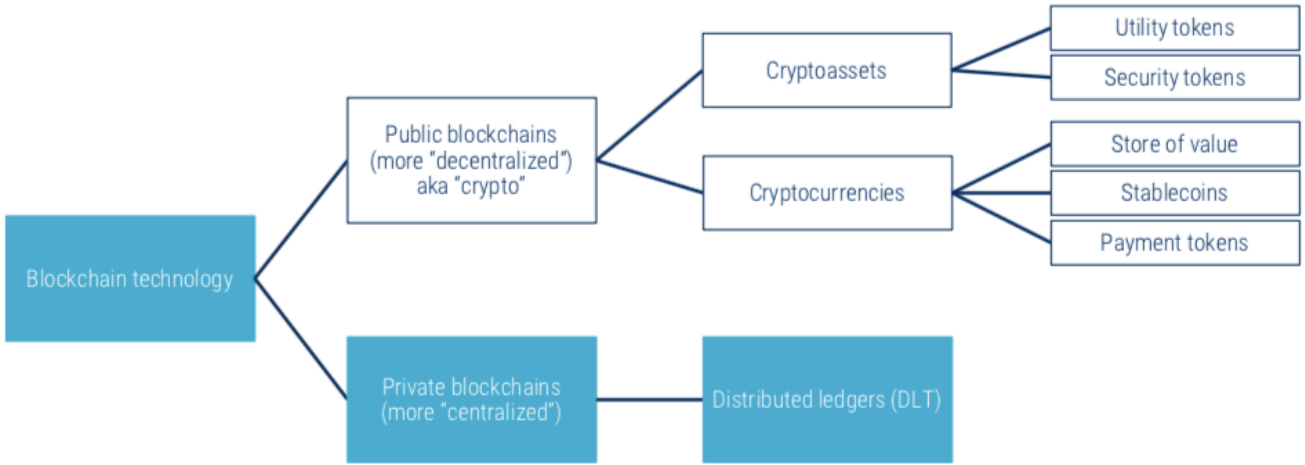


The conversation is much larger than Bitcoin

The ingredients for public blockchains have existed for decades. Bitcoin was the first to put them together. In this way, Bitcoin has reinvigorated conversations around pre-existing “distributed” technologies, as well as expanded the conversation to more novel blockchain-focused use cases.



Corporates have been looking at ‘enterprise blockchain,’ DLT for years



BLOCKCHAIN, NOT BITCOIN

"We really want to distinguish **the blockchain**, which is an area of huge emphasis and investments across our industry and across many industries, from **a particular application of blockchain** which tends to get all the news cycles; which is **cryptocurrencies**."

Martin Chavez
CFO, Goldman Sachs

Q1'18 Earnings Call

Big banks are among the most active investors

Equity investments and consortia involvement. Q1'12 – Q1'18

	citi	Goldman Sachs	JPMorgan Chase & Co.
INVESTMENTS	Digital Asset AXONI Cobalt SETL Chain	Digital Asset AXONI CIRCLE BitGo veem	Digital Asset AXONI
CONSORTIA	r3		HYPERLEDGER ENTERPRISE ETHEREUM ALLIANCE

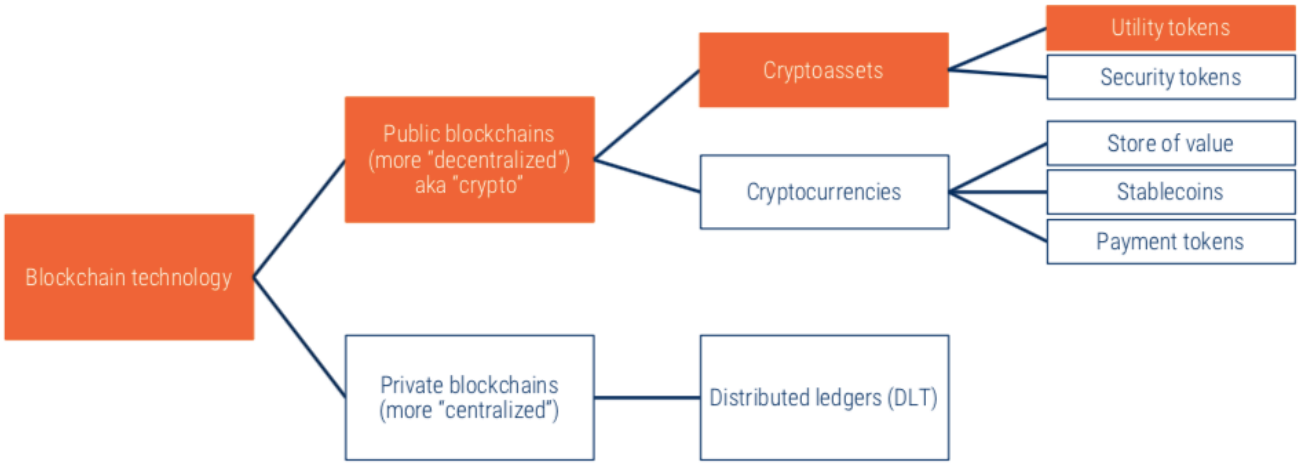
Lots of pilots have stalled, while the jury is still out on some high-profile projects

Cryptoassets

1. **Utility tokens:** Plans to reshape the web haven't quite panned out, with speculation drying up, regulators clamping down, and users failing to show up.

2. **Security tokens:** In what looks like crypto's next act, security token projects are seeing lots of investment, but could face similar challenges to those faced by corporates in earlier attempts to tokenize financial assets.

Developers are looking to use public blockchains and utility tokens to build a decentralized web



The centralized web has its share of issues

Facebook faces fresh lashing from nine countries for its inability to stop the spread of fake news

November 27, 2018 | The Washington Post

The Privacy Battle to Save Google from Itself

November 1, 2018 | WIRED

Fixing the internet

November 23, 2018 | Science

facebook

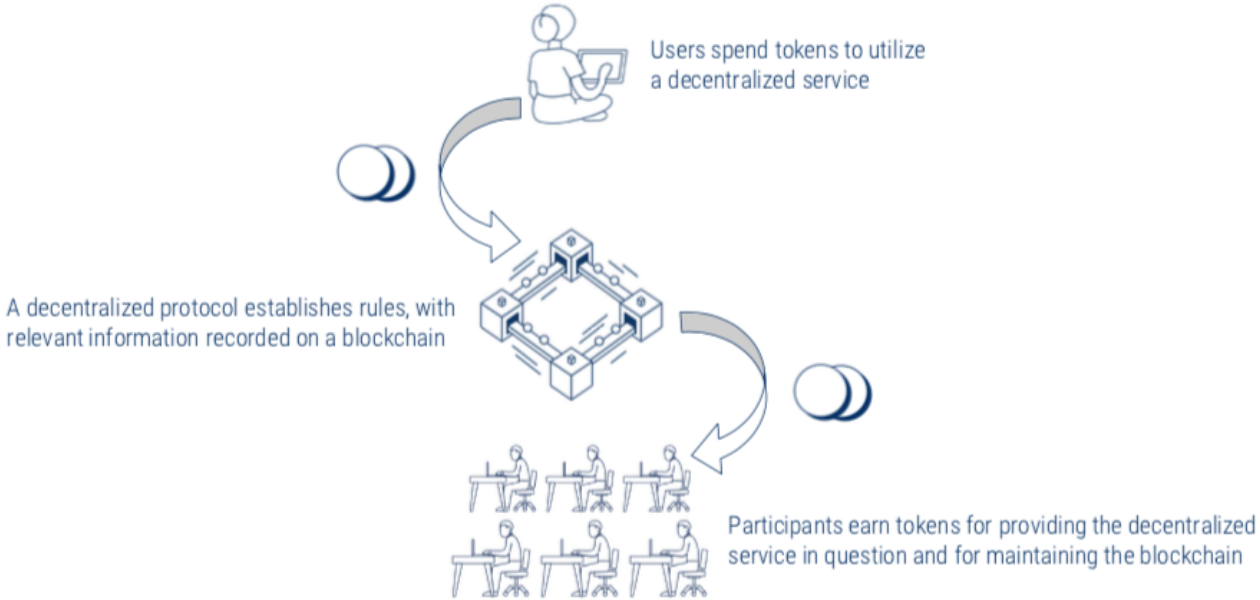
WEB 3.0

"The **real promise** of these new technologies, many of their evangelists believe, lies not in displacing our currencies but in replacing much of what we now think of as the internet, while at the same time **returning the online world to a more decentralized and egalitarian system**."

Steven Johnson
Author, *Beyond the Bitcoin Bubble*

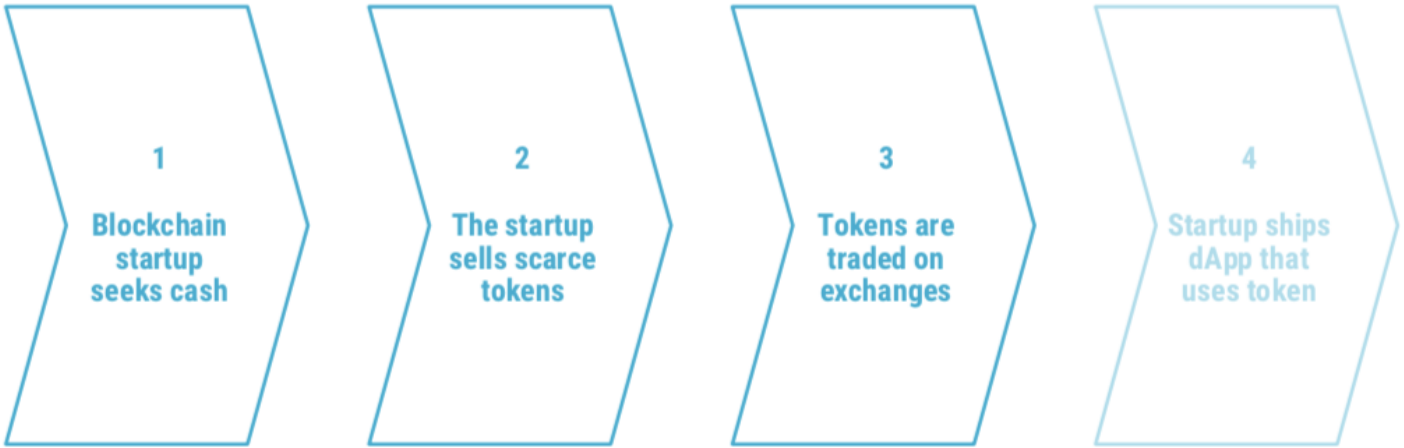
Could utility tokens reorganize the web?

Native tokens incentivize various stakeholders in decentralized networks and applications.



Most companies building ‘utility token’ networks received funding via ICOs

Many ICOs were unregulated, and played a game of ‘regulatory arbitrage’



ICOs LOOK LIKE – ILLEGAL – UNREGISTERED SALES OF SECURITIES

"If you finance a venture with a token offering, you should start with the assumption that it is a security."

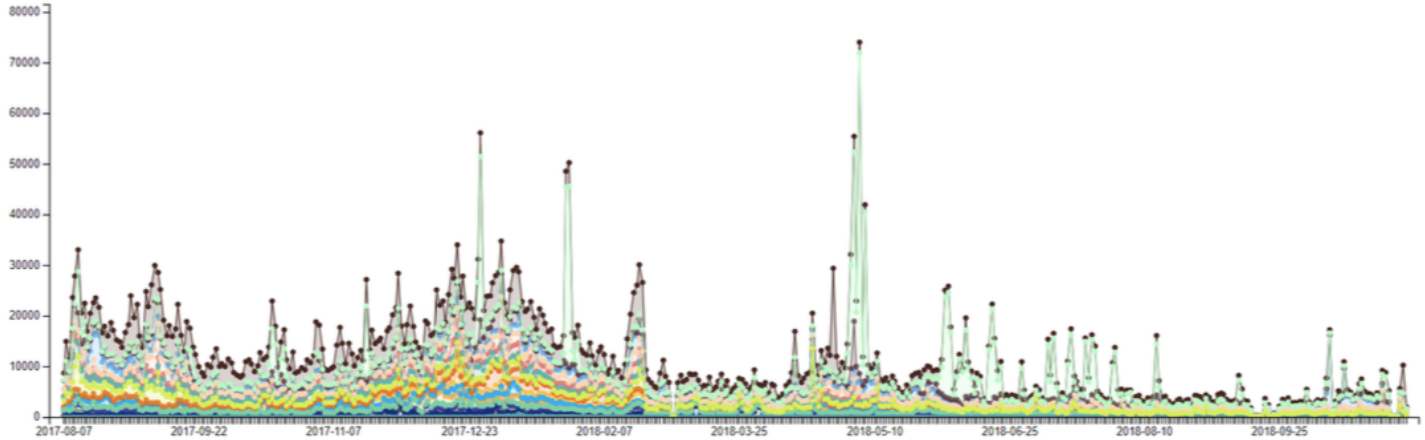
Jay Clayton
Chairman, SEC

Consensus Invest – November 27, 2018

SEC, other regulators are cracking down hard

Almost nobody is using decentralized applications, with some seeing no usage at all

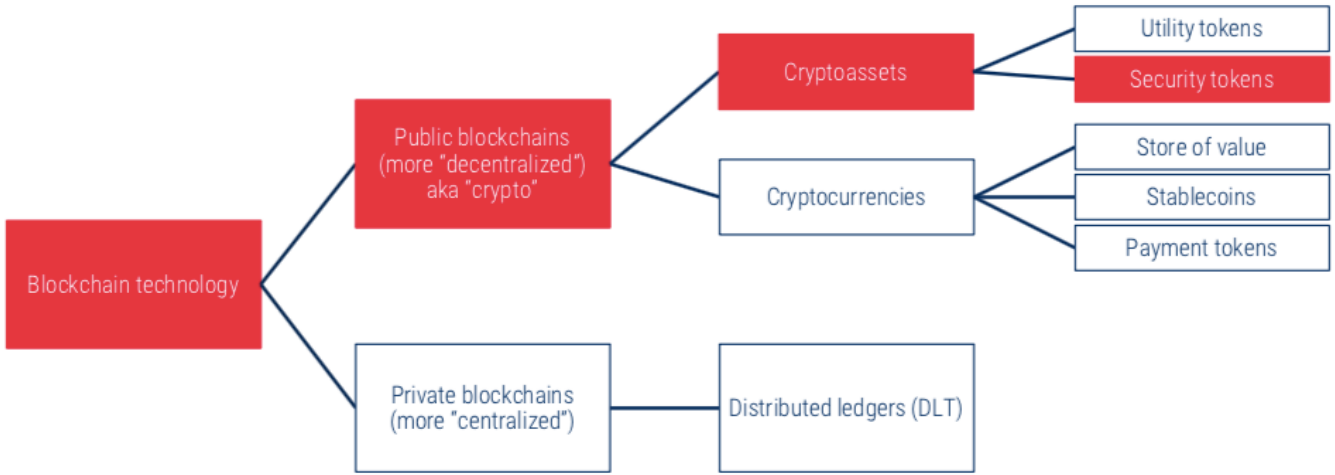
User metrics of 19 popular decentralized applications (dApps). 08/07/2017 – 11/26/2018



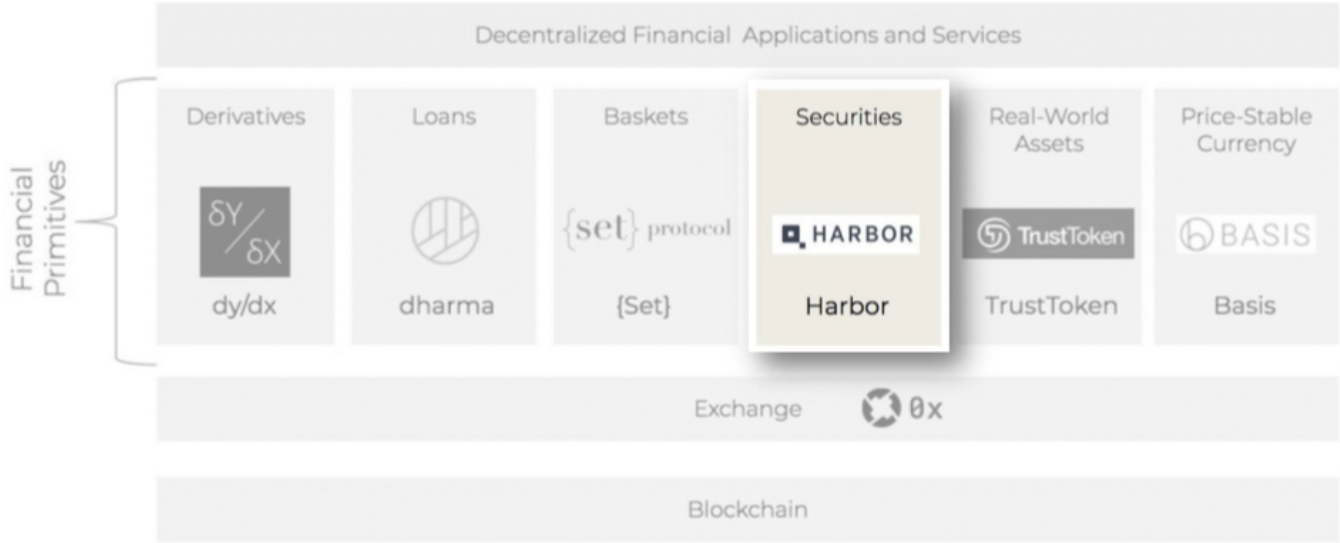
1. **Utility tokens:** Plans to reshape the web haven't quite panned out, with speculation drying up, regulators clamping down, and users failing to show up.

2. **Security tokens:** In what looks like crypto's next act, security token projects are seeing lots of investment, but could face similar challenges to those faced by corporates in earlier attempts to tokenize financial assets.

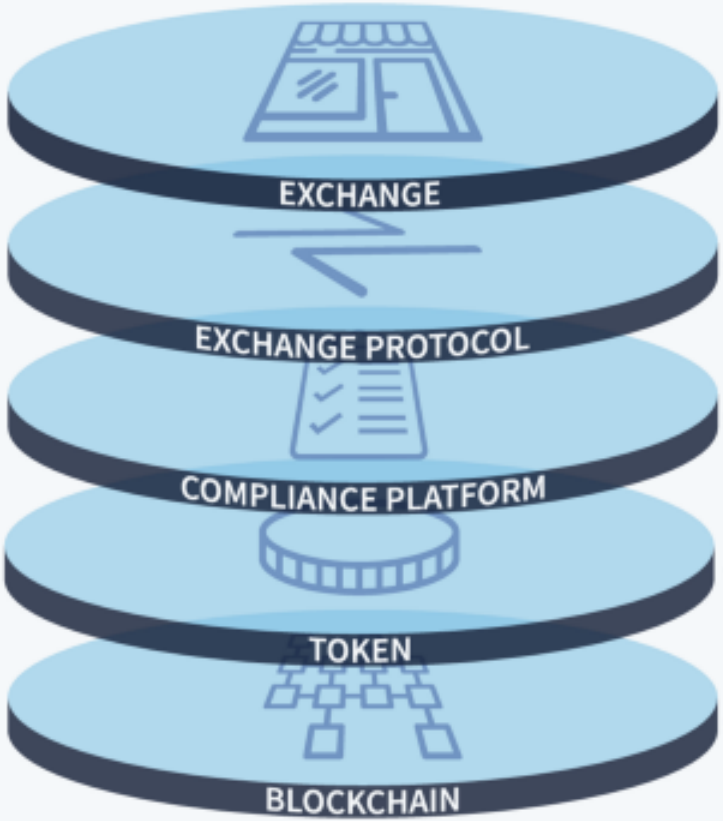
Security tokens hope to enable an open, decentralized financial system



Security tokens are one piece of a blockchain-based financial stack

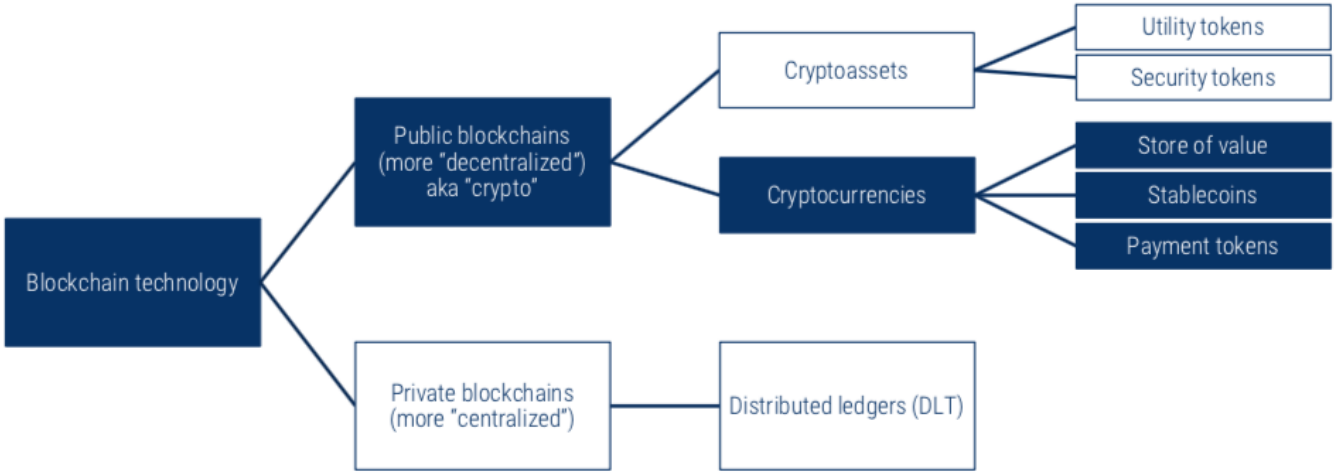


The Security Token Stack



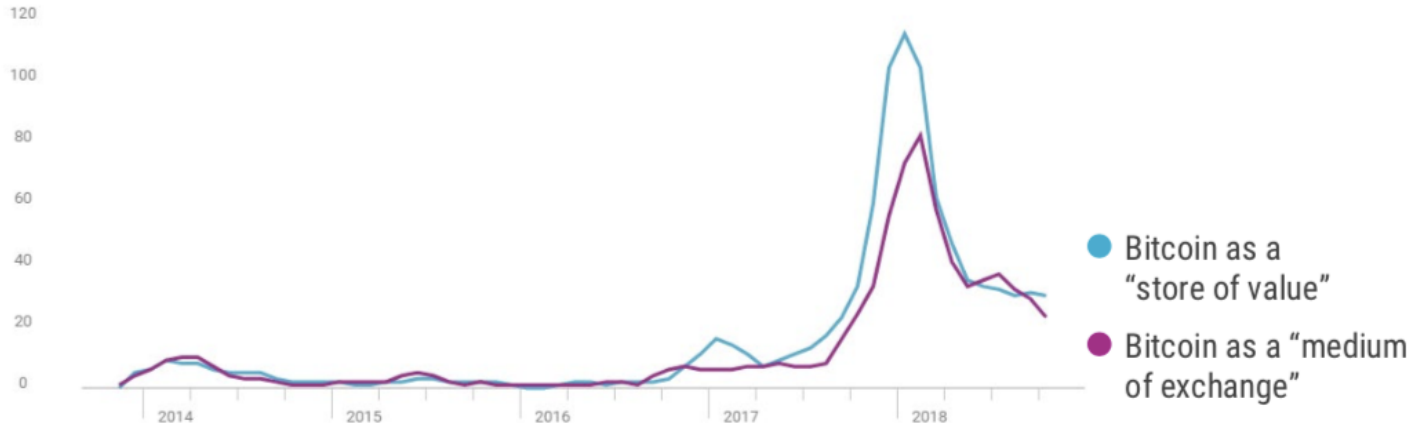
The Ocean
SHARESPOST
AIRSWAP
0x protocol
SWAP
HARBOR
R-Token (ERC20)
ethereum

Development on blockchain's first use case – censorship-resistant money – continues apace



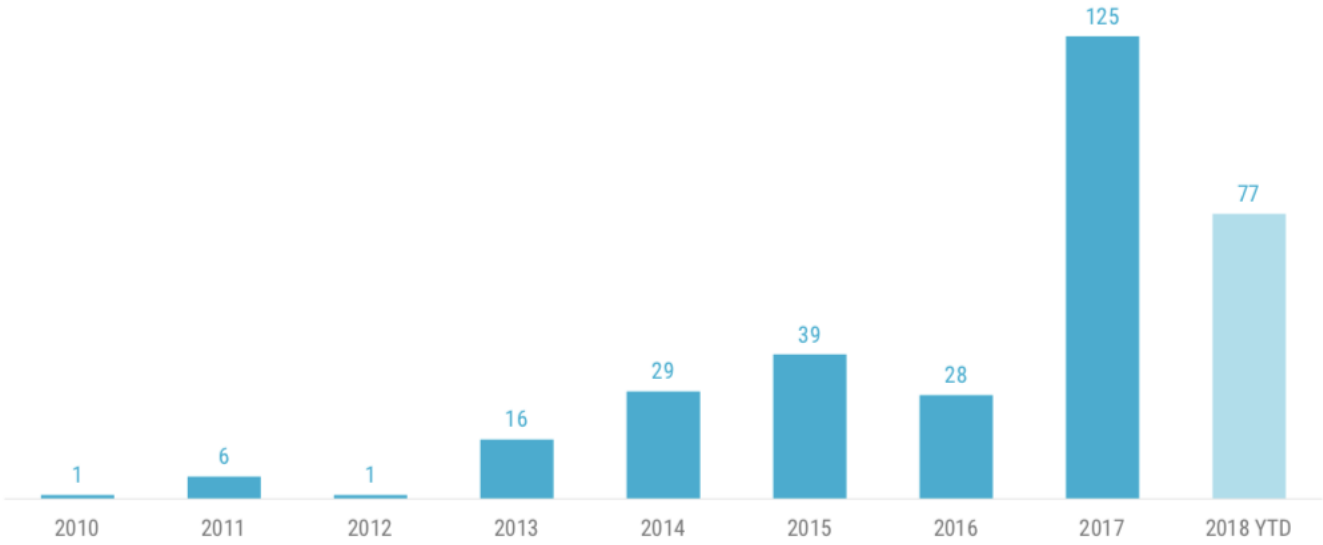
Bitcoin isn't yet 'peer-to-peer electronic cash'

Media mentions of bitcoin as a "store of value" and as a "medium of exchange." Q4'13 – Q4'18 YTD



Still, Bitcoin hasn't died yet – even as its price falls

Bitcoin "obituaries" by year. 2010 – 2018 YTD (11/26/2018)

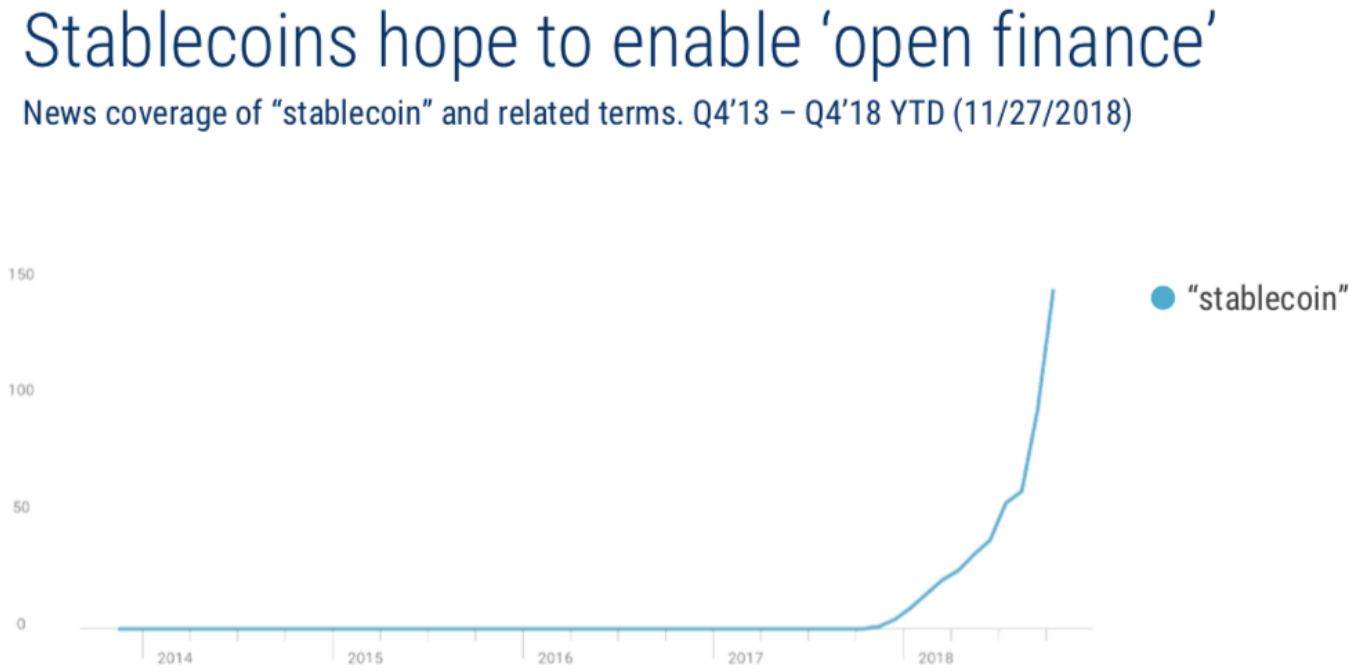


Bitcoin proponents: “we’re just getting started”

Bitcoin’s volatility remains a barrier to adoption

30-day BTC/USD volatility vs. 30-day USD/EUR volatility. 2014 – 2018 YTD (11/08/2018)

A useful currency should be a medium of exchange, a unit of account, and a store of value.



Companies are employing different strategies to create stable cryptocurrencies

Fiat-Collateralized

tether

TrueUSD

USD Coin

Commodity-Collateralized

DG

Crypto-Collateralized

HAVEN

Non-Collateralized

BASIS

Terra

CARBON

THE STABLECOIN THESIS

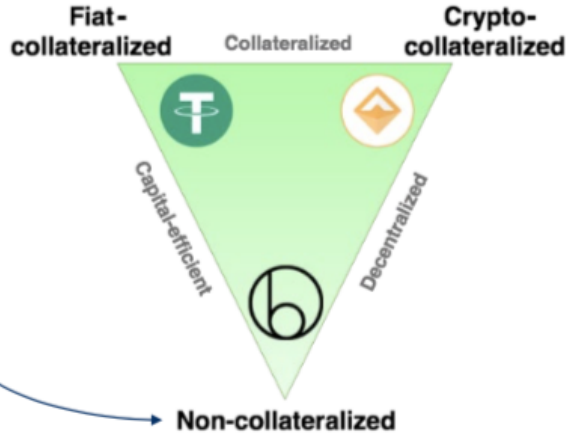
BASIS

Funding

$125M

Basis is building a “stablecoin,” that hopes to be less volatile than other cryptocurrencies.

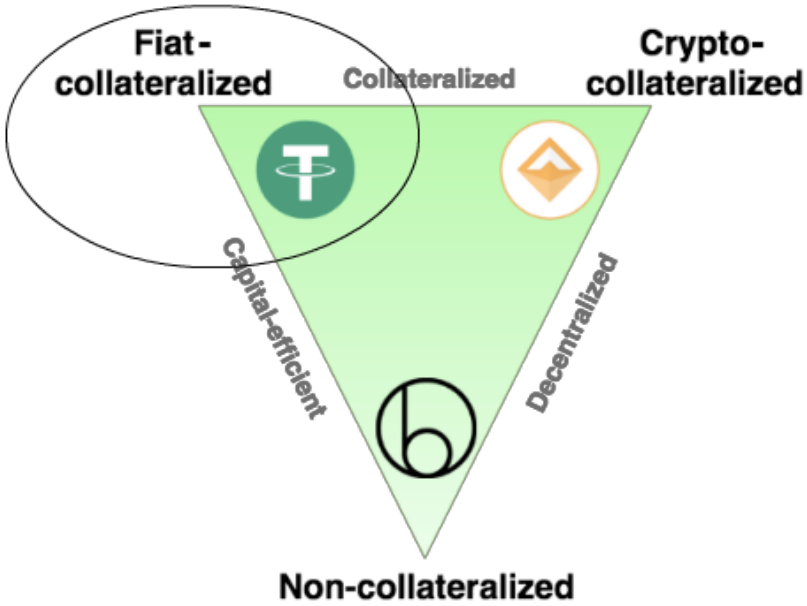
Creating an “algorithmic central bank,” Basis’s blockchain will automatically sell “bond tokens” to peg the price of a single Basis token at a dollar.



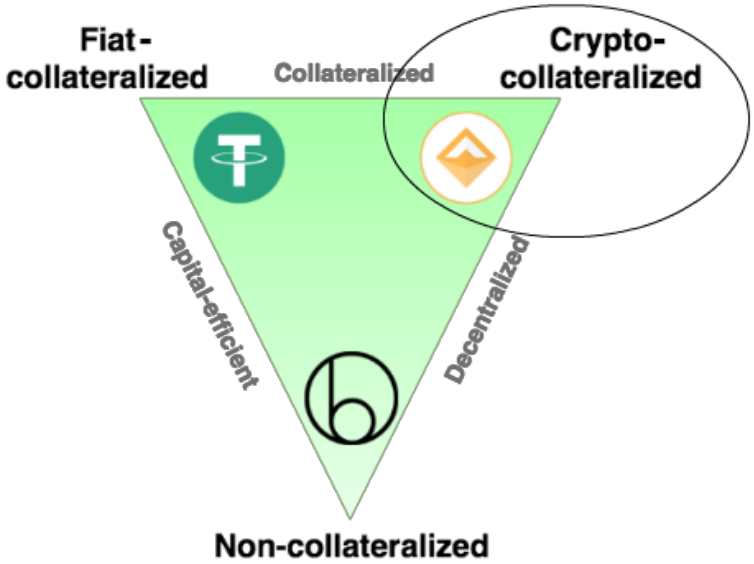
SELECT INVESTORS

Andreessen Horowitz, Bain Capital Ventures, Lightspeed, Google Ventures, Polychain Capital

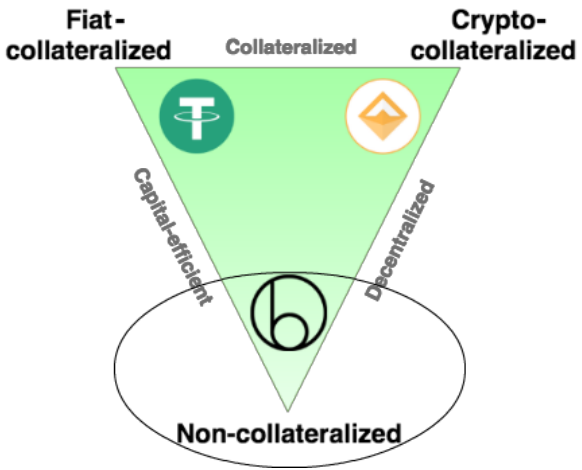
- You deposit dollars into a bank account and issue stablecoins 1:1 against those dollars.
- When a user wants to liquidate their stablecoins back into USD, you destroy their stablecoins and wire them the USD.
- This asset should definitely trade at $1 — it is less a peg than just a digital representation of a dollar.



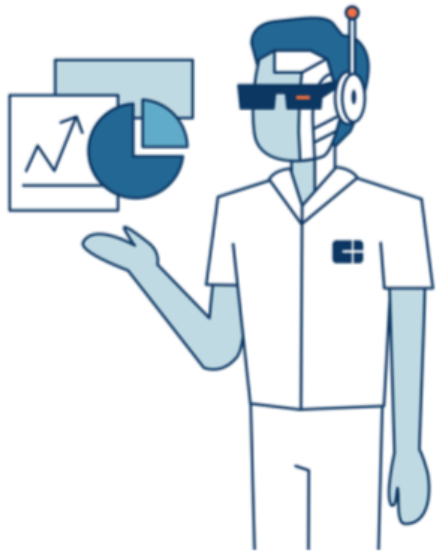
- Let’s back the coin with reserves of another cryptocurrency.
- Over-collateralize the stablecoin so it can absorb price fluctuations in the collateral.
- Say we deposit $200 worth of Ether and then issue 100 $1 stablecoins against it. The stablecoins are now 200% collateralized.



- What if you model a smart contract as a central bank? The smart contract's monetary policy would have only one mandate: issue a currency that will trade at $1.



To recap



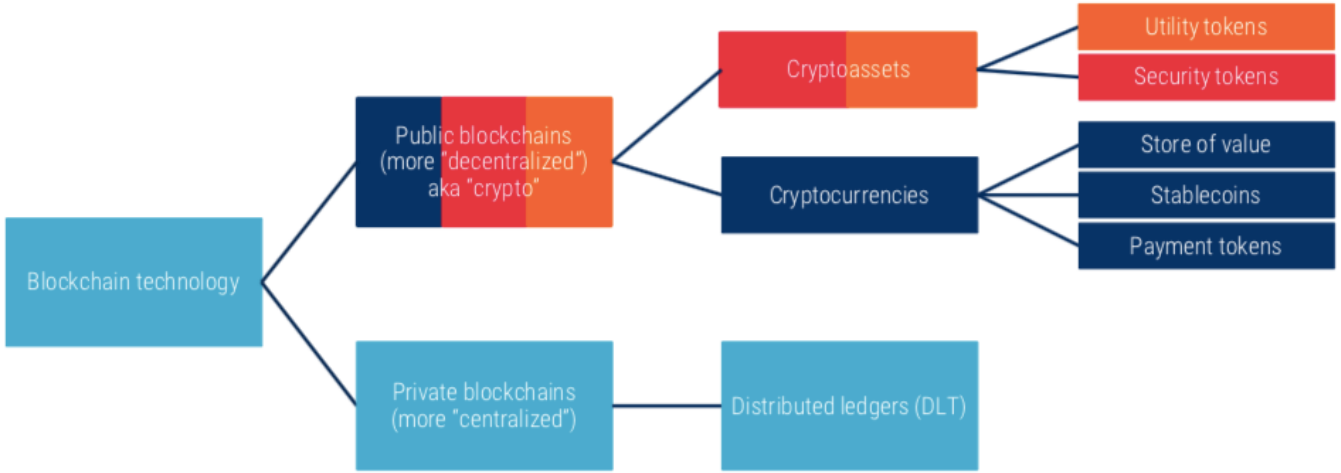
1. **Distributed ledgers:** While not blockchains per se, distributed ledgers could reinvigorate conversations around corporate data sharing, governance.

2. **Utility tokens:** Plans to reshape the web haven't panned out yet, but development continues apace as crypto's bear market flushes out bad actors.

3. **Security tokens:** Security token projects are seeing lots of investment, but could face familiar challenges faced by earlier asset tokenization projects.

4. **Cryptocurrencies:** Blockchain technology's first use case – money – might still be its best one, as stablecoins and second-layers hope to enable adoption.

‘Blockchain’ is different things to different users



Collaborate.

Indian Fintech Ecosystem

burnmark

@Sanjeevk_k