What is Blockchain Technology?

Explaining Bitcoin, Ethereum, ICOs,
and blockchain technology

CBINSIGHTS

WITHIN 24 HOURS

Webinar recording will be distributed

The presentation will also be sent to you. Feel free to share with colleagues. The resolution of some slides may be suboptimal due to the webinar software. Those slides will look fine in the presentation that we send you.

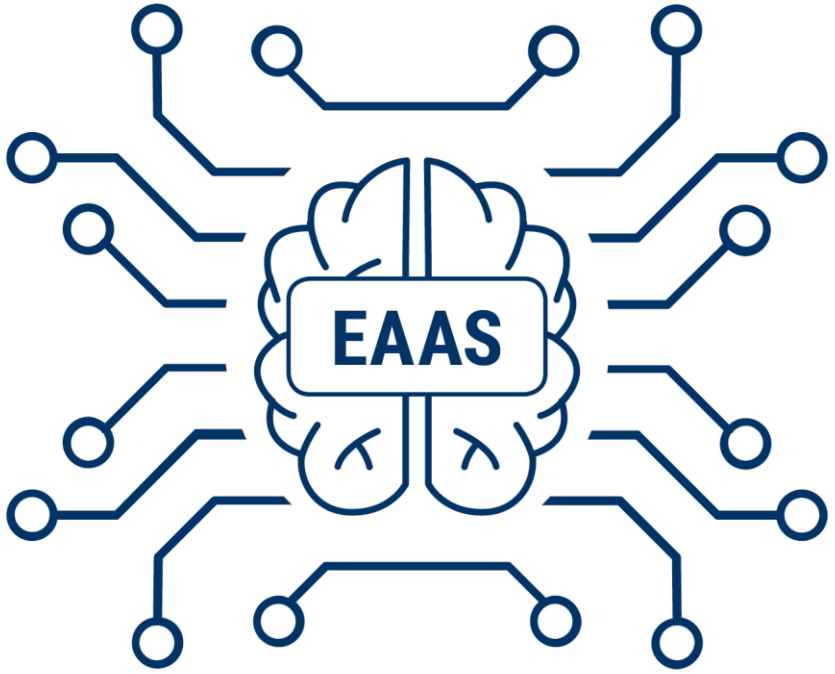
JOIN THE CONVERSATION ON TWITTER

@cbinsights
@arieh313
#CBIBlockchain

WHO ARE WE

The technology market intelligence platform.

CB Insights software lets you predict, discuss, and communicate emerging technology trends using data in ways that are beyond human cognition.



TRUSTED BY THE WORLD'S LEADING COMPANIES

BARRICK citi F-PRIME FIRSTMARK GE IBM NORWEST VENTURE PARTNERS Riviera SEQUOIA

"We use CB Insights to find emerging trends and interesting companies that might signal a shift in technology or require us to reallocate resources."

Beti Cung, Corporate Strategy, Microsoft

Microsoft

FUTURE OF FINTECH

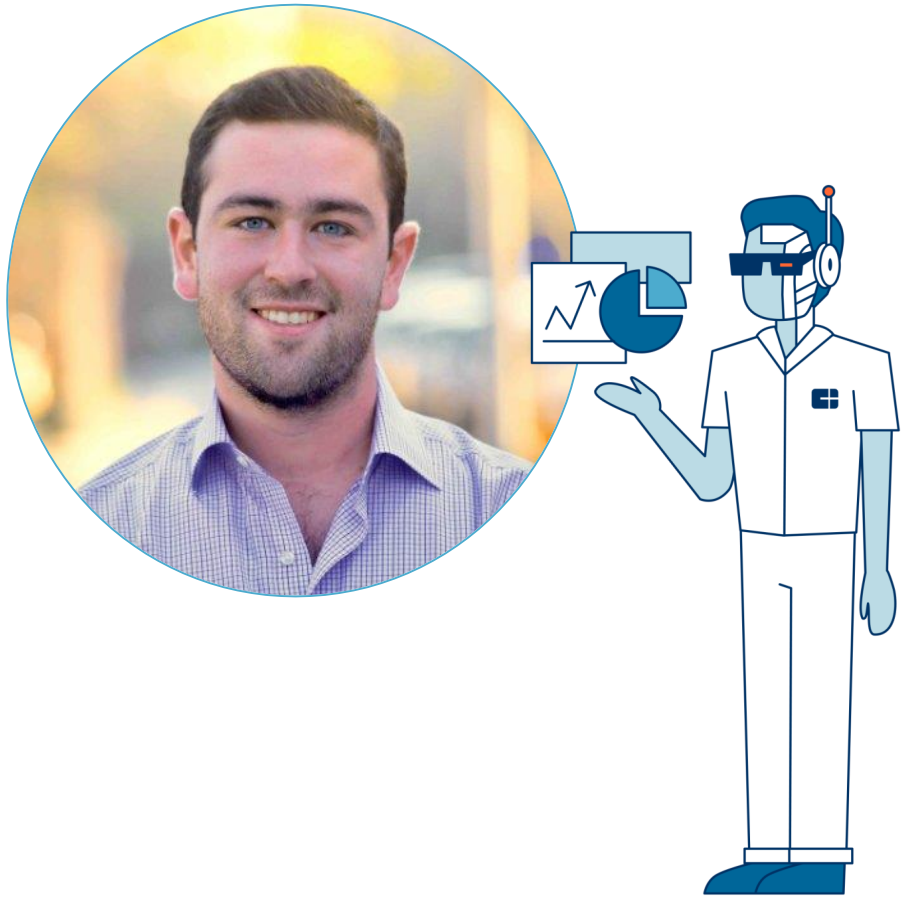
CBINSIGHTS

June 19 – 21, 2018 I NYC, NY

The Future of Fintech is an exclusive gathering of the world's largest financial institutions, best fintech startups, and most active venture investors.

ABOUT THE ANALYST

Arieh Levi



Intelligence Analyst

@arieh313 | alevi@cbinsights.com

Arieh Levi is an intelligence analyst at CB Insights, where he produces data-driven analysis and research reports on trends across emerging industries, geographies, and investors. Arieh focuses on fintech and blockchain technology.

Prior to joining CB Insights, Arieh held roles in healthcare and financial services. Arieh is a summa cum laude graduate of Yeshiva University.

Most popular research:

What Is Blockchain Technology?
Blockchain Investment Trends In Review

Contents

AS OF MID-DECEMBER 2016…

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

AS OF MID-DECEMBER 2017…

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

Bitcoin’s wild ride

BTC/USD average daily price, 12/12/2015 – 12/11/2017

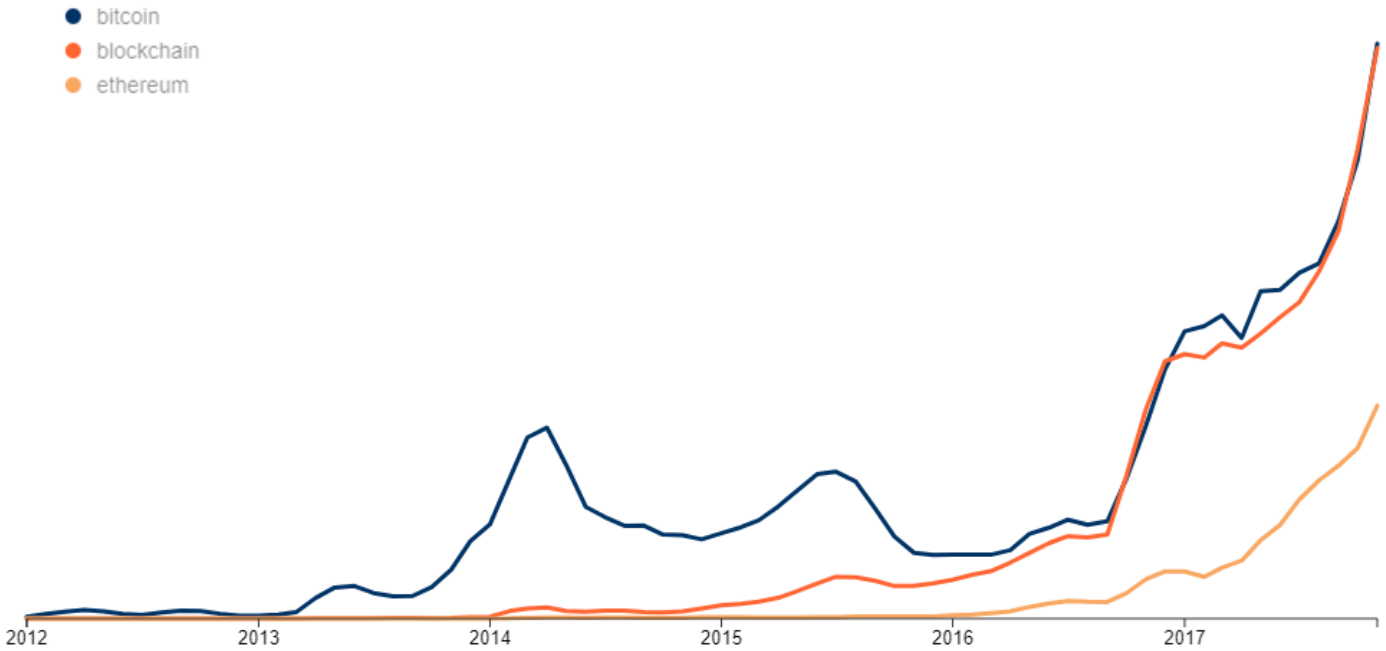
CBINSIGHTS Source: Bitcoinity; Coinbase

Blockchain media interest skyrockets

Blockchain technology took 2017 by storm.

CB Insights media trends analysis

2012 – 2017 (12/13/2017)



CB Insights Trends mines a massive corpus of media articles to enable a data-driven, real-time method to discover, predict, and plot the arc of rising expectations and excitement.

1. What is Bitcoin?

Source: Dilbert

A typical physical transaction

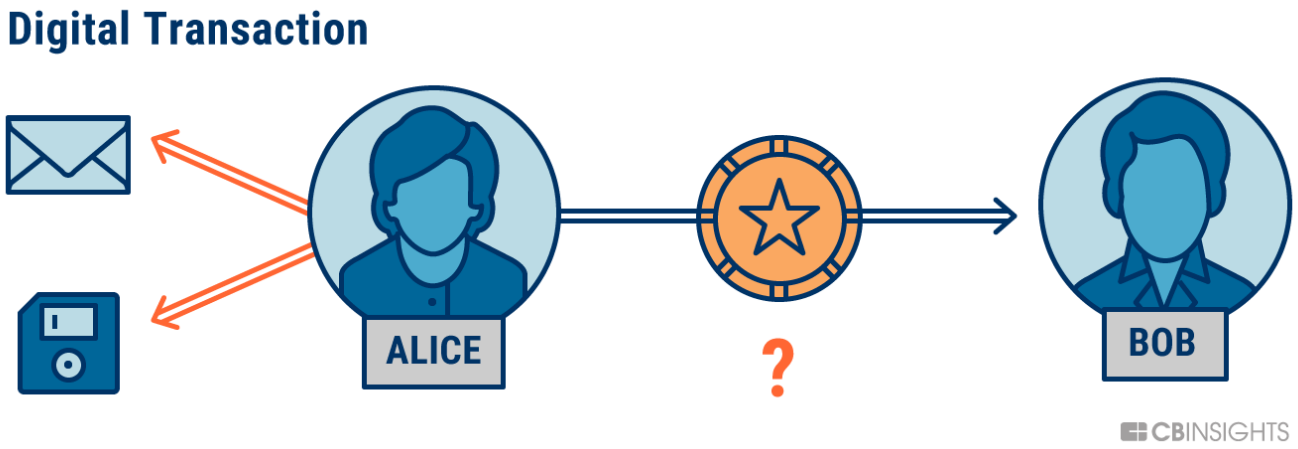
Alice hands Bob a physical arcade token.

Bob now has one token, and Alice has zero. The transaction is complete.

A typical digital transaction…?

Alice sends Bob a digital arcade token — via email, for example.

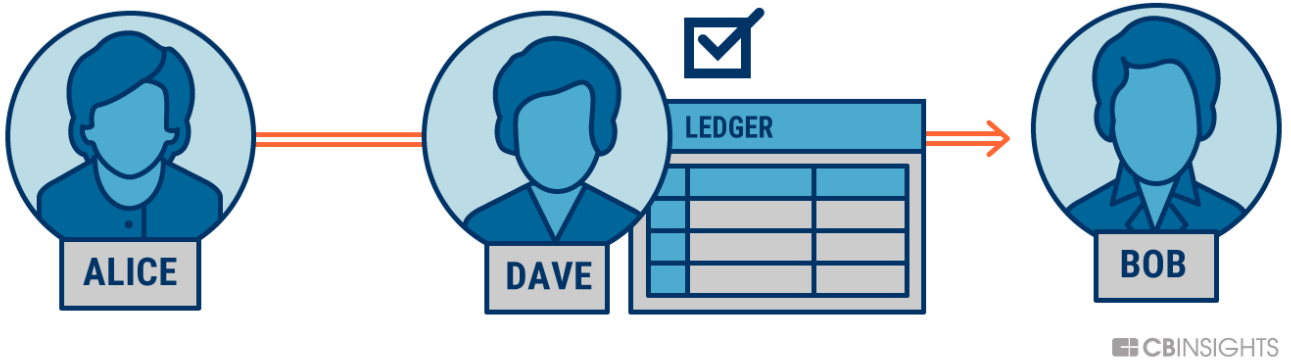
If a digital token is a string of ones and zeros, how can we determine the unique "**owner**" of the digital token?



Let's use a middleman

A trusted third party will record the digital transaction in a database.

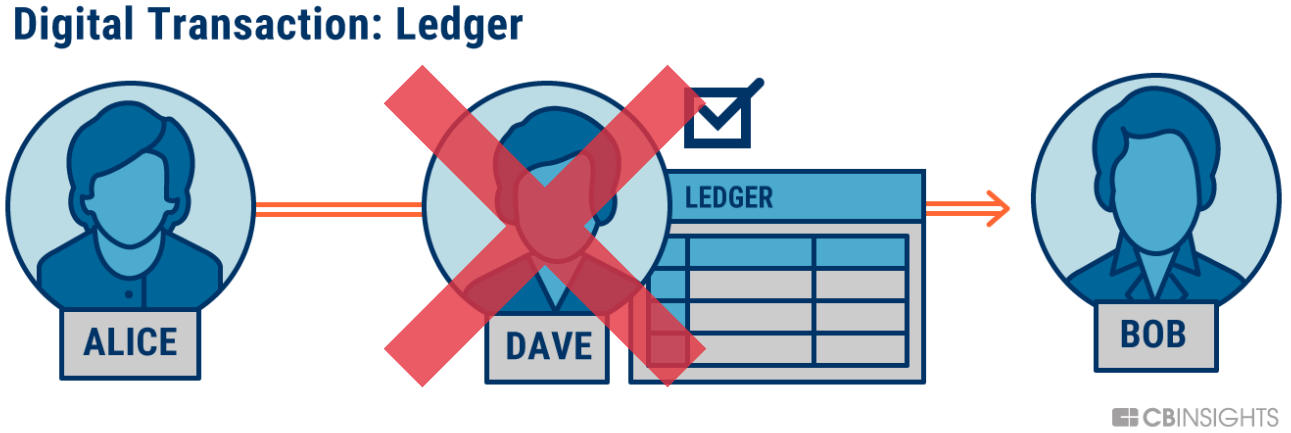
This database — or ledger — will track a single asset: digital arcade tokens. This ledger is now the "source of truth."



What if we can't trust the middleman?

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

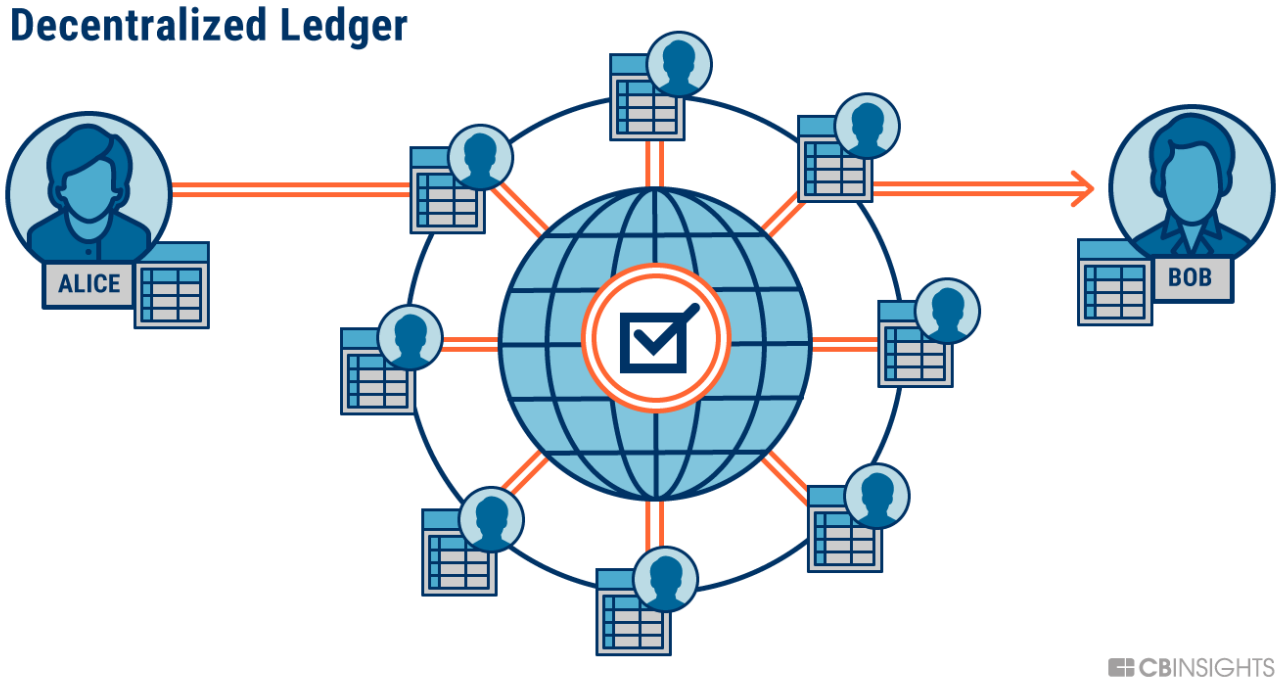
In other words — what happens when Alice and Bob **cannot trust the trusted third party**?



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**.



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.

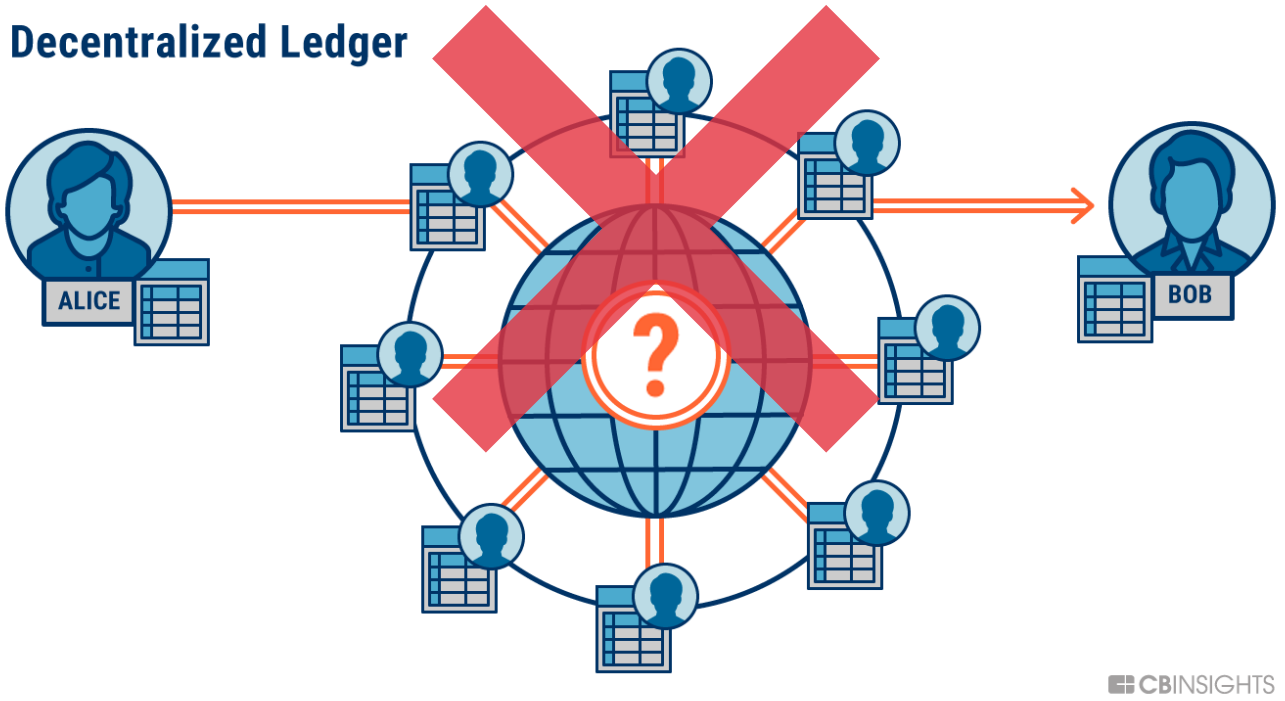
2. This ledger's unit of account is "**bitcoin**." Bitcoin's rules state that there will only ever be 21 million bitcoin.

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

What if we gave this database to everyone?

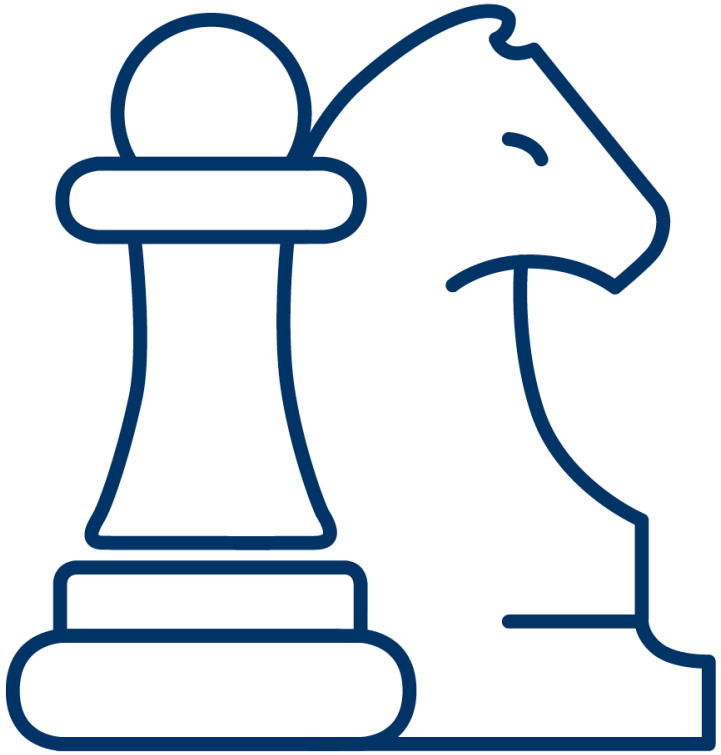
Our “arcade token” ledger only allowed “trusted friends” to participate.

In contrast, **Bitcoin is entirely public, and anyone can participate**.



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

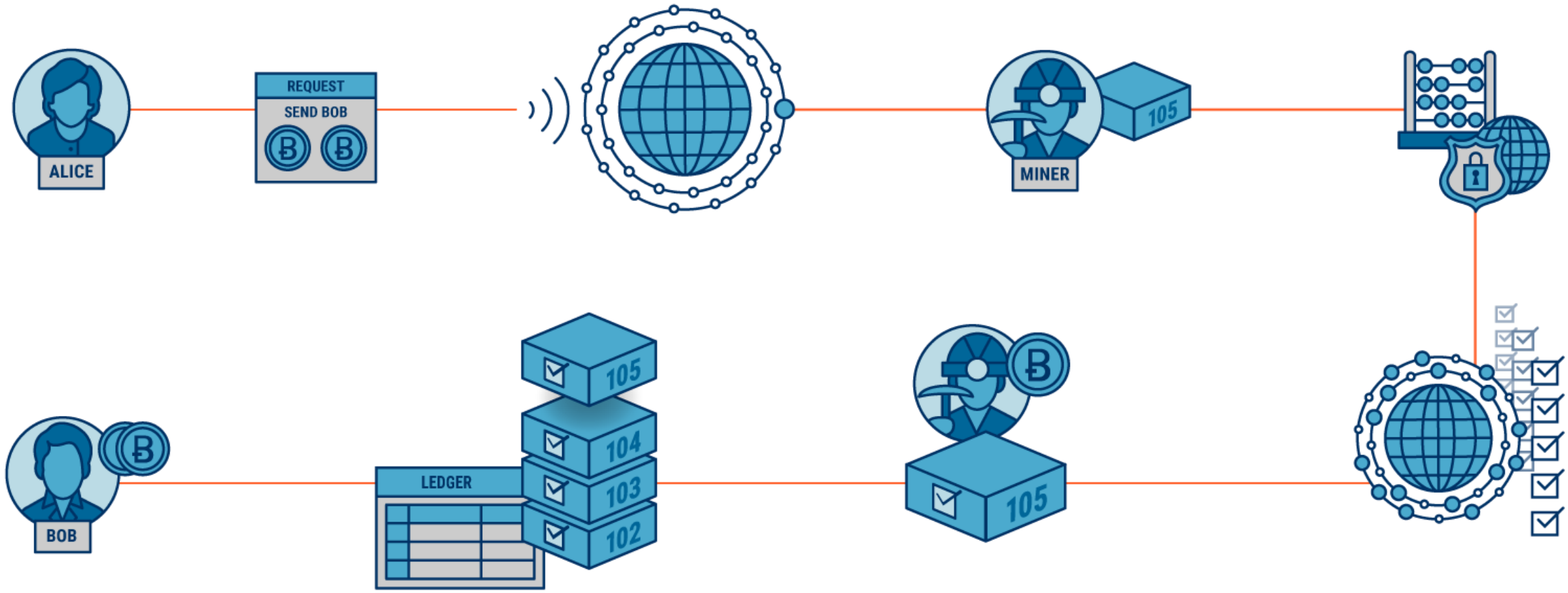
Bitcoin is secured through clever incentives



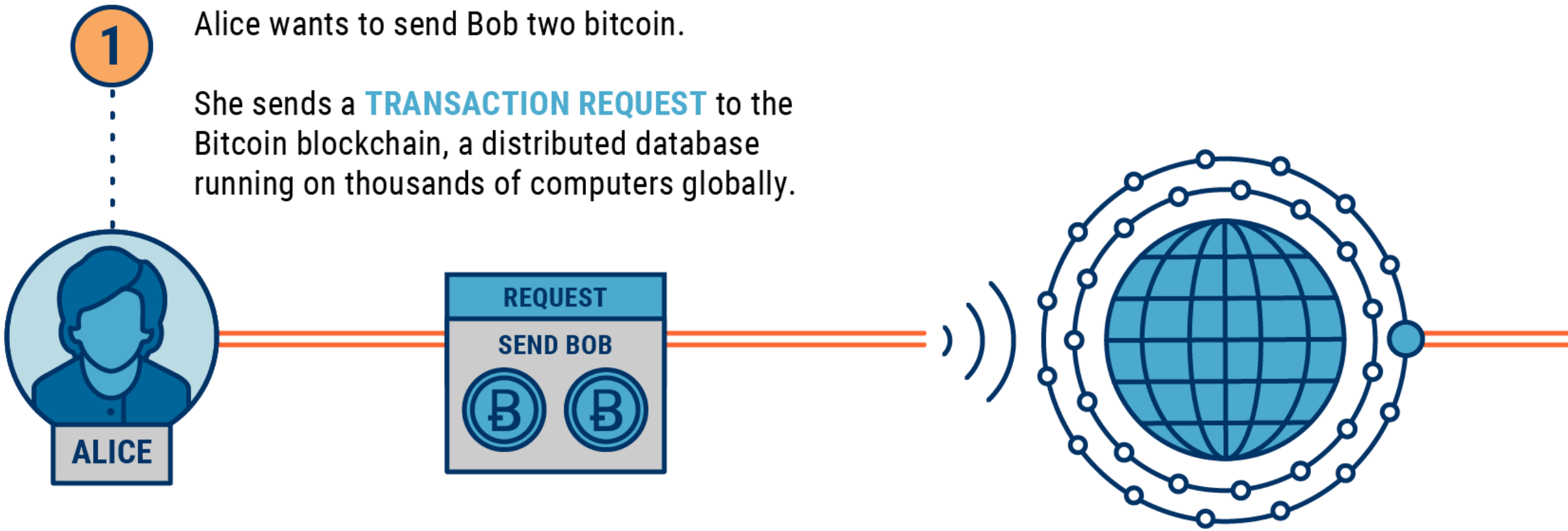
1. **CARROT:** Monetarily reward participants (“miners”) for maintaining and securing the ledger

2. **STICK:** Monetarily punish bad actors for attacking the ledger

Understanding a bitcoin transaction



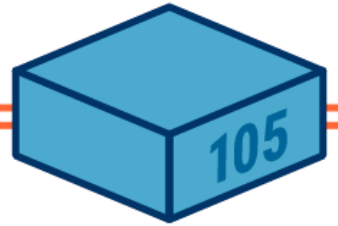
Understanding a bitcoin transaction



Understanding a bitcoin transaction

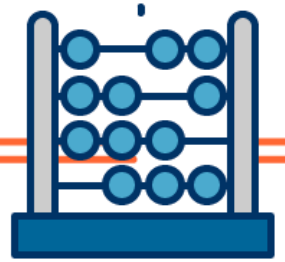
2

Computers known as **MINERS** verify this transaction (e.g. check Alice's balance) and compete to place it into a **BLOCK** with other transactions.



3

To append a block to the chain of prior blocks (hence: "blockchain"), miners solve a **MATH PUZZLE** that requires a lot of computational power to solve.

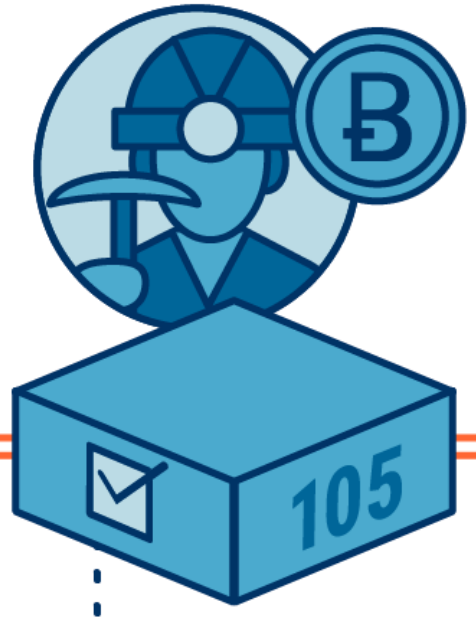


All this computational power **PROTECTS THE BLOCKCHAIN** against hackers — it would be difficult and expensive to falsify transactions or attack the network.

Understanding a bitcoin transaction

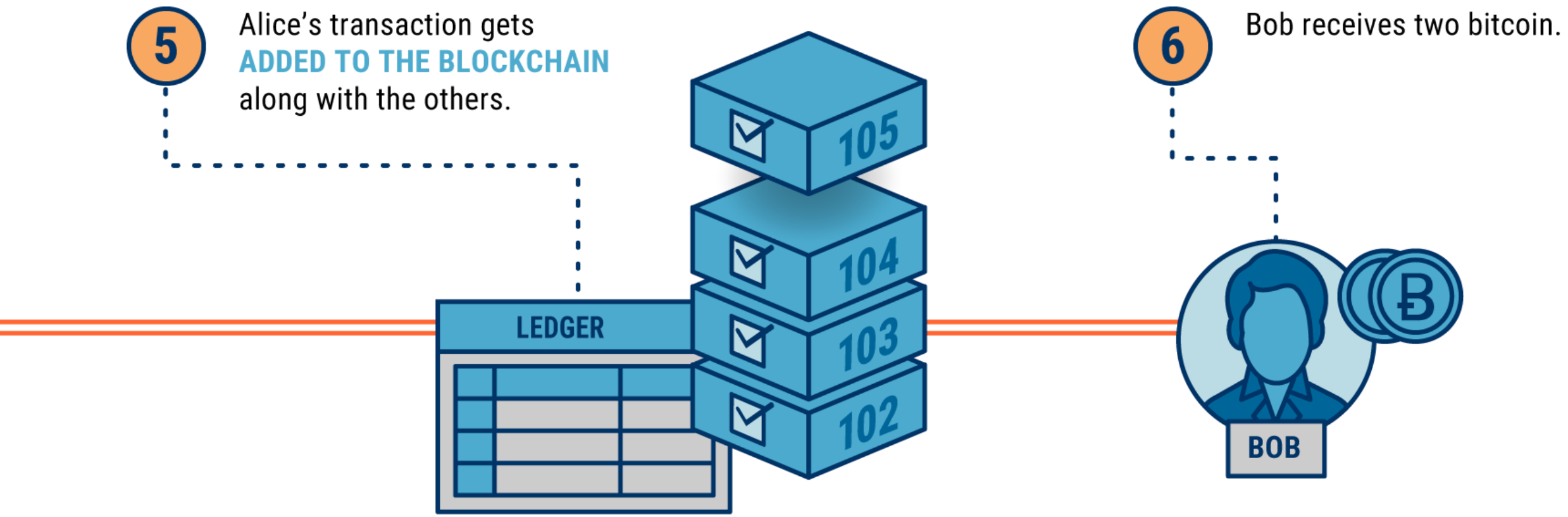
4

Others in the network check the miner's work.

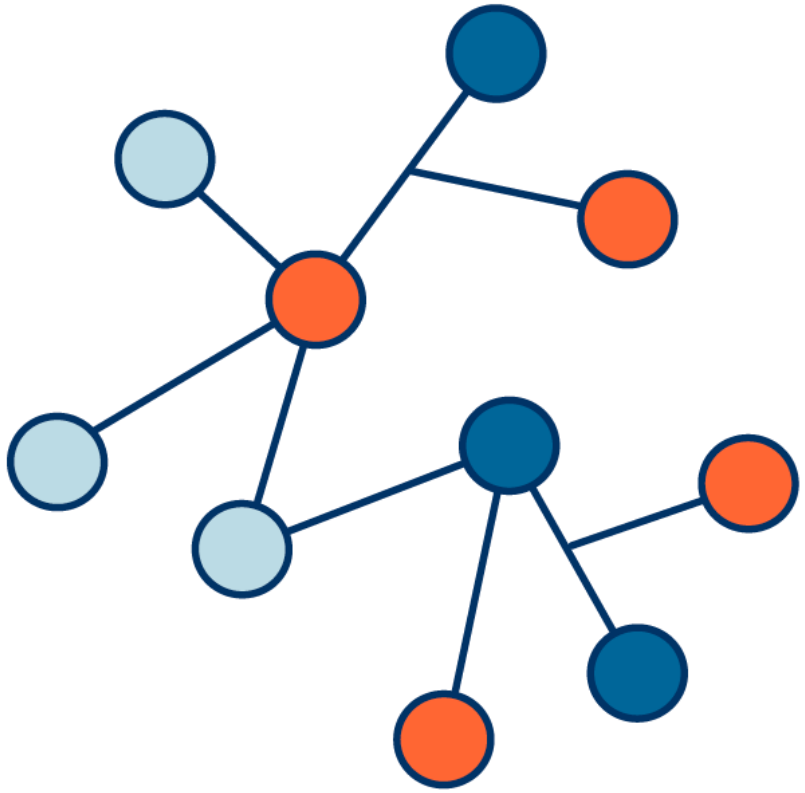


Once the answer is **VERIFIED** – when a majority of miners in the network approve the block – the miner who solved the puzzle gets paid in bitcoin.

Understanding a bitcoin transaction



Wait… what is Bitcoin?



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

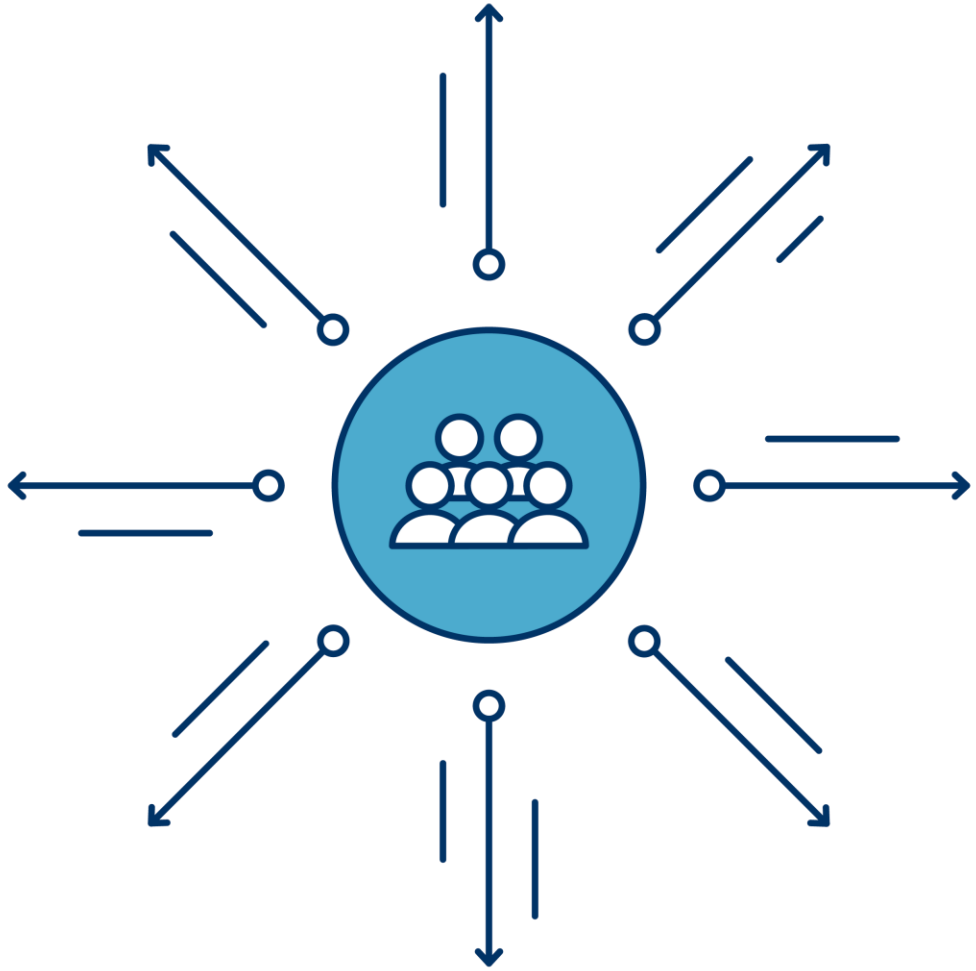
2. This ledger's unit of account is "bitcoin." Bitcoin's rules state that there will only ever be **21 million bitcoin**.

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

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?



LET'S REPLACE THE WORDS

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

Select blockchain use-cases

Where else could a “shared digital history” bear fruit?

IDENTITY

civic

CRYPTID

iD 2020

uport

SUPPLY CHAIN

Sweetbridge

origintrail

T-MINING BLOCKCHAIN LOGISTICS

CHRONICLED

CONTENT ATTRIBUTION

UJO MUSIC

po.et

MYCELIA

JAAK

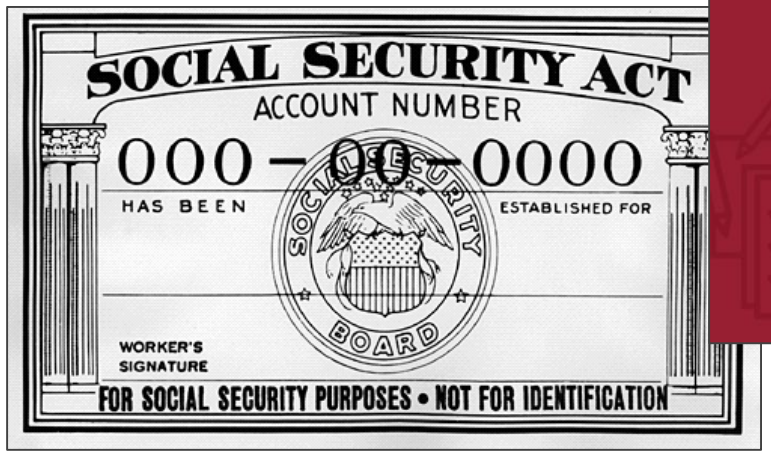
The promise of user-controlled identity

civic

iD 2020

CRYPTID

uport



Companies are using blockchain technology to allow users to control their own identities.

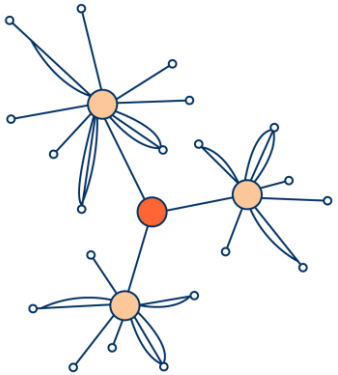
In a not-too-distant future, this might allow users to grant and revoke access on a case-by-case basis.

Blockchain technology in healthcare

DATA SECURITY

Blockchain technology could enable patient-owned records, giving the patient control to grant and revoke data on an as-needed basis.

INTEROPERABILITY



A single distributed EMR system could replace siloed data across different hospitals and medical facilities.

REIMBURSEMENT

Blockchain technology might enable instantaneous insurance claims verification and fulfillment of prior authorization requests.

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

Blockchain technology faces technical obstacles

What does it take to scale?

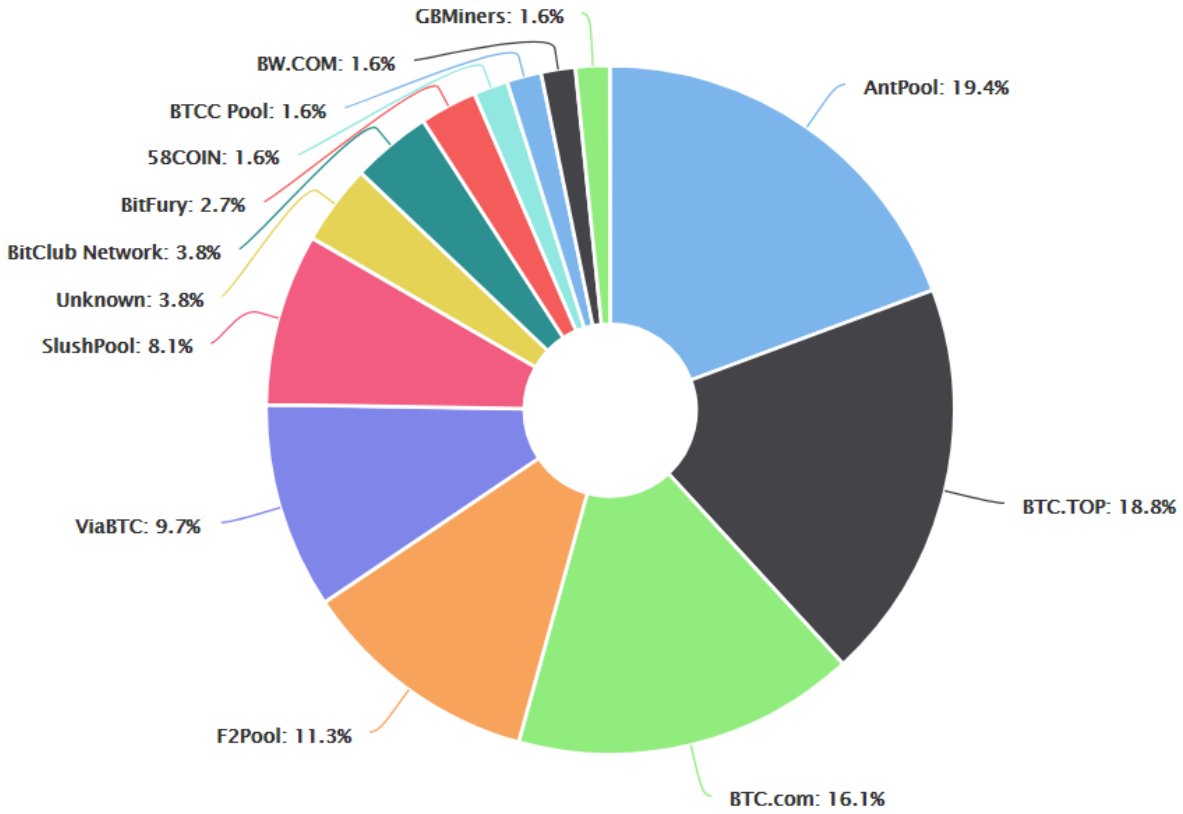
LEDGER STORAGE SIZE

TRANSACTION SPEED

MINERS TOO POWERFUL

Mining centralization

Data for Bitcoin blocks mined on 12/13/2017



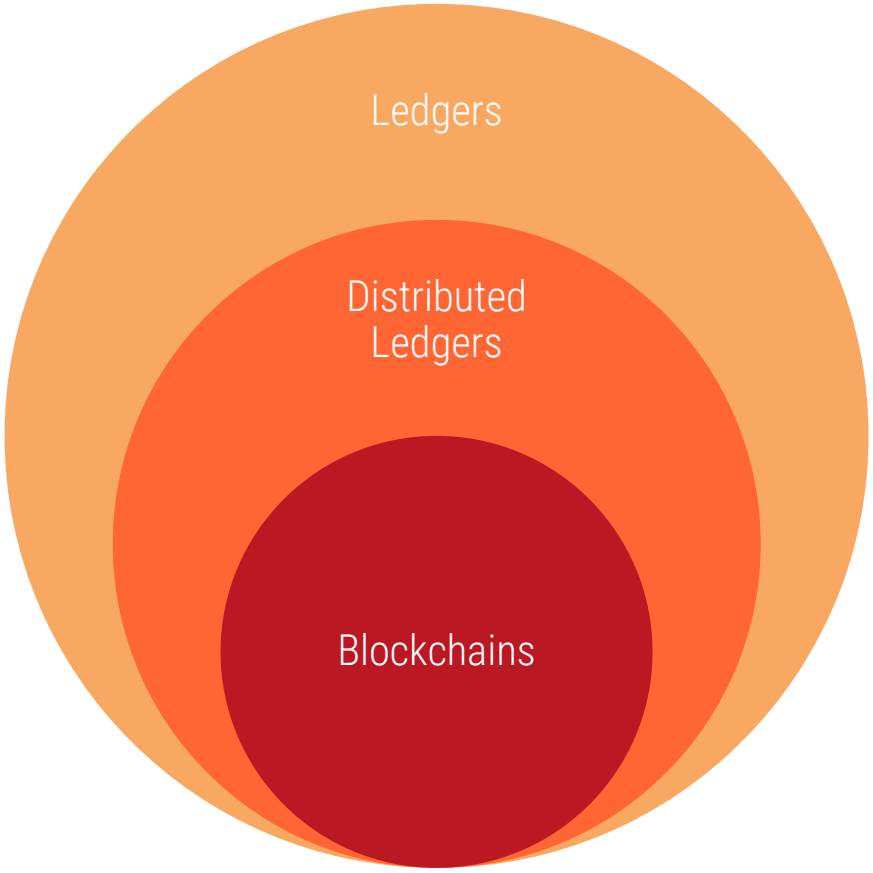
CBINSIGHTS Source: Blockchain.info

Blockchain technology solves a specific problem

Blockchain technology makes sense when:

1. Everyone needs a record of ownership

2. A 3rd party isn't trusted to administer this record

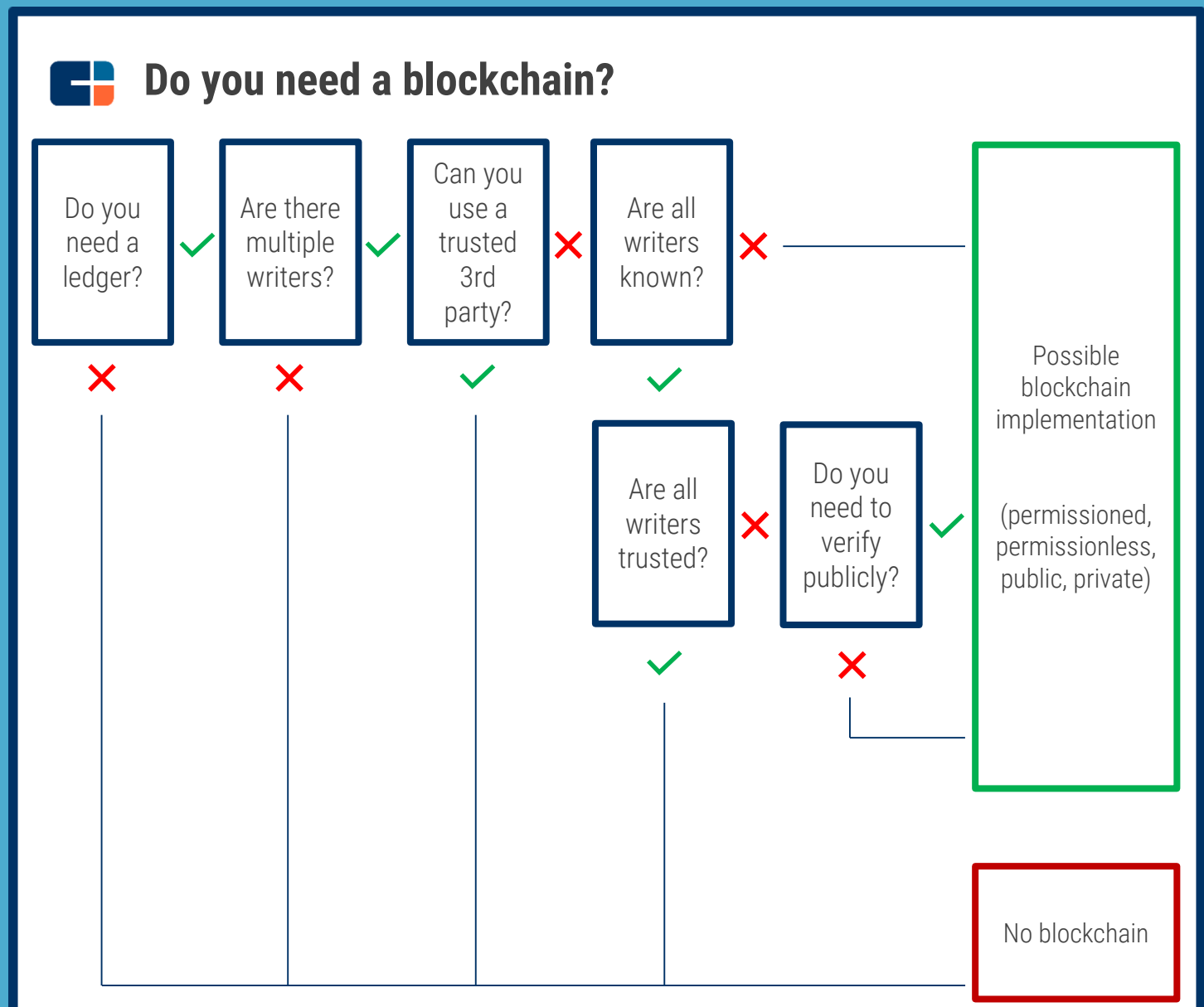


Source: Tim Swanson

Distributed ledger technology as an alternative

If a trusted 3rd party could administer the ledger, then a blockchain would be unwieldy, slow, and a poor solution.

Distributed ledger technology (DLT) might be better suited for many business use cases.



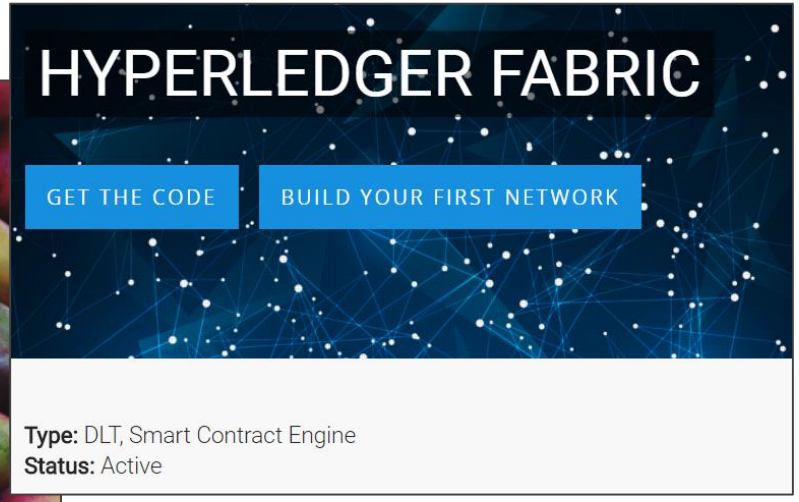
Source: doyouneedablockchain.com

The DLT alternative: powering food safety

Walmart

HYPERLEDGER

IBM



Walmart and IBM successfully tested a pilot of Hyperledger Fabric's DLT to quickly track food through the supply chain.

One immediate implication is for food-borne illnesses — with DLT, it becomes easier to launch investigations and recall products.

Far-ranging use cases

Blockchain and distributed ledger technology is being explored across verticals, from capital markets, to healthcare, to media.

Blockchain and distributed ledger market map

WALLETS & MONEY SERVICES

BLOCKCHAIN, bitpay, coins.ph, case, uphold, NETKI, coinplug, wyre, SNAPCARD, Streami, xapo, ripio, CIRCLE, ABRA, COINJAR, Ledger

EXCHANGES & CRYPTOCURRENCY TRADING

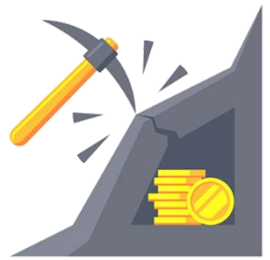
coinbase, Tech bureau Corp., BTCChina, KORBIT, BITKAN, Polychain Capital, QUOINE, kraken, BITSTAMP, bitt, PAYMIUM, BITSO, bitaccess, coinsecure, crypto facilities, LUNO, bitFlyer, SHAPE SHIFT, BKCoin, Unocoin

P2P MARKETPLACES & P2P LENDING

Atlas, OpenBazaar, BTCjam

MERCHANT SERVICES

POSaBIT, Coinify, Purse, BitPesa, bitWAGE, loyyal, simplex, billon, BitGo, Align Commerce



ENTERPRISE SERVICES & CURRENCIES

Gem, 区块链数字资产平台, 小蚁 AntShares, blocko, FACTOM, orb, BIGCHAIN DB, HASHED HEALTH, BLOCKCYPHER, colu.

SOCIAL & BROWSERS

brave, Reveal, blockstack

CRYPTOCURRENCY MINING

HASHRABBIT, BitFury

IoT, IDENTITY & CONTENT MANAGEMENT

BITMARK, mediachain, SatoshiPay, FILAMENT, ShoCard, evernym, Cambridge Blockchain, CHRONICLED, ascribe

STORAGE, SECURITY & REGULATORY

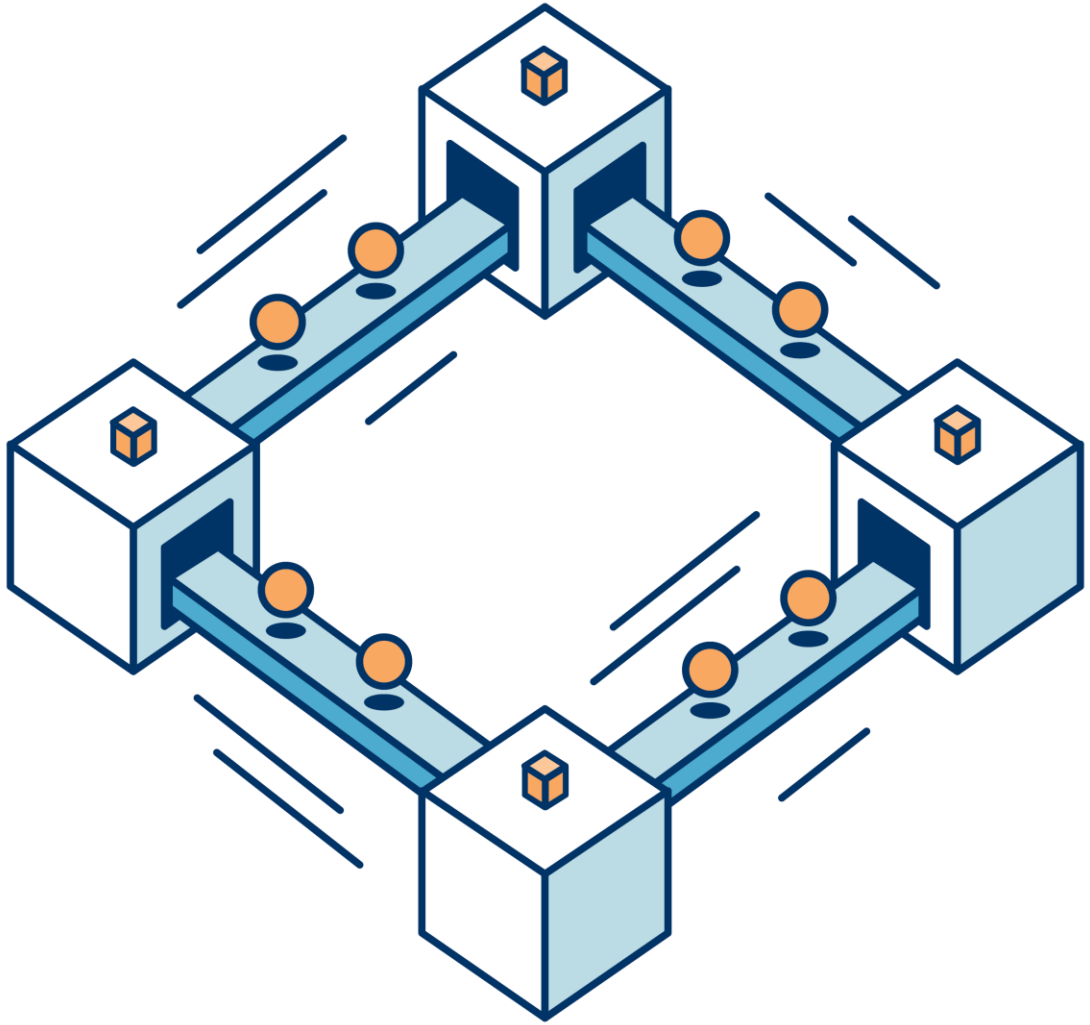
Skry, CHAINALYSIS, ELLIPTIC, STORJ

CAPITAL MARKETS & FINANCIAL SERVICES

ripple, symbiont, PEERNOVA, LedgerX, Chain, Hijro, Blockstream, Digital Asset Holdings, JU 矩阵金融 JUZHEN.IO, AXONI, SOLIDX, DIGITAL CURRENCY GROUP, PAXOS, SETL, funderbeam, NEUFUND, CRYEX

CBINSIGHTS

3. What is Ethereum?

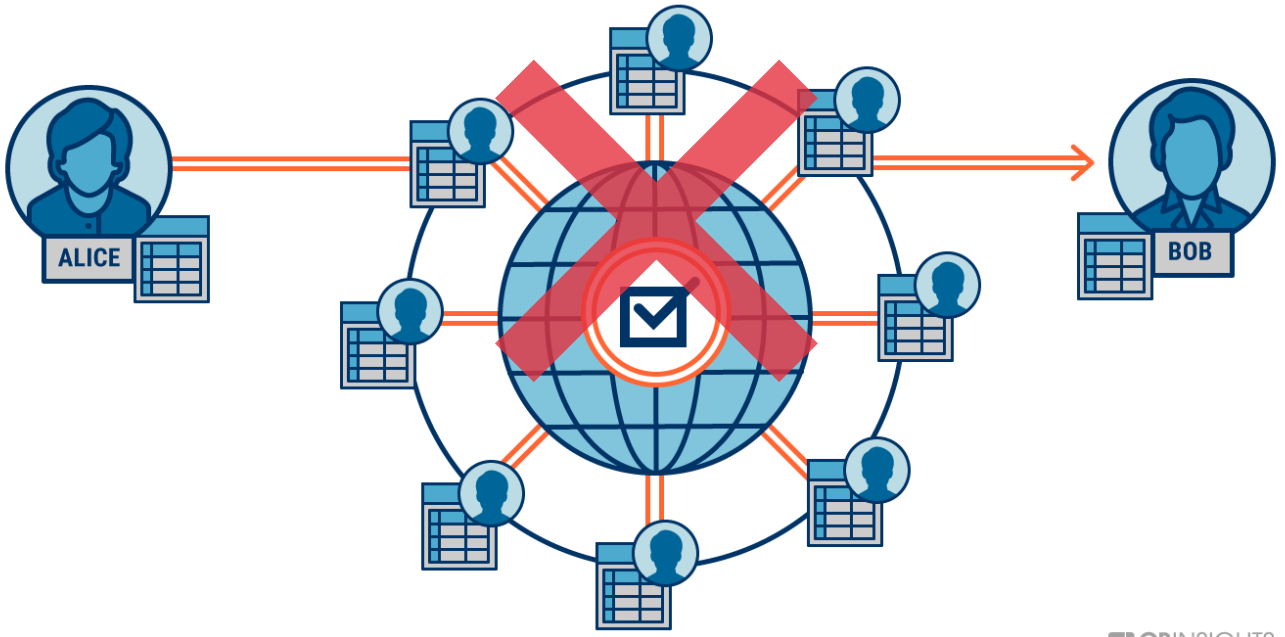


If Bitcoin is a decentralized ledger for **payments**, then Ethereum is a decentralized computer for **applications**.

Can we do more with blockchains?

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?

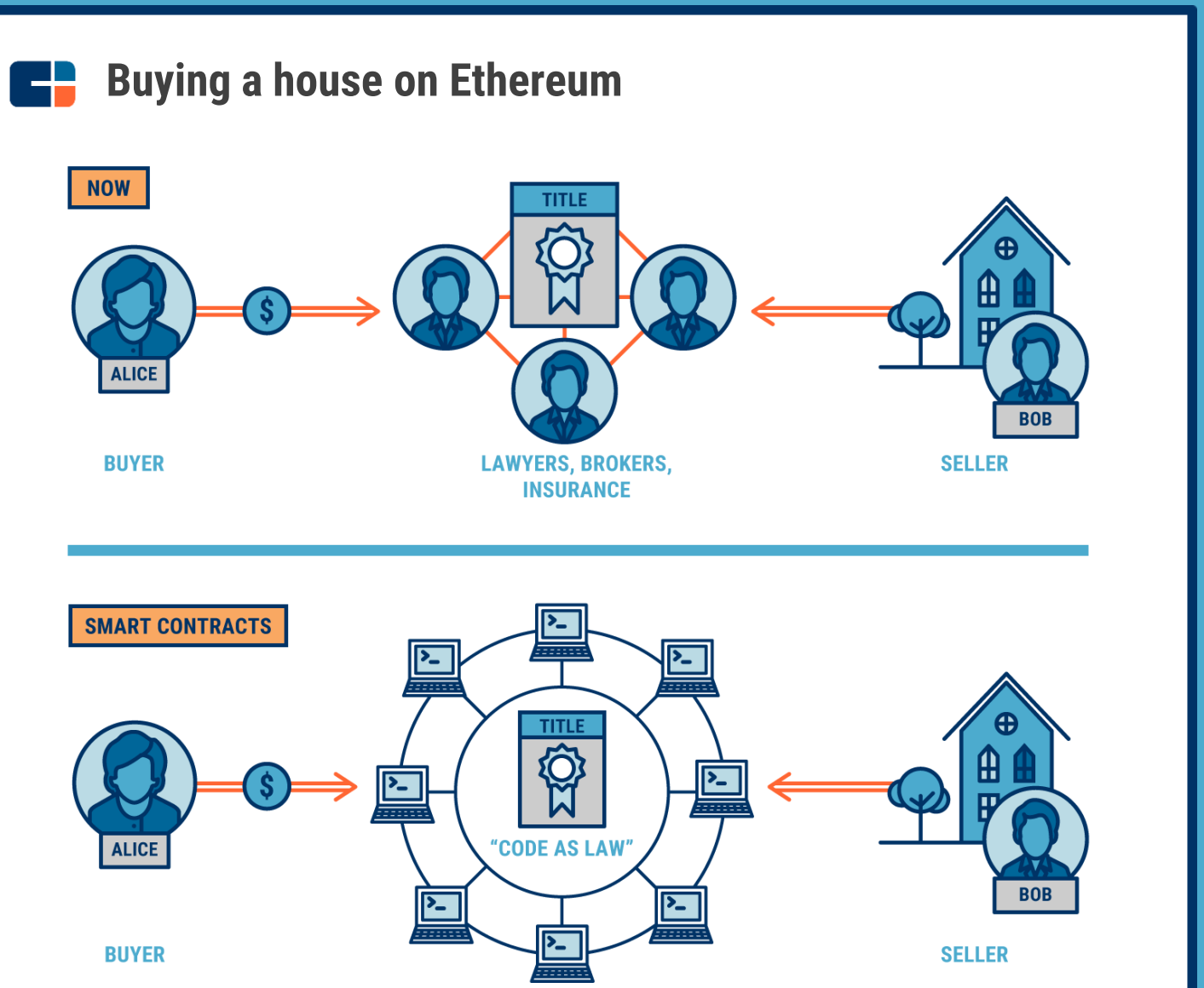


Ethereum does more with ‘smart contracts’

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**.

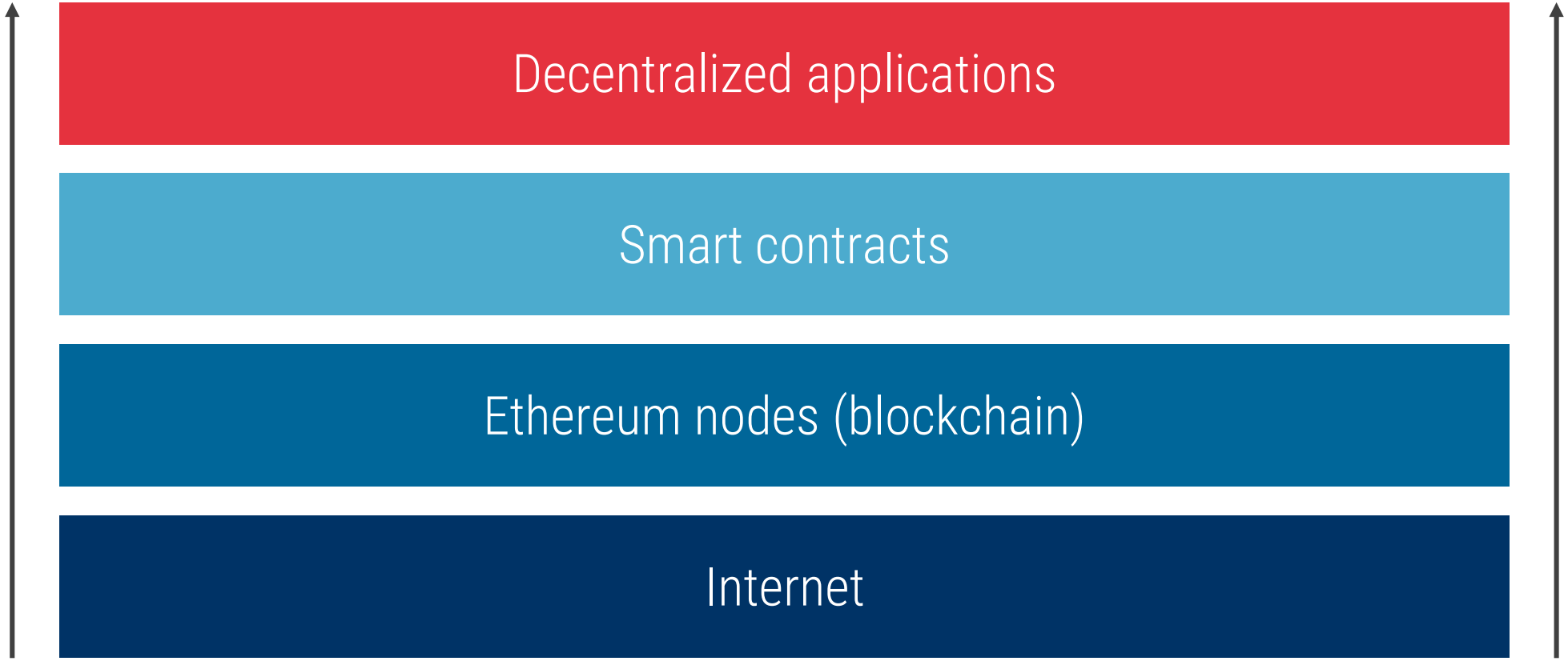
This enables counterparties to build **decentralized applications**.



2ND GENERATION BLOCKCHAIN

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

The Ethereum development stack



Cats: An Ethereum case study

CryptoKitties is a **decentralized application** that uses the Ethereum blockchain to create collectible, digital cats.

Smart contracts determine each cat's unique appearance.

The Ethereum blockchain tracks **ownership** of these "tokens," or digital cats.

What's the big deal?

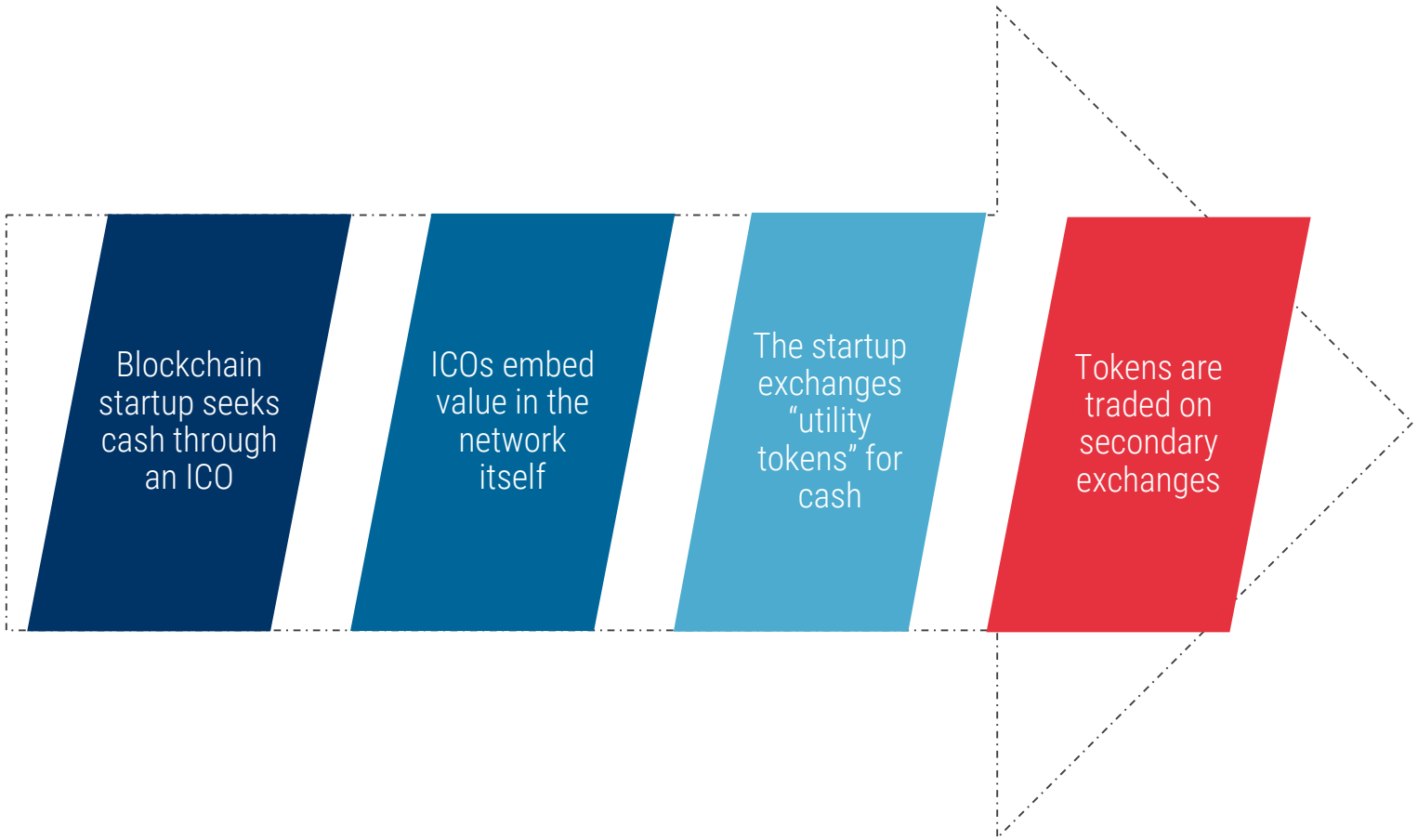
CryptoKitties is one of the world's first games to be built on blockchain technology —the same breakthrough that makes things like Bitcoin and Ethereum possible. Bitcoin and ether are cryptocurrencies but CryptoKitties are cryptocollectibles. You can buy, sell, or trade your CryptoKitty like it was a traditional collectible, secure in the knowledge that blockchain will track ownership securely.

Source: Cryptokitties.co

4. What are initial coin offerings?

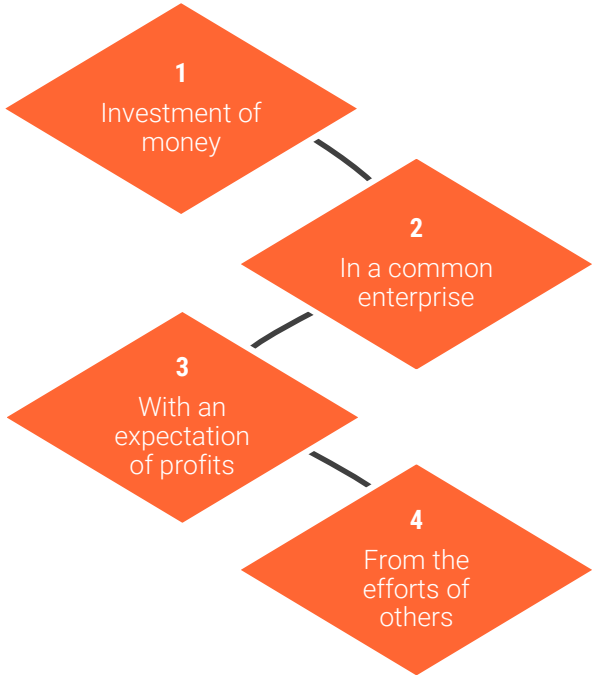
An initial coin offering (ICO) is when a company sells **tokens** to the public. Just like bitcoin or ether, these tokens provide **utility within the network**.

How do ICOs work?



Is your token a security?

The Howey Test



TOKENS START TO REPLACE VC

"We have a good thing going with the equity-based model, but we understand that we have to adapt and react to changes in the market, and **we are doing that, fairly aggressively, with tokens**."

Fred Wilson

Co-founder & Managing Partner, Union Square Ventures

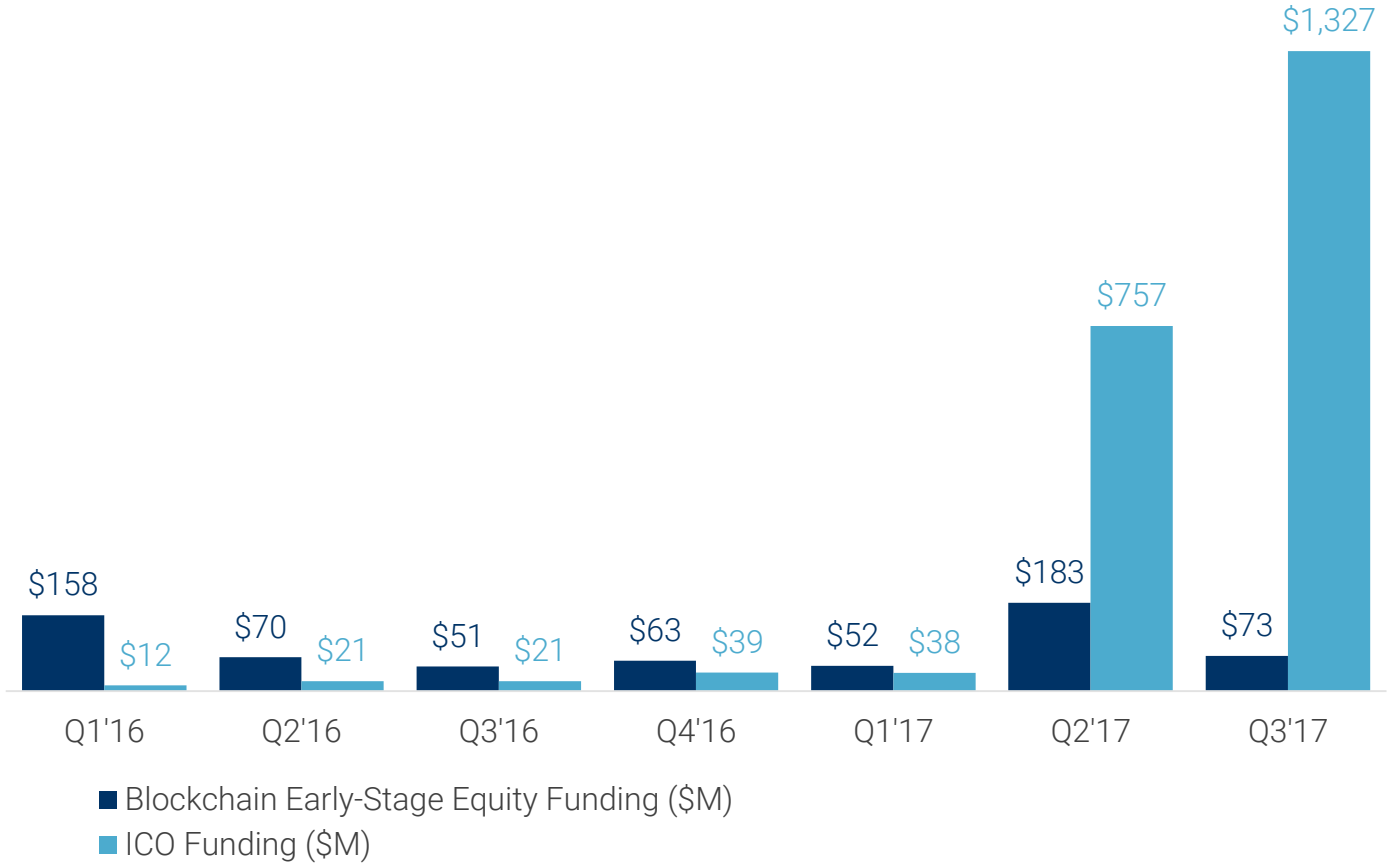
Tokens challenge the status quo

ICO funding roars past early-stage equity funding

"Token logic" is louder than concerns over incentives and over-capitalization, as companies opt for the new financing mechanism instead of traditional VC.

Blockchain early-stage equity funding vs. ICOs

Q1'16 – Q3'17



Note: "Blockchain Early-Stage Equity Funding" includes angel, seed, and Series A funding
Sources: CB Insights, TokenData, CoinSchedule

Conversation shifts, as ICOs take spotlight

Blockchain investment trends have moved over time — first from bitcoin to blockchain, and now from blockchain to **crypto**.

Blockchain companies funded via ICOs

Closed initial coin offerings, Q1'14 – Q3'17

Note: ICO data sourced from TokenData.io. Map is illustrative, not exhaustive

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.

FURTHER READING:

What Is Blockchain Technology?
What is Ethereum?
Blockchain Investment Trends In Review

WHERE IS ALL THIS DATA FROM?

The CB Insights platform has the details on all the information included in this report

CLICK HERE TO SIGN UP FOR FREE

Questions?

@cbinsights
@arieh313
#CBIBlockchain

cbinsights.com

@cbinsights