CBINSIGHTS

EMERGING TRENDS

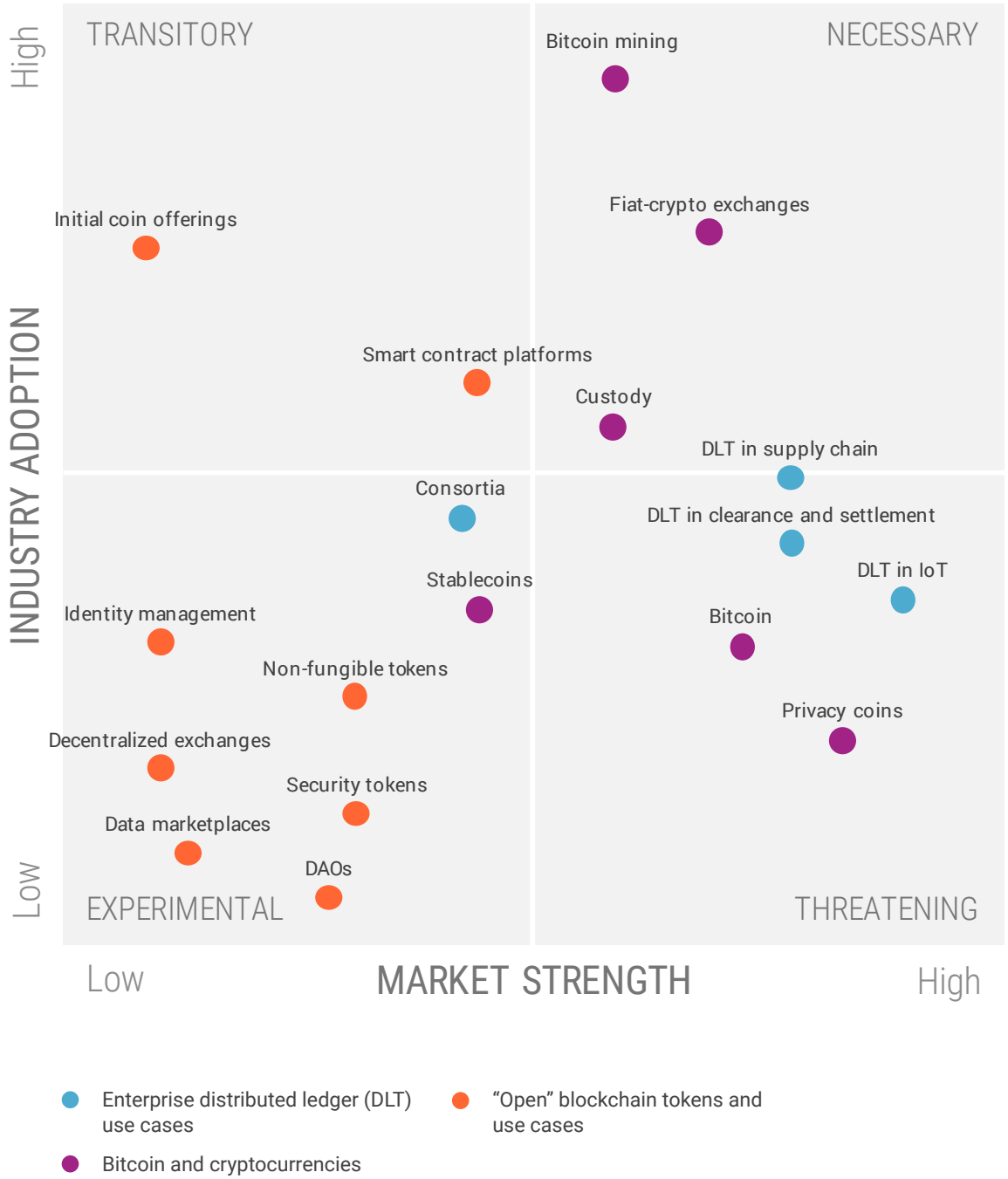
What's Next In Blockchain

2019

Table of Contents

NExTT FRAMEWORK

Emerging Trends in Blockchain Technology



NExTT Trends

We evaluate each of these trends using the CB Insights NExTT framework.

The NExTT framework educates businesses about emerging trends and guides their decisions in accordance with their comfort with risk.

NExTT uses data-driven signals to evaluate technology, product, and business model trends from conception to maturity to broad adoption.

The NExTT framework's 2 dimensions:

INDUSTRY ADOPTION (y-axis): Signals include momentum of startups in the space, media attention, customer adoption (partnerships, customer, licensing deals).

MARKET STRENGTH (x-axis): Signals include market sizing forecasts, quality and number of investors and capital, investments in R&D, earnings transcript commentary, competitive intensity, incumbent deal making (M&A, strategic investments).

Necessary

FIAT-CRYPTO EXCHANGES

As crypto prices fall and financial services incumbents wade in, exchanges are looking for cryptocurrency use cases to drive additional revenue streams.

For most people, their first purchase of cryptocurrency begins at an exchange. “Fiat-crypto” exchanges allow speculators, investors, and crypto enthusiasts to trade fiat currencies like the US dollar or euro for cryptocurrencies like bitcoin or ethereum. By enabling trade in and out of fiat currencies, exchanges act as “on-ramps,” bridging the worlds of cryptocurrencies and more traditional finance.

Among the many exchanges, Coinbase has emerged as the most popular in the US. It recently raised at an $8B valuation and has seen repeat venture investments from top investors.

Still, exchanges, which generate money from transaction fees, have seen their respective revenues fall quarter-over-quarter as speculative trading has slowed. To remain competitive, exchanges are listing additional cryptocurrencies, launching new trading products (especially for larger, institutional investors), and investing out of newly-formed venture arms.

Exchanges are still looking for token use cases

Entering 2019, major crypto-fiat exchanges will have to fend off competition from larger, more traditional players. For example, the Chicago Board of Options and Exchange (CBOE) now offers bitcoin options, and ICE (owner of the NY Stock Exchange) is planning to launch bitcoin futures next year.

The question looms: will big financial firms take over from here, or will independent exchanges retain their market share? And perhaps more importantly, will fiat-crypto exchanges find a business model that doesn't rely exclusively on speculation to drive revenues? The answer may lie in whether exchanges can help enable broader use cases for this new asset class beyond pure speculation.

BITCOIN MINING

Mining companies are facing increased competition and decreased demand, but substantial cash-on-hand should give them runway.

It is not surprising that bitcoin mining players like Bitmain are the first blockchain companies looking to go public. After all, the biggest winners of 2018's crypto gold rush were the picks and shovels: mining companies and exchanges.

However, mining companies are now facing rising competition, mounting environmental concerns, and declining demand.

In terms of competition, crypto-focused players are raising funds to build better chips. In September, Bitewei raised $20M to build mining hardware that is "30% more efficient." Bitewei's CEO is the former director of design at Bitmain, perhaps the largest global Bitcoin mining chip designer.

Incumbent chip manufacturers are also making their first forays into the sector. In November, GPU manufacturer AMD announced the launch of eight mining rigs in conjunction with manufacturers.

Environmental criticisms are also hurting miners' bottom lines. Bitcoin uses a "proof-of-work" consensus mechanism to secure its blockchain, which requires a lot of energy. To lower energy costs (and environmental effects), developers are building other consensus mechanisms.

Chief among these alternative consensus mechanisms is "proof-of-stake." Proof-of-stake requires users to wager that their version of the blockchain is correct, and could eliminate the need for power-hungry mining rigs. If more blockchains opt to use proof-of-stake to achieve consensus, mining companies could see lost revenues.

Bitcoin mining rig.

Last, declining speculation has led to declining demand for mining equipment. According to Bitmain's IPO documents, the company recorded a significant loss in Q2'18, with inventory write-downs of $350M+ and falling profit margins.

Mining companies are expanding into other sectors to stay relevant. In November, bitcoin mining giant Bitfury raised $80M to expand into "adjacent markets" like artificial intelligence, and Bitmain has also said that it's looking to AI as an area of expansion.

Altogether, these challenges signal that mining is both a mature sub-sector and a profitable one. Although the years ahead could prove challenging for mining incumbents, their war chests (due in no small measure to this past year's boom-and-bust) should help them in their second acts.

CUSTODY

To fully enter the crypto space, financial institutions must figure out how to hold and secure cryptoassets.

While large financial institutions have expressed interest in enabling cryptocurrency investment, a recurring challenge is "custody," or the ability of financial institutions to hold cryptocurrencies on behalf of trading clients.

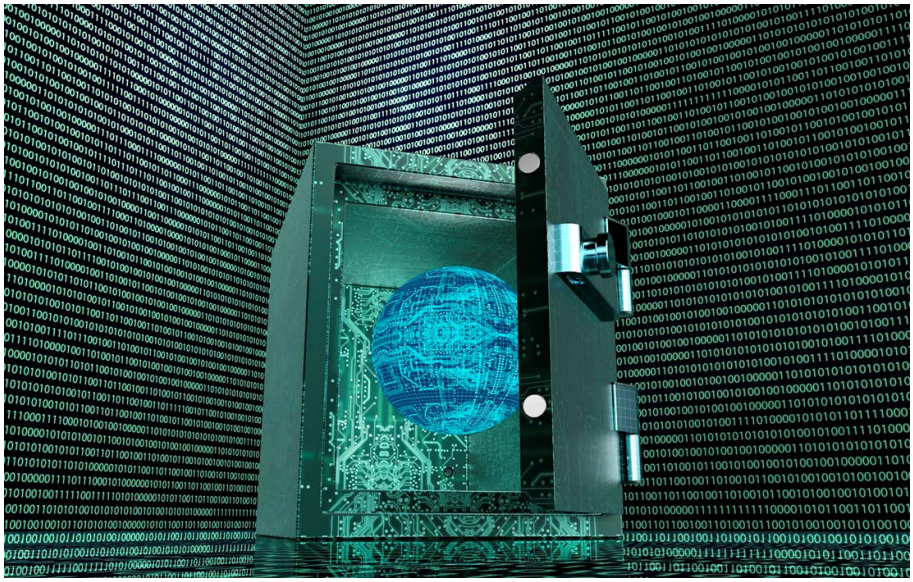
An early bitcoin paper wallet, which includes the "public address" and "private key." Source: BitcoinPaperWallet.com.

Creating custodial solutions for cryptocurrencies is a deceptively difficult problem.

Bitcoin and other cryptonetworks generally work like a digital safe deposit box — access is controlled by a private key (a long string of numbers that allows an owner to access their crypto holdings). Anyone with access to the "private keys" — the owner, a bank, or a hacker — has total control. Handling this at scale mean banks must go to great technical lengths to keep private keys in the right hands.

Some companies solve this problem by offering offline “cold storage” solutions. Xapo, a bitcoin-only exchange and storage service, operates inside a decommissioned Swiss military bunker to protect users’ coins and keys. The ultra-secure site has steel doors that can resist a nuclear blast and uses methods to prevent electromagnetic pulse (EMP) attacks.

Of course, most Wall Street banks don’t guard their clients’ assets in military bunkers. Indeed, in a report on the sector, Morgan Stanley pointed to major obstacles preventing large-scale investment in the crypto space, including a lack of custodial solutions.



The tide, however, may be turning. Fidelity, which has over $7T under administration, recently launched a digital asset arm to handle custody services in-house. In its announcement, the asset manager said it’s “a first step in a long-term vision” and cited findings that 70% of finance executives think cryptocurrencies will be part of the future of finance.

As more VCs, hedge funds, and traditional players in finance look to gain exposure to cryptocurrencies, they will need access to custodial infrastructure. For cryptocurrencies to “cross the chasm” and see mainstream adoption, it will likely require trusted blue-chip firms to stamp their approval on custodial tools.

Experimental

DECENTRALIZED EXCHANGES

Can decentralized exchanges operate in tandem with US securities regulations?

Today's major exchanges such as Coinbase or Binance are typically centralized companies, incorporated and compliant with federal and state regulations. These hubs for buyers and sellers serve as on-ramps to crypto, and they charge fees for their services.

A new set of companies, dubbed "decentralized exchanges," plan to use blockchain technology to enable exchange without a centralized middleman. In theory, such an exchange enables a wild west of sorts: marketplaces where participants are anonymous, any token can be bought or sold, and no authorities can shut it down.

One prominent project in the space is 0x, which is a blockchain-based protocol for building decentralized exchanges. According to the company, "tokenized assets" could be exchanged via 0x without a middleman charging fees.

This concept is already hitting a roadblock, however, as evidenced by EtherDelta, an exchange that used smart contracts for its underlying code. The SEC brought enforcement actions against the company for acting as an unregistered securities exchange, and recently EtherDelta's CEO reached a settlement that included having to pay over $300,000 in fees.

The regulatory clampdown has cast uncertainty onto how decentralized exchanges will operate in the near term. The SEC's cyber unit chief recently said, "using any blockchain to create an exchange without central operations doesn't remove the original creator's responsibility."

For any exchange serving US-based customers, innovation in the space will need to be weighed against securities laws, KYC/AML, and a dialogue with regulators. However, it seems it's only a matter of time before a successful decentralized exchange emerges somewhere.

CONSORTIA

In theory, consortia bring competitors together to collaborate, but significant hurdles remain before consortia see broader adoption.

While distributed ledger technology (DLT) consortia like R3, Hyperledger, and the Enterprise Ethereum Alliance have made headlines for years, their offerings remain thin, and have not gained widespread adoption.

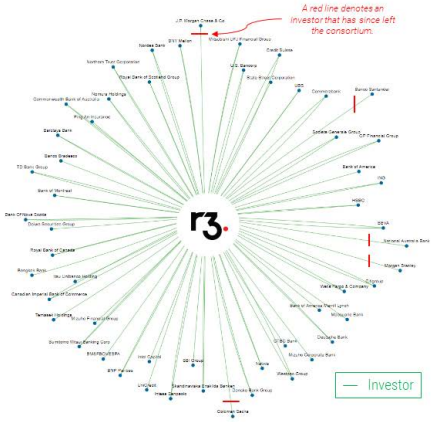
There are a number of reasons for this.

For one, fostering cooperation between competing organizations remains as challenging as ever. In theory, consortia establish a cooperative, neutral proving ground for distributed ledger technology. In practice, distributed ledgers are collaborative, and competitors don't generally collaborate.

For another, integrating into existing IT stacks is difficult. At the DTCC's Fintech Symposium, co-founder of R3 Todd McDonald spoke about some of the legal issues pilots have faced, even as the technology itself worked as hoped. "From the legal side, there were about seven or nine pieces of paper that had to get signed for […] one transaction. None of this is easy. We need to bring in the existing legal constructs. It's still a lot of work that has to be done."

200+ banks, DFIs are part of R3's consortium

While the firm saw early setback with some high-profile exits, R3 has countered with new members, pilots, and shipped software. At the same time, the firm has made a point of moving away from "blockchain" and toward "distributed ledger technology."



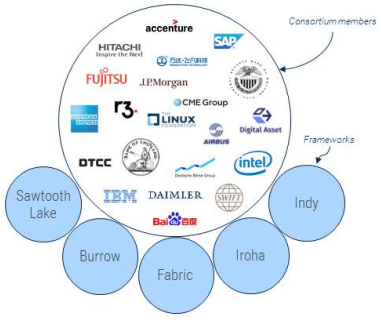
CBINSIGHTS Note: The business social graph above is not exhaustive of R3's members and partners.

To this end, more directed and focused projects with champion stakeholders have found some success.

For example, IBM's distributed ledger service, IBM Blockchain, utilizes Hyperledger, which is an open-source consortium developing industry-specific distributed ledger frameworks. IBM has worked with big corporate players like Walmart, Kroger, and Nestle to integrate distributed ledger solutions, most notably for supply chain management. Larger companies like these have leverage over suppliers, and can likely mandate adoption of their distributed ledger projects.

Hyperledger finds first use case in supply chain

Hyperledger's Fabric framework is geared toward supply chain. The consortium has seen members come and go – by the end of 2017, 15+ members had left or downgraded membership. Still, Hyperledger is adding new members, and now counts over 200 banks, startups, and corporates in its consortium.



CBINSIGHTS

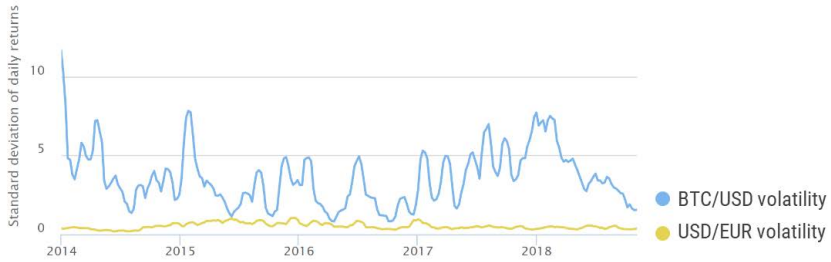
STABLECOINS

Could more stability could bring mainstream adoption to cryptocurrencies?

One repeated knock against bitcoin is its volatility. At the start of 2018, bitcoin's trailing 30-day volatility stood at ~7.5% (in terms of standard deviation of daily returns). In contrast, gold averages about 1.2%, and major fiat currencies average 0.25% - 0.75%. There's no question that bitcoin will need to be less volatile to see real, commercial adoption.

Bitcoin is volatile compared to other currencies

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



CBINSIGHTS Source: Bitcoin Volatility Index.

Stablecoins — cryptocurrencies optimized for stability — hope to solve bitcoin's volatility problem. Close to 60 stablecoin projects have received upwards of $350M in financing. These projects fall into three buckets: (1) fiat- and commodity-collateralized, (2) cryptoasset-collateralized, and (3) algorithmic (non-collateralized).

- **Fiat- and commodity-collateralized:** These stablecoins are backed by fiat or commodities. Often, this means that US dollars (locked in a vault) back each coin one-to-one.
- **Cryptoasset-collateralized:** Dai is a cryptoasset-backed stablecoin. Users lend and borrow ethereum to keep Dai's price one-to-one with the US dollar. As of this writing (11/19/18), Dai has a market capitalization of $75M, with daily volume hovering around $12M.
- **Algorithmic (non-collateralized):** Basis (still in development) automatically buys and sells bonds to maintain a peg with the US dollar. Basis has raised $133M in token financing from GV, Andreessen Horowitz, and Bain Capital Ventures, among others.

If stablecoins gain broader adoption, they could enable bitcoin's original vision. Trust in a cryptocurrency's stability could make it a true means of exchange, leading to what Coinbase deems an "open financial system."

Still, that vision remains a long ways away. The largest stablecoin is fiat-backed Tether (USDT), with a market capitalization of $1.7B (as of 11/19/18). To maintain its stability, Tether claims that all issued USDT are backed one-to-one by bank-held US dollars. That claim has been repeatedly called into question. Further, USDT remains most often used for cryptocurrency trading, not commerce.

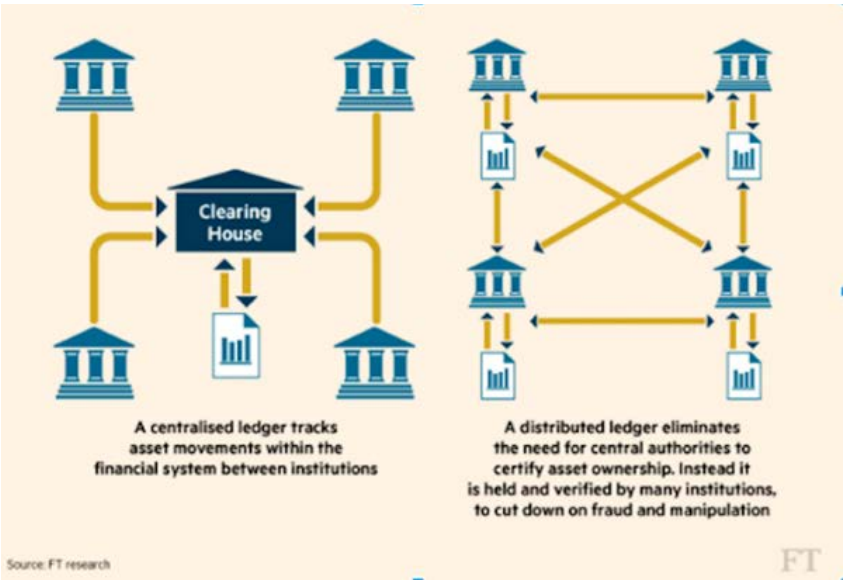
Even if stablecoins are seeing the most use for trading and speculation for now, the fact remains that many of them have achieved their stated goal: stability. Broader use cases could come next.

SECURITY TOKENS

Bringing real-world assets onto the blockchain could democratize access, but faces familiar challenges.

Security tokens are assets that are “tokenized” — digitally represented — on a blockchain. These are different than utility tokens popularized in the recent ICO boom-and-bust, which which allow users to interact within networks. Most importantly, security tokens are subject to securities regulations, like stocks, bonds, and other types of securities.

Security tokens often correspond to real-world assets, like vehicular titles or shares of a company. Tokenizing real world assets could make them easier to access and trade over the web. Easier trading reduces friction, which correlates to increased liquidity and more “open” and accessible securities.



Another advantage of security tokens is that they're programmable. Since these securities are tokenized on a blockchain, "smart contracts" can make them act in a certain way, without the use of a third party. For example, a loan "tokenized" on a blockchain could automatically make payments without the use of a traditional middleman like a bank.

At the same time, migrating real-world assets to a blockchain and satisfying various stakeholders is difficult.

For example, imagine transferring a real estate title onto a blockchain. Is the blockchain then the "record of truth"? What role do local, state, and federal governments play — do their own records still hold weight? How might a court of law rule?

Because security tokens are seeking regulatory compliance, they look more immediately promising than their utility token counterparts. But security token projects may face some of the same hurdles that blockchain consortia have faced: namely, establishing cooperation and collaboration between long-standing stakeholders with differing incentives.

Building a new financial system with blockchain

Finance-focused, blockchain-based building blocks are receiving lots of VC money and attracting talent.

CBINSIGHTS Image source: Felix Feng

NON-FUNGIBLE TOKENS

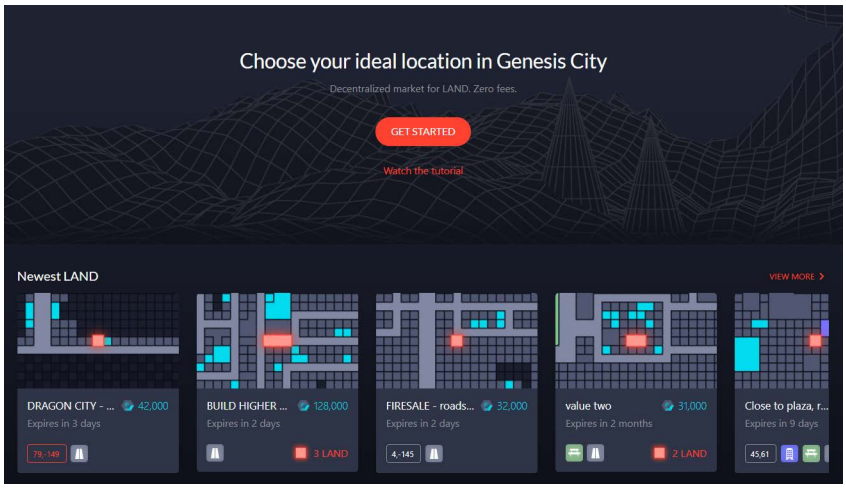
Digitally scarce, unique tokens are finding their first use case in gaming, but are there additional applications?

Non-fungible tokens are unique, blockchain-based tokens that are distinguishable from one another. “Non-fungible” means that the good or commodity is not interchangeable. Diamonds are not fungible, because one diamond may not have the same properties and/or value as another diamond. In this sense, each diamond is unique.

In contrast, fiat currencies as well as some more typical cryptocurrencies, are “fungible.” One US dollar will always be equal to another US dollar.

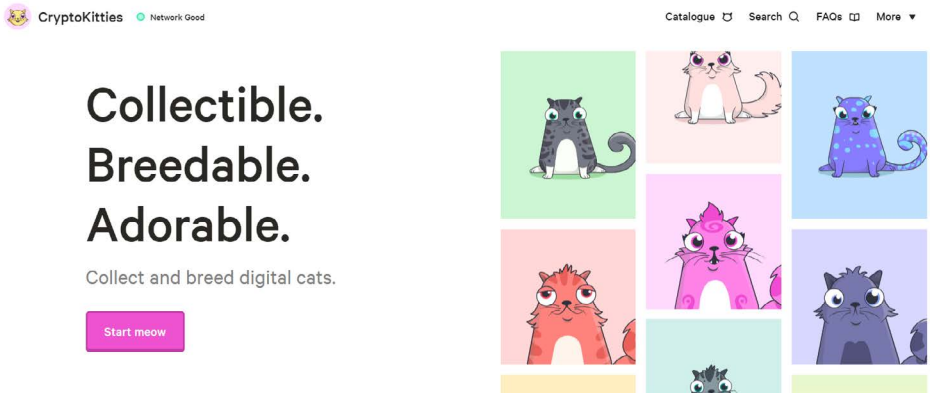
So what is the purpose of non-fungible tokens (NFTs)?

One emerging use case for NFTs is in gaming. Decentraland is building a virtual blockchain-based world. Decentraland’s public blockchain tracks non-fungible tokens, called “LAND.” Owners of LAND own plots of virtual reality real estate within Decentraland. The blockchain here acts as the ledger of record, tracking NFTs to ensure scarcity and ownership rights.



If Decentraland turns into a successful gaming platform, LAND could be quite valuable. To this end, a large plot of LAND sold for upwards of $200K in November.

Another game is Cryptokitties, which raised a $15M Series B in November (bringing the company's total to $27M). Like Beanie Babies, which were once considered a financial investment due to their scarcity and collectibility, each digital Cryptokitty is unique and scarce. Speculators hope that these first "digital collectibles" might one day prove valuable, and are investing accordingly.



The promise of NFTs extends beyonds gaming. Companies are experimenting with NFTs for digital art, digital AR/VR experiences, and even tokenized sunflowers.

The promise of NFTs is to establish digital scarcity online. This has rarely been possible before — the internet has made it easy to copy digital images, music, or text. NFTs could allow for unique digital ownership, using public blockchains as ledgers of record.

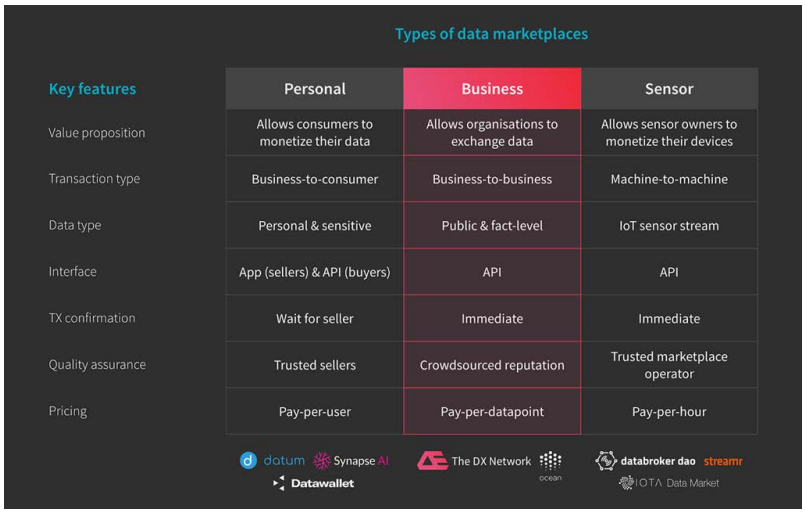
DATA MARKETPLACES

AI is creating huge demand for user data. Blockchain could give individuals the ability to control and sell their own.

To develop AI applications, companies need access to massive datasets.

Consider how Facebook's facial recognition algorithm auto-tags new photos, or how Google uses deep learning to tweak its ranking algorithm. Making these predictive models requires enormous datasets. This is why tech giants with a significant amount of data like Facebook, Amazon, Microsoft, and Apple (FAMGA) and China's Baidu, Alibaba, and Tencent (BAT) are leaders in the field of AI.

But for many other companies, obtaining a lot of quality data can be challenging. As a result, emerging blockchain startups are proposing "data marketplaces" that widen access to AI training data. These data marketplaces might align supply — users or companies with lots of data — with demand, or projects in need of big datasets.



Source: The DX Network

Importantly, blockchain technology enabling such data marketplaces could ensure that shared data remains secure. An open, distributed ledger would remove middlemen, thereby stemming data leakage and keeping data private.

In the not-too-distant future, new ways to control and share data could flip existing business models on their heads. Users could share data with advertisers on an as-needed basis. enomics companies could give contributors “royalties” for sharing their genomes.

Data marketplaces also could lead to more data-sharing between companies. Presently, the process of data partnerships takes months of back-and-forth, legal teams, and often presents issues around data leakage. With encryption, transparent pricing and usage, blockchain-based marketplaces could automate away the frictions of corporate partnerships.

DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAOS)

Companies without owners could be possible with blockchain technology.

In addition to transforming areas like data and payments, blockchain technology could shake up traditional corporate structures.

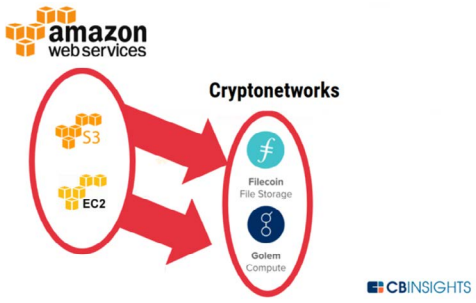
Through blockchain, "ownerless" companies could fundraise without stocks, operate without traditional banking or financial infrastructure, or pay employees without even knowing their names.

In 2016, The DAO (short for decentralized autonomous organization) was the first to attempt this concept, using the Ethereum blockchain to create a crowdsourced venture capital fund. However, The DAO infamously failed when a hacker exploited a bug in the code. For some, the DAO fiasco proved decentralized organizations might be nothing more than a pipe dream.

At the same time, sentiment around decentralized organizations is shifting. In a recent fireside chat, Coinbase executive Balaji Srinivasan said that: “Blockchain companies, to build a community, only need an internet connection and a good regulatory environment… They’re open source groups that [manage internal funds in] straight crypto and might not even have traditional, terrestrial bank accounts.”

Already, blockchain projects are working on this concept of digital incorporation. Companies aim to create digital jurisdictions, where a community will act like an online court system for resolving disputes,effectively giving borderless projects a borderless legal system.

Elsewhere, blockchain-based networks are building decentralized compute and storage services. For example, Filecoin and Golem offer peer-to-peer networks that pay users to lend out idle hardware for various tasks.



While far from a reality today, the tools for making a successful DAO are increasingly within reach.

IDENTITY MANAGEMENT

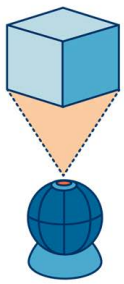
With blockchain technology, users — not internet giants — could control their own digital identities.

The role of centralized internet giants as "digital identity brokers" is under fire. Ad-based internet giants make money by collecting, selling, and analyzing user data, primarily on behalf of advertisers. As these companies collect data, the probability of misuse rises.

Across the web, Facebook's "single sign-on," called Facebook Connect, makes it easy for users to sign in to other sites with their pre-existing Facebook login credentials. This seamless user experience gives the company even more user data for targeted advertising.

What does ideal identity management look like?

1. **Personal:** unique to the user
2. **Persistent:** lives with the user from life to death
3. **Portable:** accessible anywhere the user happens to be
4. **Private:** only the user can give permission to use or view data



CBINSIGHTS Source: ID2020

Blockchain technology might present a better means of establishing identity online. Identity could be verified on an open, global blockchain — controlled by nobody and trusted by everybody. Users could control their own identity, and shift power and control away from the enterprise.

Of course, it's never that simple, and there are challenges to a blockchain-based identity system.

The first is that many governments and organizations don't want it. ID systems such as social security numbers help governments keep tabs on the citizens they govern. Governments may be reluctant to give up their role as de facto ID issuers.

How users currently establish identity online

TRADITIONAL IDENTITY

Traditional forms of identity – like SSNs or birth certificates – still hold weight in much of the developed world, but are increasingly insecure.

TRADITIONAL IDENTITY, DIGITIZED

Attempts at digitizing traditional forms of identification – like India's Aadhaar – (and placing them in secure, central databases) have found mixed success, and are a "honeypot" for would-be attackers.

BROKERED IDENTITY

Companies (like FAMGA) that offer free services in exchange for personal data have acquired billions of users, but now find themselves as brokers of key information and personal identity.

CBINSIGHTS

Because of the network effects, the second problem is that centralized platforms are more convenient than their blockchain technology counterparts, and users don't care enough about privacy to swallow the switching costs. While privacy and control are ideal, users might not want to change over to blockchains with limited network effects.

Threatening

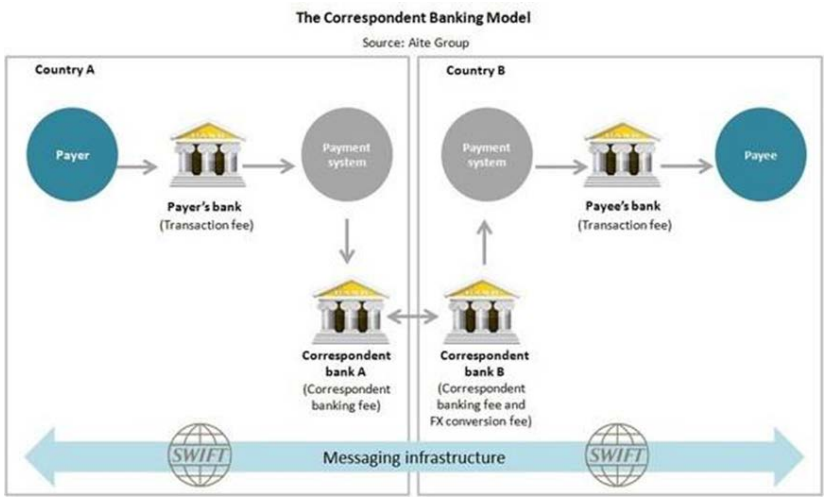
DLT IN CLEARANCE AND SETTLEMENT

After years of experimentation, banks are still looking to reduce clearing and settlement inefficiencies with distributed ledgers.

One recurring mantra among corporate executives has been "blockchain technology, not Bitcoin." Implicit in this refrain is the idea that Bitcoin's underlying distributed ledger technology is more valuable than the cryptocurrency itself.

Financial institutions were among the first to experiment with distributed ledger technology. One area where banks have looked to apply distributed ledgers is in improving the time-consuming clearance and settlement process — if banks are looking at the same databases, clearing and settling transactions between them might become nearly instant.

To illustrate the challenge, today, a simple bank transfer from one account to another has to go through a complicated system of intermediaries, from correspondent banks to custodial services, before it ever reaches its destination.



Source: Aite Group

Distributed ledgers might simplify this process. Instead of having to rely on a network of custodial services and correspondent banks, transactions could be settled directly on open and transparent distributed ledgers.

This could mean serious cost savings for banks. Banks have estimated that distributed ledgers could cut at least $20B in costs by providing better infrastructure for clearance and settlements.

While some projects have stalled, others are meeting early milestones. The Depository Trust and Clearing Corporation (DTCC) — one of the largest clearing and settlement service providers in the US — recently released a study proving that distributed ledgers could support clearance and settlement of trades at a high volume. This is in stark contrast to statements released last year, in which the DTCC said that blockchain technology might be a solution looking for a problem.

BITCOIN

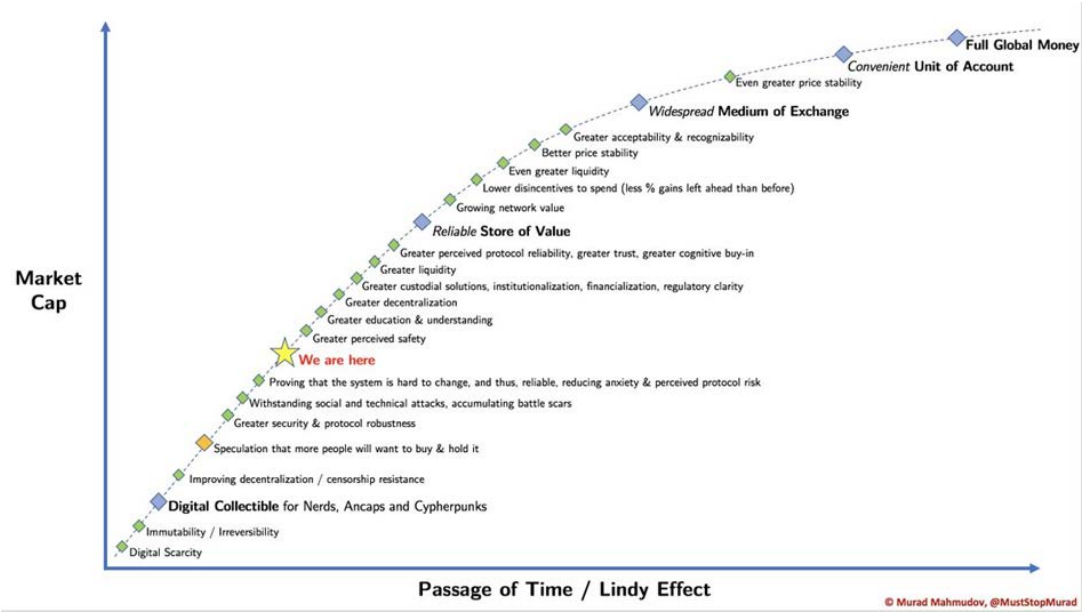
Bitcoin is already a popular speculative asset, but real-world use cases remain limited.

Bitcoin, a "peer-to-peer electronic cash system," first appeared on the scene in 2008. The software's origins remain mysterious — similarly, bitcoin's main use case still remains unclear.

Ten years out, bitcoin is not yet widely accepted as "electronic cash." First off, the vast majority of merchants don't accept bitcoin. Among other things, this is due to historically high transaction fees. Indeed, for smaller merchants, bitcoin's transaction fees are prohibitive — why pay $5 in fees for a coffee?

Bitcoin also hasn't moved the needle in peer-to-peer payments. Most consumers prefer traditional platforms like Venmo, Zelle, and WeChat to crypto-based ones like Coinbase or Circle.

But proponents believe bitcoin still has potential for widespread adoption.

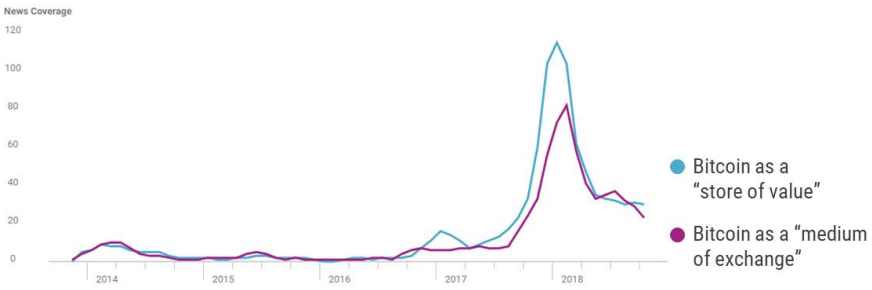


Source: Murad Mahmudov

They see bitcoin on a timeline, with bitcoin first gaining acceptance as a “store of value,” and later gaining acceptance as a medium of exchange. Indeed, media mentions for “bitcoin” alongside “store of value” have outpaced those for “bitcoin” and “medium of exchange.”

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



CBINSIGHTS

In countries with severe inflation, citizens might be hedging with bitcoin, rather than simply speculating. While the data is sparse and early, bitcoin trading volume is up alongside rising inflation in Argentina and Venezuela. Still, whether citizens are treating bitcoin as an alternative means of exchange, or as a store of value, remains to be seen.

Last but not least, "second-layer" networks are scaling Bitcoin to process more transactions at lower costs. The Lightning Network, for example, is a second layer on top of the Bitcoin blockchain that enables cheap, instant bitcoin payments.

All this is to say that, despite other use cases for blockchain technology dominating the conversation in 2017 and 2018, there is still plenty to talk about around the sector's very first use case, Bitcoin.

PRIVACY COINS

Privacy coins have earned a bad rap, and are still seeking acceptance beyond the black market.

A longstanding concern around bitcoin is that it allows terrorist groups and criminals to circumvent traditional financial regulation and launder money.

The reality, though, is that bitcoin is actually quite traceable. This is because bitcoin's blockchain its distributed ledger of record is only "pseudo-anonymous" — while "public addresses" are anonymous, the transfer of a bitcoin from one public address to another is entirely public.

This has helped law enforcement to surveil nefarious transactions. Indeed, a number of companies specialize in tracking such movements for law enforcement agencies.

To create full anonymity, teams have built cryptocurrencies where transactions cannot be tracked. Known broadly as "privacy coins," these alternatives are often bitcoin-like,but built chiefly for privacy. Major players here include Monero, Zcash (which has a privacy-optional feature), Horizen (fka ZenCash), and Dash.

Source: The Block

While privacy coins are associated with black markets, it is certainly possible to use privacy coins elsewhere. Indeed, some might argue that paper cash today is often used specifically for its privacy.

Still, it's likely that centralized crypto-fiat exchanges — the primary place where users purchase cryptocurrency — will not list privacy coins due to poor public sentiment and adverse regulatory regimes.

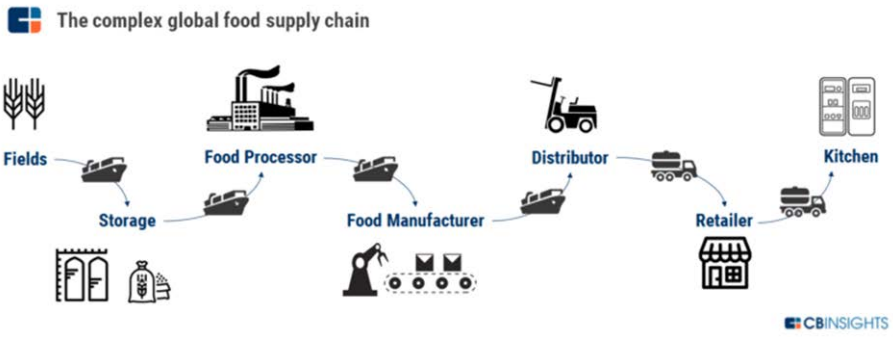
As it stands today, though, that's not yet the case and privacy coins have gained listing on major exchanges such as Gemini and Coinbase. As custody solutions and decentralized exchanges develop to offer "unstoppable" hubs of commerce, it's likely that privacy coins will get even easier to purchase and hold.

DLT IN SUPPLY CHAIN

Supply chains are complex and inefficient. Corporates are looking to DLT to reduce the time and costs of moving products.

Beyond applications in healthcare, real estate, banking, and other industries, distributed ledgers could have a broad impact on the supply chain.

Today's global supply chain is complex, bringing together farmers, warehousers, shipping companies, distributors, and retailers. Involving so many different parties also means involving many different types of record-keeping methods, from robust databases to email chains to paper printouts.



As products move across a supply chain from manufacturer to sale, distributed ledger technology (DLT) could be used to document transactions in an open, distributed, and real-time database. Such a system could reduce delays, increase transparency, and reduce human errors.

To illustrate the problem, shipping giant Maersk found that a single shipping container requires approvals from 30 different parties and authorities. All these approvals take time, and often use manual paper processes.

Maersk is looking to use DLT as a potential solution. TradeLens, Maersk's distributed ledger joint venture, recently announced it recruited 94 global supply chain participants — including major port operators, shipping lines, and freight forwarders — to join its platform this year.

Blockchain shipping initiatives remain fragmented

Select blockchain shipping initiatives (2017 – 2018)

Date	Summary	Select Players
Mar'18	Consortium that tested a blockchain solution on 12 separate shipments to eliminate the need for printed shipping documents.	APL, ABInBev, accenture, KUEHNE+NAGEL
Jan'18	After previous collaboration, Maersk and IBM formed a new blockchain company "TradeLens" to commercialize blockchain use. So far, dozens of companies have been onboarded.	MAERSK, IBM
Sep'17	Carrier HMM (Hyundai Merchant Marine) completed its first blockchain pilot voyage, as part of a larger consortium, tracking cargo with blockchain and IoT technology from booking through delivery.	HMM, SAMSUNG SDS
Sep'17	Partnership to launch a blockchain platform that helps to simplify marine insurance, an area commonly plagued by excessive paperwork. The platform, dubbed "Insurwave," went live in May 2018.	MAERSK, EY, guardtime, Microsoft, ACORD
Aug'17	Official partnership to improve shipping security and efficiency through blockchain. Completed successful blockchain trial tracing cargo from Chongqing to Singapore in February 2018.	PIL, PSA, IBM

CBINSIGHTS

As a growing roster of corporate names deploy distributed ledger initiatives, many will be watching the progress of Maersk and other logistics giants as a barometer for success in the space.

With trade wars and tariffs casting uncertainty over the global supply chain, distributed ledgers could see increased use as a way to cut costs and keep organizations lean.

DLT IN IOT

DLT will compete against existing tracking databases and RFID tags.

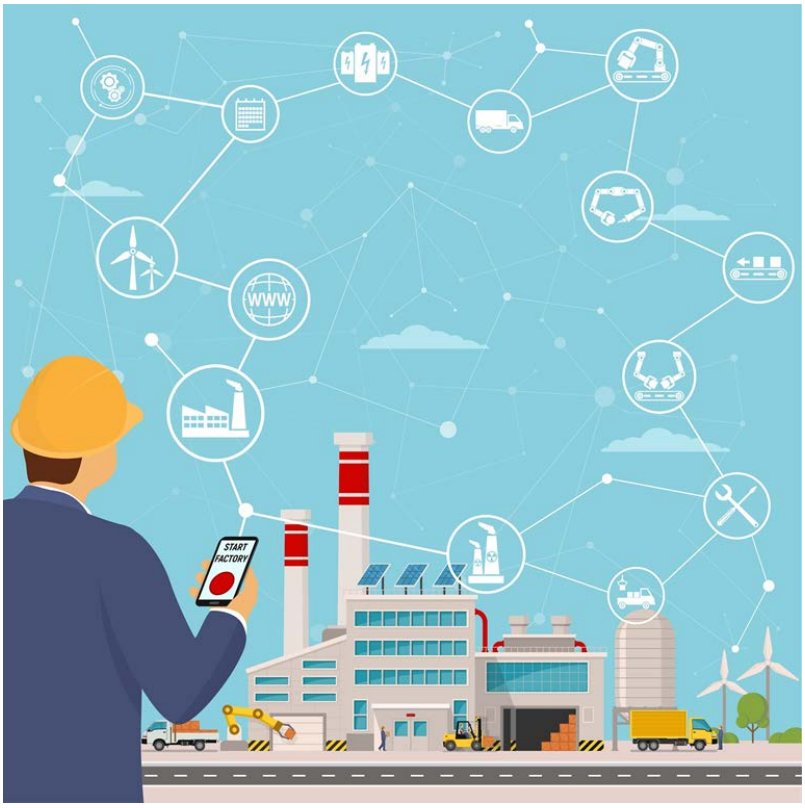
Companies often turn to the internet of things (IoT) to digitize physical processes. Across plants, warehouses, and factories, companies are using connected devices to monitor machines and productivity through manufacturing and shipping processes.

Distributed ledgers are emerging as tools for enhancing IoT.

As a product moves along an assembly line, or between suppliers, sensors could update data in a distributed ledger. This would help involved parties access the status of the product in question.

Distributed ledgers could also improve inventory accuracy by allowing retailers to communicate with their supply chain partners in a secure digital platform. This might mean better planning, especially around inventory shipment delays.

As the world of IoT has been roiled by hacks, IoT security could be another potential application of distributed ledgers.



The real test for IoT-specific distributed ledgers will be in how they stack up against traditional technologies. Relational databases and RFID tags often suffice, and bringing IoT and DLTs together might create unnecessary complication for many enterprise use cases. Companies will look to see whether DLTs can help them make any efficiency gains that give them an overall edge.

Transitory

INITIAL COIN OFFERINGS

ICOs have dropped off a cliff as regulators ramp up crackdowns.

Initial coin offerings (ICOs) are sales of tokens by blockchain companies looking to raise funds. According to teams holding ICOs, tokens provide "utility" within a decentralized ecosystem.

To use a metaphor: a company building a new subway system might sell limited tickets that (1) offer future access to the subway, and (2) fund the subway's development. If the subway is a success, those scarce tickets would be in high demand. Increased demand could lead to higher prices (in secondary markets), rewarding early backers.

To this end, teams holding ICOs argue that such "tickets" aren't securities, and that the sale of these tickets doesn't represent an unregistered securities offering.

So far, it looks like US regulators disagree. Speaking in June 2018, the SEC's Director of Corporation Finance, William Hinman, suggested that most ICOs are unregistered securities offerings. Since then, the SEC has subpoenaed dozens of companies that held ICOs. Many of these have refunded investor funds and paid fines.

Unfavorable regulatory stances have taken a toll on the ICO market. Quarter-over-quarter, ICO funding fell off a cliff. According to TokenData, ICOs raised just $181M in September, well below the $2.4B+ raised in January. In contrast, traditional venture funding to the sector more than doubled year-over-year, peaking in Q2'18.

ICO funding has dropped off a cliff

Total funding ($M) raised by initial coin offerings, by month. January 2017 – September 2018

CBINSIGHTS Source: TokenData.

There's no question that regulatory activity has quieted the once-raucous ICO market. Moving forward, ICOs in the US and abroad will face sustained pressure, and companies should look to avoid the mistakes of 2017 and 2018. Selling "centralized" tokens to retail investors may no longer an option.

Of course, there are workarounds. Companies that held ICOs exclusively for "accredited investors" have largely sidestepped regulatory activity.

Another, more direct way to hold a compliant ICO is to build a "sufficiently decentralized" network, which could make the network's tokens more like digital commodities than securities. Hinman highlighted this in his June comments: "If the network on which the token or coin is to function is sufficiently decentralized — where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts — the assets may not represent an investment contract." This would put an ICO on the right side of the law.

SMART CONTRACT PLATFORMS

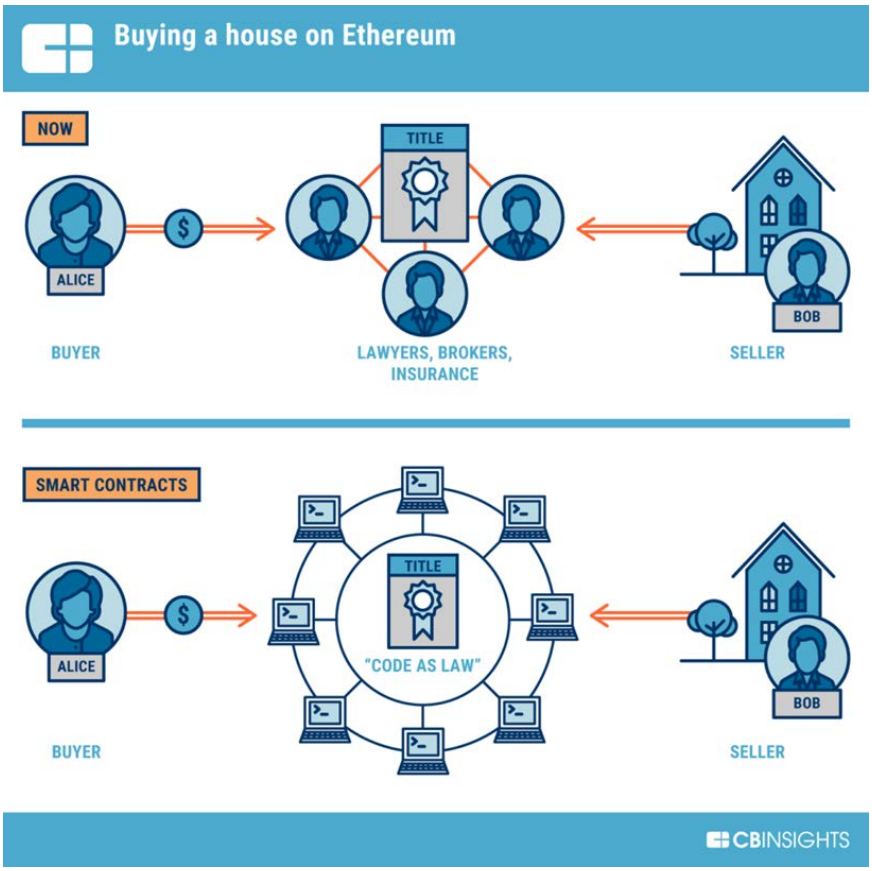
Automating agreements has potential across industries, but for now consumer adoption remains limited.

A smart contract is code placed on a blockchain, which digitally enforces the performance of a contract. This code lives on an open, transparent, and decentralized database and runs automatically when preset conditions are met. Many of the companies that raised funds via ICOs in 2017 and 2018 used smart contracts to build "decentralized applications," or dApps. The idea is that these dApps could operate continuously, without dependency on centralized providers of web infrastructure.

To illustrate, let's say that Alice and Bob enter into a bet. The pair could agree to use some basic code — an "if, then" contract — to gamble on tomorrow's temperature. If the temperature is higher than 70 degrees, the code is programmed to pay Alice, otherwise it pays Bob.

Alice and Bob could use a middleman or they could place this bet onto a blockchain, effectively creating a smart contract.

This bet is a "contract," because Alice and Bob have agreed to its terms, to some degree transforming code into law. And, this bet is "smart" and "decentralized" because all the blockchain's nodes hold a copy of this contract.



The most well-known smart contract platform is Ethereum. Hundreds of companies launched ICOs in 2017 and 2018 atop Ethereum, and the platform continues to have the largest developer community of any crypto project. Still, consumer adoption remains extremely limited.

Some see Ethereum — not the concept of smart contracts — as a poorly constructed platform. To this end, other smart contract platforms with strong teams have raised big sums of capital to compete. Companies like Tezos, Hedera Hashgraph, and Dfinity are all looking to displace Ethereum as a smart contract hub.

Some have even created “ecosystem funds” to gain developer adoption; Dfinity and Polychain Capital co-manage a fund. These funds underscore the importance of getting developer traction early, even if it means paying for it.

With all this activity, smart contracts remain an exciting area of blockchain technology development. At the same time, only a limited number of developers will create dApps until there is a widely adopted smart contract platform for them to run on.

WHERE IS ALL THIS DATA FROM?

The CB Insights platform has the underlying data included in this report

CLICK HERE TO SIGN UP FOR FREE