INSIGHT

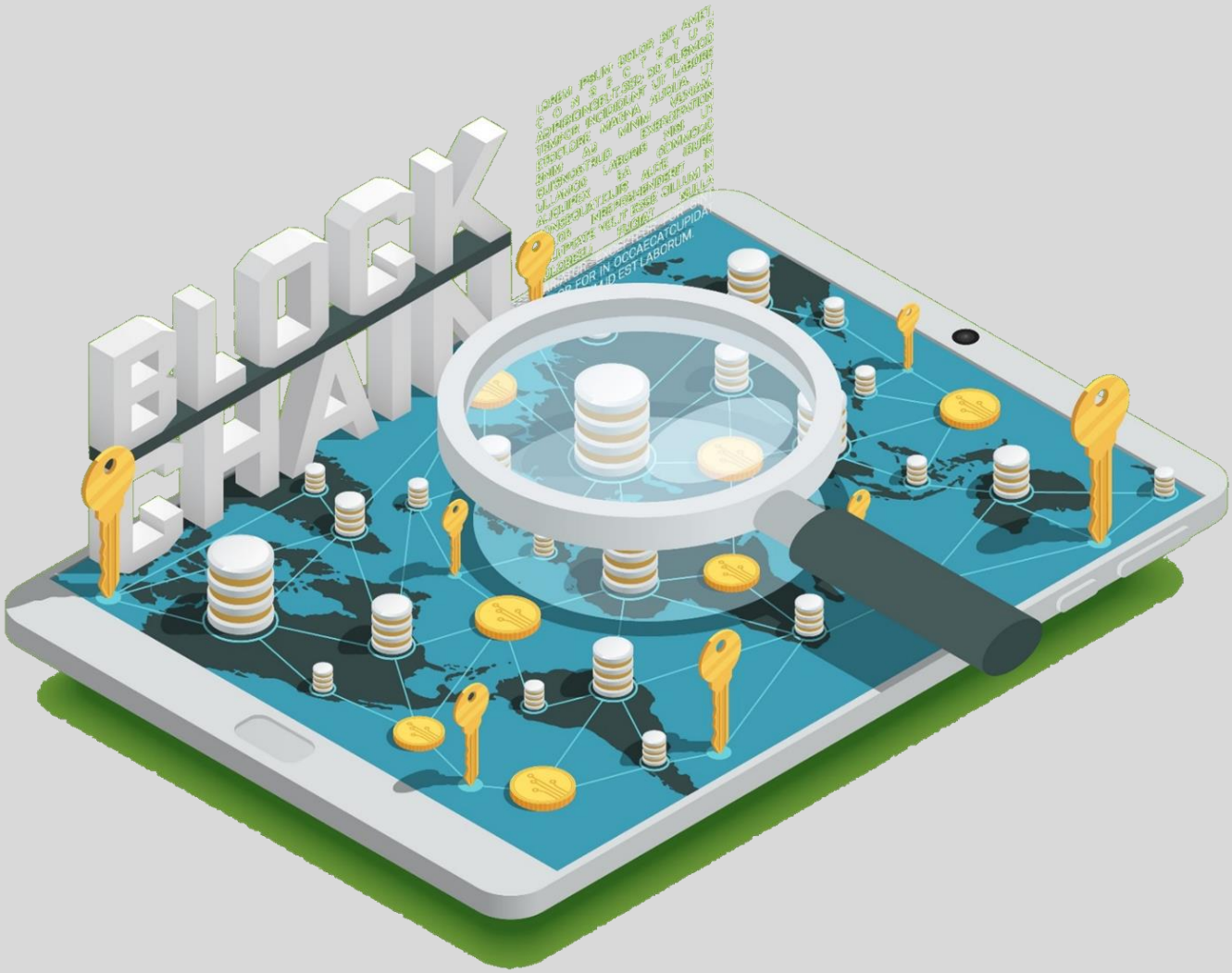
APRIL 2018

FTI Consulting

Telecom, Media & Technology Practice

Are Blockchains in Your Company's Future?

An In-Depth Look at this Important Technology



Are Blockchains in Your Company's Future?

As if CEOs didn't already have enough digital disruption to worry about, the blockchain is yet another "game-changing" new technology to cope with. The good news is we believe this technology is much more friend than foe. Because of its security, transparency and potential to dramatically reduce transaction costs, it could usher in a future worth embracing.

This article is an in-depth companion to our article in CEO World found here, and outlines blockchain's key features in non-technical terms and describes some business use cases happening now. We believe understanding these important concepts will allow executives to envision how they might put blockchains to work in their own companies or industries.

What's the Big Idea?

Most people know by now that blockchain technology was originally developed to support the bitcoin ecosystem. Bitcoin developers' ongoing ambition is to provide an unregulated and highly decentralized currency requiring no central bank. The key requirements of such a system are daunting: the transaction records must be transparent so anyone can verify them and it must be "trustless", meaning parties do not have to know or trust one another to transact. It must be virtually unhackable, and it must be highly distributed across a set of independent computers so failures or attacks on some do not affect the integrity of the whole. Finally, it must be open-source, so that anyone can download the code and become a participant.

The inventors of bitcoin's blockchain technology achieved all this and more. Bitcoins themselves are growing in use for transaction payments. Bitcoins that were originally worth less than a dollar were recently trading for $10,000 and Japan's central bank recently began recognizing it as a legitimate currency. But more importantly, the underlying blockchain technology, being open source, can be used by anyone to develop applications that rely on its powerful features. So, what are they?

A Decentralized Ledger. First, the blockchain is a decentralized ledger whose entries are instantly spread and verified across many independent computers. By "ledger" we simply mean a list of transactions stored sequentially. The set of all the deposits and withdrawals you've made in your checking account is a ledger, and when summed up represent your balance. One's bitcoin balance is derived in exactly this way.

This decentralized ledger means there is no central authority or master server holding the official ledger. Instead, the accurate ledger is what the majority of individual computers agree it is. New transactions are only added once a majority of these computers agree it is the right entry and their revised ledgers match.

Beyond not needing a central authority, this decentralization means the system is trustless. No computer has to trust another, since they all independently verify the proposed modification to the ledger. It is sufficient for the majority of independent nodes to agree that Person A has enough bitcoins to transfer to Person B, and to agree to the amendments to their ledgers. This is far different than the centralized computers and banking systems today, where everyone must have confidence in the third party verifying and housing the transactions.

The decentralized ledger also provides a significant defense against attacks because there is no central server to attack. The majority of computers would have to be hacked in order for them to agree to fake ledger changes.

Not Just Money. A powerful feature of these ledger entries is they can refer to anything. A ledger record is

essentially just text. This makes it possible to set up blockchain-based systems to record the buying and selling of songs, or a ledger of artwork provenances, or stock trades, or shipping container transfers, or election votes. The possibilities are limitless. The "trustlessness" ensures anonymity between those transacting – so parties don't have to have prior relationships to engage (just like a stock exchange) – and it means computers in the network don't have to trust each other or even be set up by the same organizations.

Blocks and Chains and Even More Security.
Each block on the blockchain is made up of ten transaction records. This is done to keep the chain smaller and reduce the amount of work done by the individual computers doing the verification. But blocks have some very important properties. Blocks are linked together by a special key called a "hash" that cryptographically links a new block to its previous block. This hash is derived from the data in the block itself, so if anyone tries to modify the data in the block, its hash no longer matches. In addition, the new block's hash includes the hash of the previous block, so they are inextricably linked. Together these blocks form a linked chain of compatible hashes, hence the name.

Under this architecture, tampering with one block makes all subsequent blocks invalid. Consequently, it's impossible to change an individual block in the chain. A hacker must forge all subsequent blocks from the tampered block forward. And remember, the majority of other computers have to agree that this re-engineered chain is identical to their copies, which is imponderably difficult to pull off.

These security features make blockchains very safe to use for institutions and consumer applications. They are inarguablely far more secure than the centralized hacking defenses used by most companies and computer applications today.

Miners and Rewards. The independent computers we've been talking about above are "nodes" in the blockchain network. In bitcoin's network these are romantically called "miners". Anyone can become a miner simply by downloading the open source software and turning their computer system over to the task of verifying the ledger and building new blocks. This takes a lot of computing power. Obviously, miners would not do this for free. Bitcoin rewards the miner who is the first to find a new block to add to the blockchain with, you guessed it, a bitcoin.

A miner's challenge is to be first to solve a very difficult mathematical puzzle and to produce an accurate new block. This "proof of work" is part of the overall security scheme. Importantly, this mathematical puzzle has a finite number of possible answers, limiting the number of total possible bitcoins that can ever be generated. This creates the scarcity needed in all coinage systems.

Companies who want to use blockchain technologies via the public Internet will need to solve the problem of how to attract and reward miners. Alternatively, companies can establish private computer networks and no reward system may be needed. Submitting various forms of "work" to the public network and rewarding miners for doing the work can, in theory, be very cheap. This opens whole new possibilities for companies that previously had to have their own data centers or pay hefty prices to cloud-based suppliers.

Transparency. While there is a lot of cryptographic technology used in the blockchain architecture, the transaction data in the blocks are not encrypted, at least in the bitcoin embodiment. This creates public trust and auditability, since anyone can verify the data. However, the identity of the owner of the transaction is still private. With bitcoins, for example, we can know that someone with a long indecipherable address key received 50 bitcoins on July 1, 2017, but we do know who that person or institution is. While this may seem to diminish utility, it typically doesn't. For example, if a blockchain ledger was established by the government to maintain a title registry of U.S. homes, everyone could see when a home passed from one owner to the next, without knowing who the owner was. However, the current owner can prove they own the home because they have the unique

cryptographic address key for the transaction. Corporate entities who might collaborate to implement their own blockchain systems can choose to encrypt these messages using common public key encryption. The public key can be exposed in the transaction records of the blockchain while the private keys are only known by the companies who participate. In this way, only the member companies can read the ledger.

Key Enhancements & Limitations

It's clear from the features described above that the original blockchain architecture is quite powerful. Nonetheless, there are drawbacks, and there have been enhancements devised to either overcome these limitations or to augment their original capabilities. We'll start with the limitations so the enhancements can be appreciated.

The Scaling Problem. There are three key flaws in the original bitcoin embodiment of the blockchain model. The first is the growing size of the ledger itself. This is called "the scaling problem."

The ledger does not contain mere balances of who owns how many bitcoins. As described earlier, it is a record of every transaction, like your checking account, and a person's balance is derived by summing up their transactions. This is done to ensure that each computer on the network actually has the full ledger and isn't spoofing the system. The downside is that the bitcoin ledger has become very large and is growing rapidly. At the end of 2017, the size of the bitcoin blockchain was approximately 150 gigabytes, according to Statista, having nearly tripled since late 2015. This is a lot of data to cart around. If not curtailed, only the biggest computers will be able to handle it, and the network of miners will reduce to a tamperable few.

Speed Limitations. Blockchains are very secure in part because they require the participating nodes to do a lot of work. They must approve any new proposed blocks by verifying the entire blockchain and ensuring the proposed block fits. They must also compete to solve that hard math problem discussed earlier as a proof of work. This makes blockchain architectures slow as a transaction processing engine. Today, it takes bitcoin about ten minutes to ratify a proposed transaction. Compare this to the Mastercard's network that verifies approximately 2,000 transactions per second on average. In some embodiments this isn't too much of an issue – for example, waiting for an application to confirm the provenance of a piece of art isn't a problem – but asking customers to wait ten minutes before they can leave a retail store when paying with bitcoins is a significant limitation.

The Tragedy of the Commons. Blockchains as originally implemented by the inventors of bitcoin, reward the first miner who solves a hard computer problem and successfully proposes the first majority-approved new block. This means that miners with the most powerful computers have an unfair advantage over other miners. Today, there are miners who have implemented specially designed chips solely tuned to solve the bitcoin problem at super-high speeds, making this imbalance even more acute. Thus, a few actors are spoiling the egalitarian structure for everyone else, discouraging new miners from joining. This is known as the "tragedy of the commons" problem in economics, coined when England opened up common grazing lands which were overgrazed by a few herders and spoiling the land for other farmers. The bitcoin developers have since modified the original reward system to share a minority of the reward with other miners who were runners up in the contest, but this still gives most of the gain to the first successful miner.

Content Limitations. While blockchains can store message text, a block cannot exceed 1 MB. While not a problem for many uses, this limitation prevents, say, the storing of a song or movie bought by a consumer within the blockchain itself. So while the transaction is secured in the decentralized ledger, the digital content still must be stored in a centralized server for access.

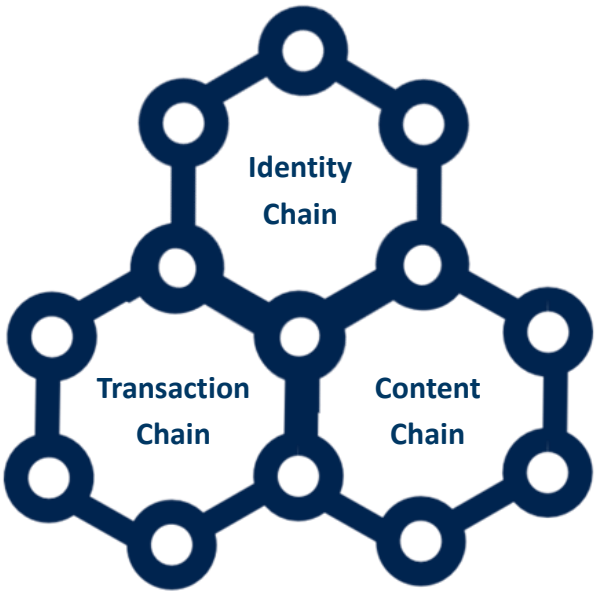
Let's now turn to some key enhancements, which solve some of these problems and also bring more power to blockchains.

Smart Blockchains. Remember that bit of text stored within each record of the blockchain? What if this wasn't just text, but executable code? If it were, then companies could submit "transactions" to the miners in the blockchain network to actually do computer work for their companies and reward them for doing it. This is the concept behind a company called Ethereum, which has enhanced blockchain technology to make their blockchain network smart.[1] Companies can embed any set of computer instructions in the message text without limitation. Companies submit these transactions to miners who are paid for the number of separate computer steps executed in the message. Hence the reward scales with the amount of work requested. This work could be anything from transferring a stock to checking a consumer's creditworthiness.

This paradigm has profound implications and also helps solve the tragedy of the commons problem. Such an enhanced blockchain network can be called on by companies to do work securely and potentially at much lower cost – especially since they wouldn't have to own the machines. But that's really the least of it.

This shift has the potential to invert the entire Internet as we know it. That's because today, the Internet works using a "thin" protocol layer that conveys messages and text around the web. But private servers do all the real work – such as settling Amazon's credit card transactions, displaying search results, etc. By putting the software in the message conveyed in the protocol and letting independent computers execute the code, we are putting the intelligence within the Internet network layer. This "fat protocol," as the people at Union Square Ventures have termed it, could transform the Internet itself and how businesses are built and global work gets done.[2] While there is no doubt economists will have a field day debating this potential economic inversion, early success in crowd-sourcing human work suggest crowd sourcing computer work is viable as well.

Embedding software in the chain also helps solve the tragedy of the commons problem. There is no point developing a custom chip affordable by only a select few to solve the bitcoin mining problem. This is because the code submitted to the network can now be anything, so the processors executing the code must be of the more general sort available today to anyone. This in turn democratizes the network and encourages participation.



Chains Working Together. We mentioned earlier that the original blockchain embodiment had speed, scale and content limitations. There are several ways of getting around these problems. One key way is by making multiple chains that interact.

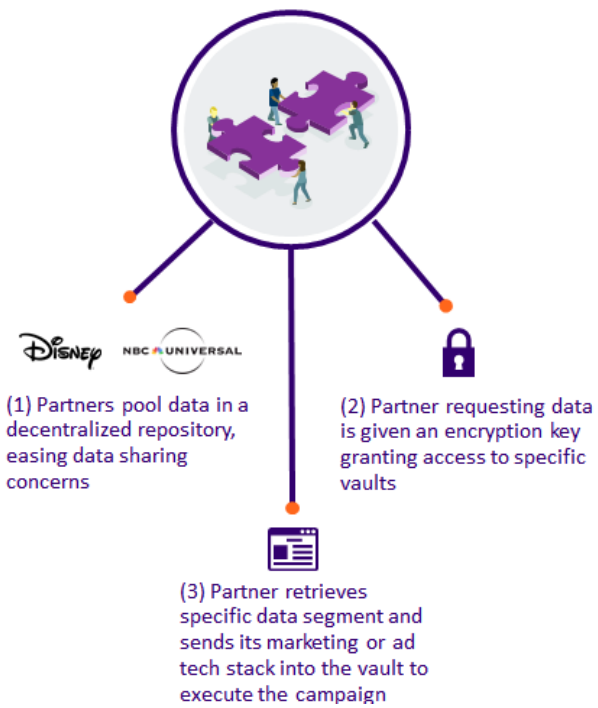
Since different blockchains can be set up for different purposes, there's nothing that stops them from being used together. In the original blockchain architecture the user's ID (address) is stored in the same block as the transaction data and the small amount of content. But what if the identity chain was separate? This would allow a shorter identity chain – since a person only has one ID – that would be much faster to validate. It could even be kept private, say within Amazon, so only Amazon knows who the actual users are. The transaction chain can still be public. In addition, the transaction records, say, for buying songs, could then point to another private chain that contains these actual encrypted songs. This allows the song chain have "fat" links (whole songs), but short

chains since there are only so many unique songs. Shorter chains speed up verification and access. We'll see an example of this below.

Two Examples

Beyond bitcoin itself, we will highlight two examples of blockchains in use today. The articles we list at the end of this paper have many more[3]. The ones discussed here were chosen because they illustrate very different uses.

Comcast. Late last year, Comcast announced the launch of its Blockchain Insights Platform. This platform will enable brands to make ad buys on both broadcast and OTT TV using blockchain technology. The partnership, which has brought together Disney, NBC Universal, the U.K.'s Channel 4, Cox Communications and Mediaset Italia, plans to allow marketers, publishers and programmers to share data in a decentralize repository. Advertisers and programmers could match data sets more effectively to build and execute media plans based on custom audience segments and more precisely target a nationwide footprint of pay-TV customers and streaming device users. The technology includes a series of encryption and rights management layers that would allow partners to find specific data segments to execute a campaign without compromising the data owner's assets and the consumer's privacy.



Citibank Launches Private Blockchain Network. Citibank and Nasdaq have recently partnered together to unite two blockchain-based systems, enabling clients who are raising funds or swapping private shares through Nasdaq to take advantage of payment services provided by Citibank. The Citi-Nasdaq partnership is one of the first examples of an dual enterprise blockchain system to enter production.

Nasdaq previously launched a blockchain-based platform called Linq in 2015, designed for private equity, but the system lacked the ability to process payments — it was mainly used to record ownership of shares. Investors or issuers had to leave the system and initiate a wire transfer to pay for shares once they were traded on Linq.

The new offering links Citibank's Worldlink payment system to Linq, which allows Nasdaq to transfer a payment request from Linq to Citibank as soon as a share is bought or sold. The bank then automatically processes that request through WorldLink, which Citibank clients primarily use to make payments that require foreign currency exchange.

Within Linq, a record of those shares will be preserved on a distributed ledger to which only the parties involved in the trade have access. Similarly, through CitiConnect for blockchain, a record of payment is also added to the same ledger as soon as it is processed. On both sides of the system, this creates a "golden record" of the transaction and payment that either party can refer back to in case of disputes.

Final Considerations

While it's often dangerous to adopt new technology paradigms far ahead of the curve, these examples show there are systems being deployed today by large companies to do real work. These two examples hint at some larger forces that could change every company's competitive landscape.

The Comcast example shows how companies who normally compete can share some of their data to improve ad targeting and reduce buying friction for advertisers. Each company can share certain consumer behavioral data in various blocks on the chain, but the consumer whose data it represents is hidden by an encrypted address pointing back to and not included in the shared database. This is a concept knows as "coopetition," between companies, and it can now be enabled through shared data on the blockchain[4].

The Citi-Nasdaq example shows how a virtual exchange and transaction processing system is developed by connecting different chains to form a larger network. This in turn will allow these two partners to enjoy certain network effects. Since they are first to market, their network could become dominant – large enough that others are better off joining the network rather than creating their own, because that's where the buyers and sellers are.

The Internet is the foundational invention of the digital age. All that has come after it has been enabled by it. It was a paradigm shift in how people and machines communicated, and it continues to spawn new services and innovations, such as Alexa and the Internet of Things.

Like the Internet, blockchain represents a paradigm shift to trustless exchanges that enable transactions, but can also perform all kinds of computer work in a decentralized, open-source manner, likely at very low cost. The power of the technology and its myriad uses are only now emerging as blockchains make their way into commercial use. CEOs should consider adding the blockchain to their arsenal of innovation now and be on the alert for projects and partnerships that could more fully and cheaply automate their businesses.

FTI Consulting has helped companies develop their blockchain strategies and business models. For more information please contact us.

Content Sources:

1. This concept has been called “smart contracts” but the term is misleading. The code can be virtually anything. Etherium’s whitepaper provides a deeper description of their system.
2. For more information on Fat Protocols, see: http://www.usv.com/blog/fat-protocols.
3. For more information on the Citi-Nasdaq partnership and Comcast’s Blockchain Insights Platform, see:
   - https://www.nasdaq.com/article/nasdaq-and-citi-announce-pioneering-blockchain-and-global-banking-integration-cm792544
   - https://www.coindesk.com/citi-nasdaq-partner-blockchain-payments-solution/
   - http://adage.com/article/digital/comcast-marketers-make-tv-ad-buys-blockchain-tech/309486/
   - https://adexchanger.com/data-exchanges/coming-2018-comcast-hopes-spur-data-sharing-blockchain-technology/
4. See the book “Coopetition” by Barry Nalebuff.

Author:

Bruce Benson, *Senior Managing Director*
John Cartoux, *PhD & Managing Director*

Views expressed here are those of the authors alone, and do not represent the views of FTI Consulting, Inc. or any of its other employees.