DXC.technology

White Paper

Blockchain in the financial services industry

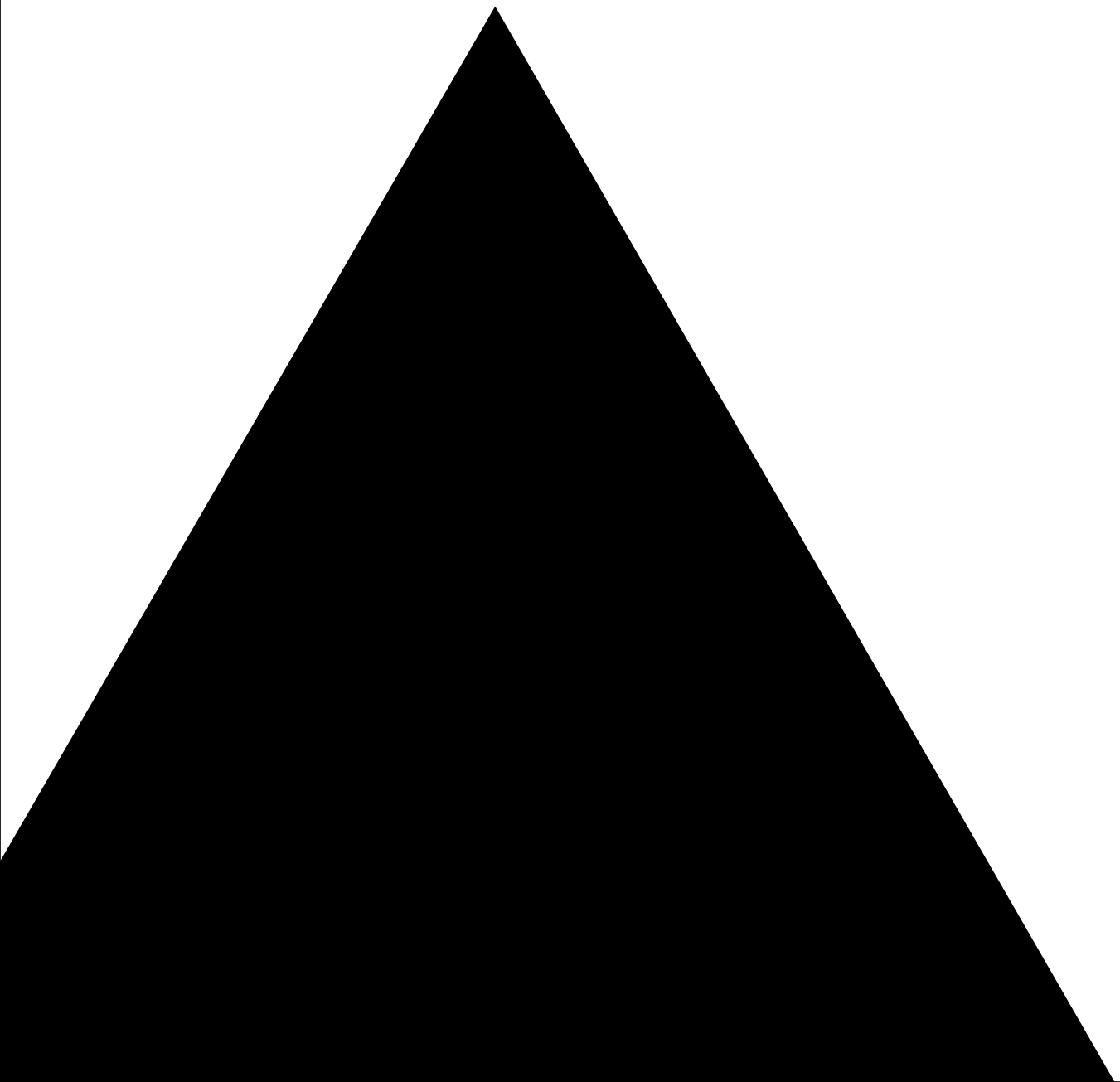


Table of contents

Blockchain is a technology that creates a distributed ledger of transactions on a network that is secure, tamper-proof, and easily accessible. The largest and best known blockchain implementation is the Bitcoin network.

A new model emerges

Banks and other financial institutions (FIs) have traditionally served as the guardians of financial activity—safeguarding accounts, extending credit, and facilitating payments—keeping the wheels of commerce turning. The entire financial system has been built on a model of centralized trust, where most financial activity is required to flow through and be controlled by financial institutions. This model enables financial institutions to perform various services, including recordkeeping, account balancing, exchange of funds, fraud detection, and others, which provide markets with the necessary stability, security, accuracy, and confidentiality to operate effectively. The model is complemented by government legislation and monitoring bodies that provide oversight to ensure a reliable banking ecosystem.

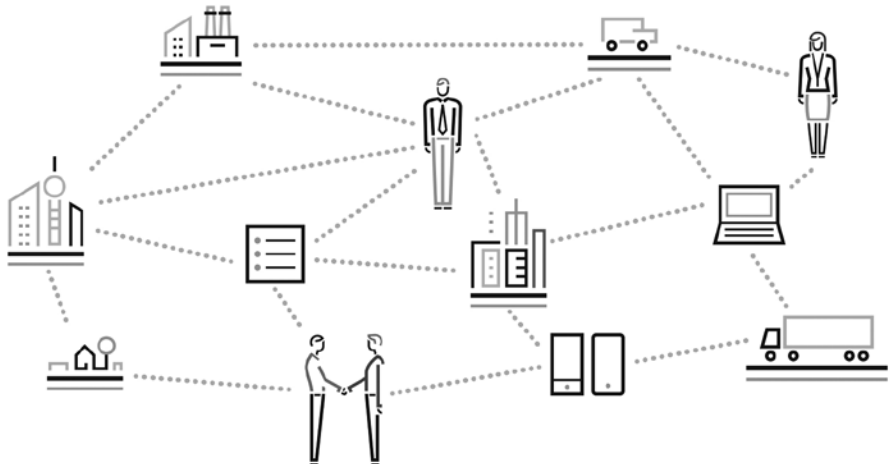
Over the past several years, the pace of technological innovation across various industries has drastically increased. Advances in networking, storage, and computing power have produced an expanding array of new technologies and business models—changes that threaten to disintermediate incumbent players in the financial services industry. New models, based on eliminating the "middle man," have also disintermediated traditional incumbents in other sectors. Companies such as Amazon, eBay, Uber, and Airbnb have been able to remove friction from the value chain in their respective industries, resulting in new innovative products and services that provide the consumer a higher purchasing power (control). A new term, "uberization," has even been coined to describe this type of disruption. The latest in this line of innovations has the potential to strike at one of the core value propositions of the financial industry itself—the notion of trust. The technology that represents this challenge? Blockchain.

This business white paper focuses on blockchain's evolution and its impact in financial services.

Blockchain—enabling a distributed ledger

In simple terms, blockchain is the technology that creates a distributed ledger of transactions on a network that is secure, tamper-proof, and easily accessible. It is a shared record of transactions, distributed over a network of users. A blockchain is made up of a series of data blocks, each of which contains a set of transactions. Blocks are electronically chained together and locked with cryptography, and a public record of every transaction is established. The more blocks there are, the less probability exists that blocks can be altered. The biggest and best known blockchain implementation is the Bitcoin network.

Figure 1. Blockchain example



Blockchain advantages

- Decentralized
- Distributed
- Distributed consensus
- Tamper proof
- Transparency

In 2008, a pseudonymous person (or group) named Satoshi Nakomoto published a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System,” describing an open, real-time, distributed payments network. What made the idea unique was that it was an entirely peer-to-peer system that was not based on a centralized trusted authority. It allowed anyone to participate and was not controlled by any one entity. The record of transactions was openly available for all to see—a model that is in direct contrast to the current banking system. Bitcoin, built on blockchain, was subsequently implemented as an open source project that was released in January 2009.

It is important to draw a distinction between Bitcoin and blockchain. Bitcoin is a widely available, electronic cryptocurrency that can be used to purchase goods or services. Bitcoins are awarded to specialized network participant nodes, called “miners,” for validating transactions. This serves to incentivize and strengthen the network. Blockchain is the underlying technology that enables the Bitcoin network to operate in an open, autonomous, decentralized model, where trust is enforced through cryptography and not its participants. In essence, there would be no Bitcoin without Blockchain, but there can certainly be Blockchain without Bitcoin. The distinction is important because blockchain technology can be applied to other uses—for example, property deeds or tracking of diamonds from source to buyers—beyond the processing of electronic currencies.

Key advantages

Blockchain and the idea of distributed ledger technology offer several distinct advantages.

Decentralized—Blockchain is based on a peer-to-peer network design—where each participant, or node, in the network is equal to all others. This means no controlling entity can unduly influence the system. No central authority is required. The rules and behaviors of the network are embedded within the software protocol. The larger the network grows, the more standardized rules and behaviors are propagated, making it increasingly unlikely that any one actor, or multiple actors, could maliciously change the system's behavior.

Distributed—Each node on the network contains a complete copy of the entire ledger, from the first block created—the genesis block—to the most recent one. In the Bitcoin example, its ledger holds every transaction ever done on every participating node for the last seven years. This distributed approach increases the overall resiliency and security of the system. If any node or collection of nodes goes offline, the system will continue to function. An attempt to defraud the system by changing the ledger to a different truth would require a majority of all copies of the ledger to be compromised to convince the network of that different truth.

Distributed consensus—The design contains a radical innovation that solved the doublespending problem through a mechanism called "distributed network consensus." This mechanism enables the entire network to reach agreement about which blocks of transactions are valid and which ones are not, enabling peer-to-peer value exchange without involving a trusted third party or intermediary for that consensus. There are different models for distributed network consensus, for example, proof of work—employed by Bitcoin—or proof of stake.

Tamper proof (immutability)—Each transaction must be digitally signed using a participant's private encryption key, which is kept only by the signer. The digital signature on a transaction can be validated by a signer's corresponding public key. Public keys, as the name implies, are designed to be shared with anyone. This ensures a transaction can only be created by the holder of a specific private key. Once a transaction signature is validated, a transaction is cryptographically bound, through a mathematical algorithm called "hash." The hash function creates a unique digital fingerprint for the transaction. Transactions are then hashed with other transactions into a block. When a block of transactions has been accepted by the network, it is cryptographically bound to the ledger and distributed to all the nodes on the network.

Transparency—The distributed ledger contains a full history of every transaction, enabling traceability of each asset—digital coin or other asset tracked by the leger—back to its origin. With the distributed ledger published openly to every node on the network, it is easy for a network participant to unambiguously determine the current and past states of assets within the ledger. This creates a highly available, auditable trail of activities for each asset that has contributed to the current system state.

Implementations as blockchain evolves

Given blockchain's far-reaching capabilities, it is not surprising that different approaches and applications have evolved from its original intent. Examples of emerging blockchain uses include:

Digital Currency—Each participant is able to issue its own currency that can be used for digital services provided by that person or entity. The more trustworthy that person, entity or service is, the higher its market capitalization of the currency will be.

Proof of existence—Takes any document and stores its cryptographic digest, including a timestamp, onto the blockchain to prove that the document existed at the given time. A cryptographic hash function takes digital content, such as an electronic version of a mortgage document, and transforms it into a unique, fixed-sized string called the digest. The digest is public and can only be generated by its original source or document.

Smart property—Proves ownership of physical and nonphysical assets, such as software, money note, or cryptocurrency. Proof of ownership of any given smart property removes friction. It also creates new business opportunities by enabling trust-based trades between unknown entities.

Smart contract—Is computer code that executes contractual logic, agreed on by all participating parties. Essentially, a smart contract program code is based on "if-then" conditions. If an event in direct relation to its contract occurs, then a set action is triggered. Participants in a smart contract communicate directly via the blockchain, which removes the need for an intermediary and minimizes contractual-related transaction costs.

Decentralized autonomous organization (DAO)—Leveraging smart contracts, it runs on blockchain technology, making it possible to establish an associated set of contracts that collectively form an autonomous corporation called a "DAO." Such an organization would exist relying only on the blockchain space, so it would be completely virtual. Its behavior would be governed by rules embedded in the corporation's smart contracts. DAO corporate actions occur when transactions are added to the blockchain.

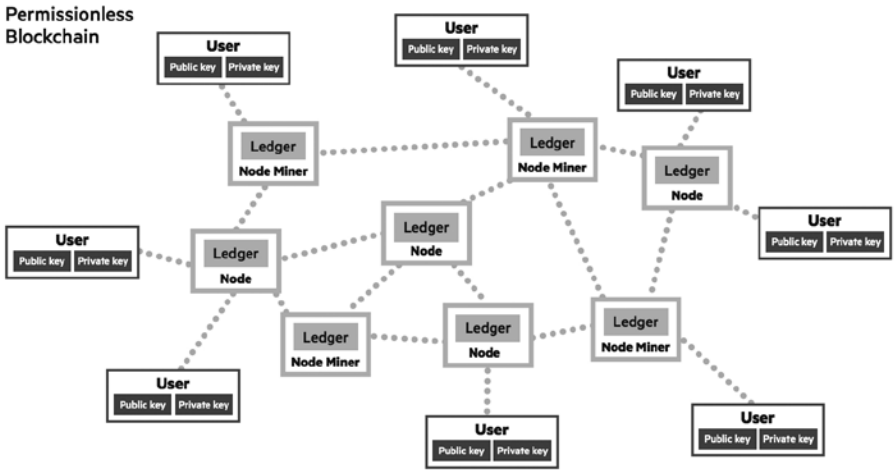
Based on these features, blockchain systems could be used to store records of digital value—transactions, identities, assets, documents, properties—into an immutable ledger, or to add self-enforcing business logic to the ledger, such as smart contracts. In general, there are currently two types of blockchain systems used to address the requirements of specific applications requirements:

- Permissionless—A public blockchain system open for participation to anyone. There is no central authority, group, or board required to allow participation. Cryptographic proof implemented within the distributed consensus mechanism replaces the need for trust in the process of transaction validation. The Bitcoin network is an example of a permissionless blockchain (see Figure 2).
- Permissioned—A private blockchain system, available only to a closed group of participants. There are two distinct variations on the permissioned blockchain system (see Figure 3):

  Distributed permissioned—A blockchain system for closed communities with similar, but competing, interests.

  Private permissioned—A blockchain system for one or more organizations that share common interests.

Figure 2. Permissionless blockchain



"…The consequences of this breakthrough (blockchain) are hard to overstate."

Marc Andreessen, Andreessen Horrowitz[1]

Transaction validation differs significantly between permissionless and permissioned blockchains. Permissionless blockchains, which are open to everyone, use miners that are incentivized by a cryptocurrency—Bitcoin or Ether—to guarantee legitimate transactions. Permissioned blockchains, which provide more restrictive access to transaction validation and insight into transaction history, rely on whitelists to permit participants—combined with some method of distributed consensus. Since there is no need for "proof-of-work," there is no need to incentivize with a financial reward. Many believe that permissioned blockchains are more appropriate for use by financial institutions due to possible issues with data privacy and concerns from regulatory bodies. Regardless of the type of implementation, the potential impacts of this technology on the financial services industry are substantial.

[1] http://dealbook.nytimes.com/2014/01/21/ why-bitcoin-matters/?_php=true&_type=blogs&_php=true&_

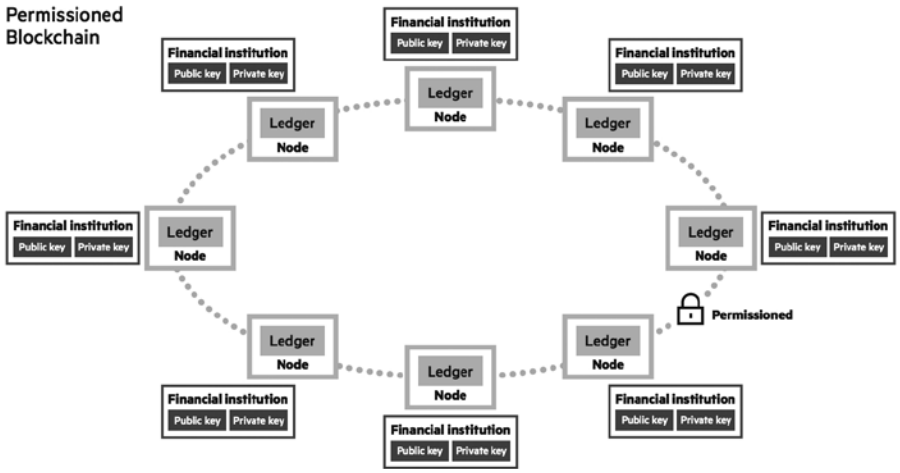


Figure 3. Permissioned blockchain

The current landscape

A number of financial institutions are exploring distributed ledger technology, while others have been actively investing time and/or funds in this area. See Figure 4.

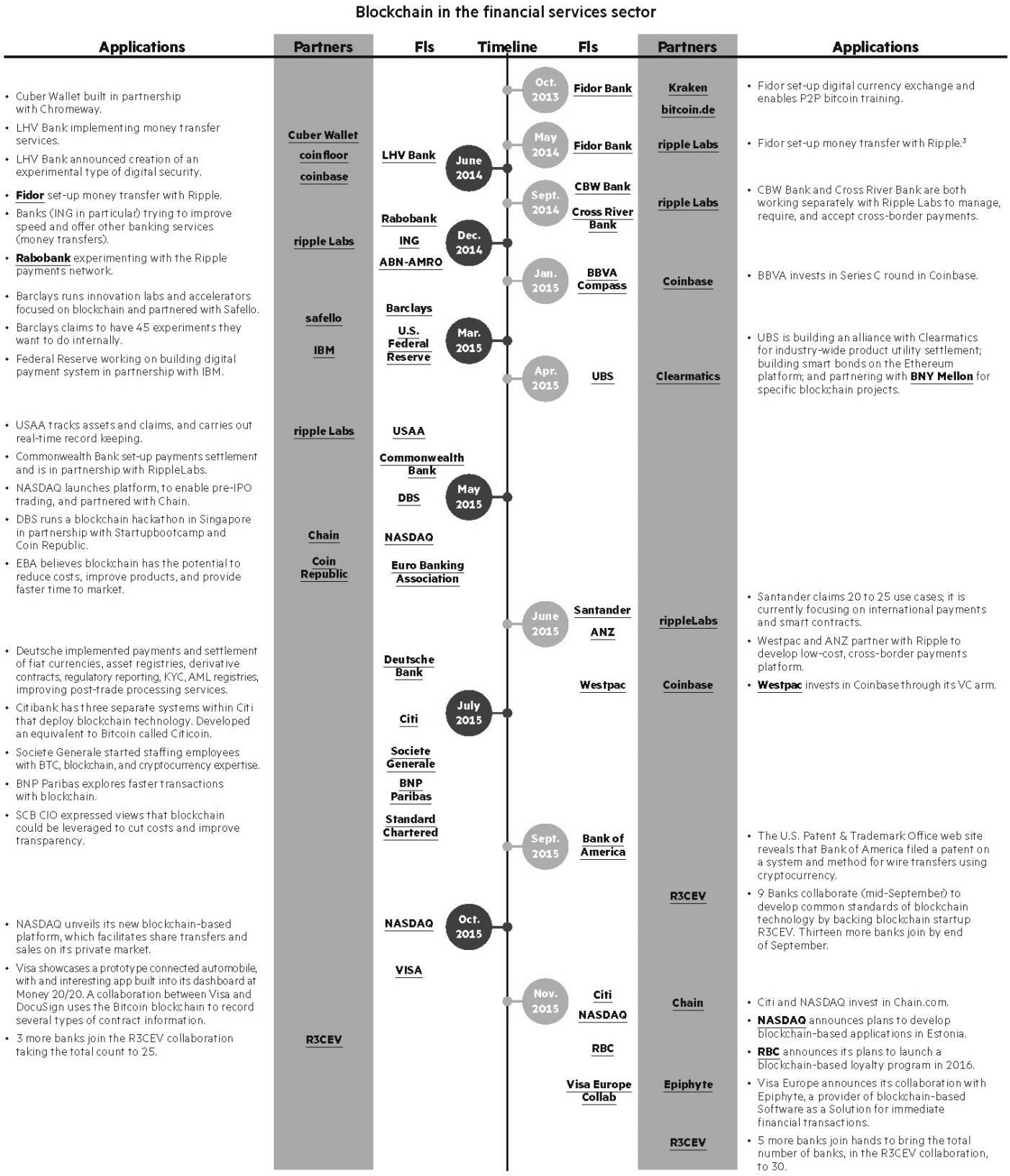
Blockchain has real potential to transform the financial services sector. Financial institutions need to look closely at specific areas where blockchain technology can disrupt their organizations and how to bring the whole ecosystem of stakeholders, such as regulators, governments, banks, and academics, along on the journey. Institutions should collaborate to explore and develop new uses for blockchain that could deliver expected and needed business value.

Blockchain could, for example, overhaul a legacy global banking system and lead to much faster payments. This will reinforce the work Australia is doing with its New Payments Platform, scheduled to come online in 2017. Regulators in Australia are putting on pressure to accelerate the payments business and change the aging infrastructure. Regulators in the U.S. and China have also pushed for faster payments. There is significant potential for blockchain technology to streamline business-to-business (B2B) payments in particular and solve the increasingly troubling issues in the area of cross-border friction and large payment volumes that are often exclusive to B2B. Other examples of potential blockchain applications include foreign exchange and currency exchange.

For this to happen, financial institutions must separate blockchain technology from its most prominent current implementation: ungoverned miners that rely on an unregulated digital currency as payment. People tend to confuse Bitcoin and blockchain, and it is alarming to see they cannot separate one from the other. For any potential uses to get any serious traction in financial institutions' boardrooms, that separation must happen.

Several recent initiatives, such as the distributed ledger experiment Citibank is working on, and the partnership between Ripple and Earthport, are addressing this issue.[2] However, for blockchain to succeed as an alternative technology and new set of "guardrails" for transferring funds globally, standards and governance must be established to protect assets, institutions, and the people who will rely and transact on this emerging system.

[2] http://www.coindesk.com/meet-the-25-banksworking-with-distributed-ledger-startup-r3/



The original graphic appeared in Financial Institutions: Blockchain Activity Analysis, Let's Talk Payments, December 2015. The format has been modified and content slightly amended for this document.

Figure 4. Financial institutions' involvement with blockchain

People tend to confuse Bitcoin and blockchain, and it is alarming to see they cannot separate one from the other. For any potential uses to get any serious traction in financial institutions' boardrooms, that separation must happen.

Blockchain-based businesses ecosystem

Large financial institutions don't feel the impact of startups initially, because they typically do not attack existing players head-on. Rather, many startups go around incumbents, and it takes a while before their market presence is visible or felt by larger players. Despite all of that, banks continue to grow, and their assets continue to increase, as do their profits. That, however, does not mean they are not being impacted by Fintech or blockchain technology.

There are more than 190 blockchain-based startups involved in or around the financial services industry—categorized as applications, middleware, or infrastructure players.

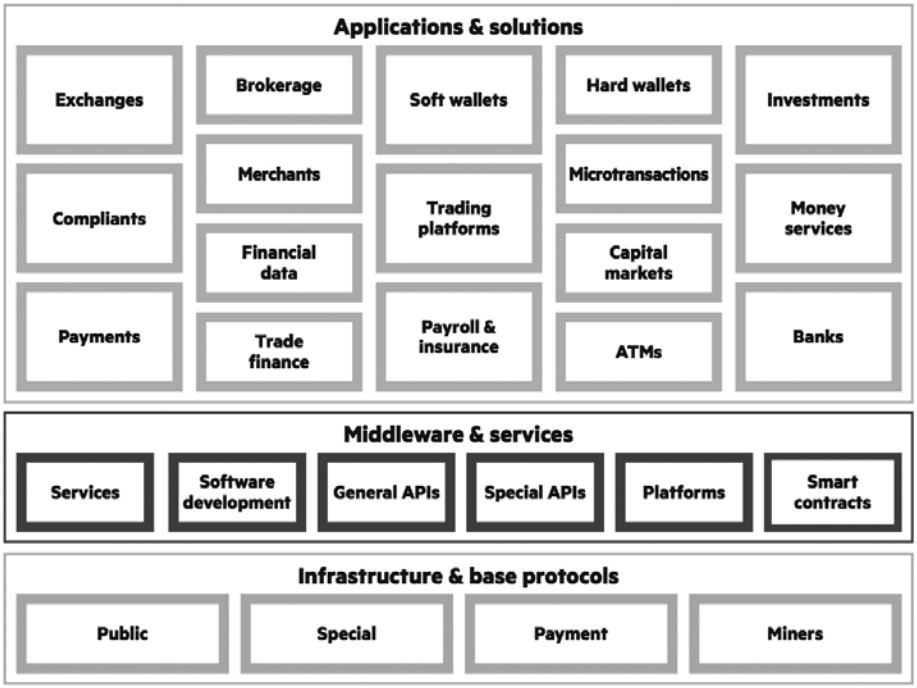


Figure 5. Blockchain ecosystem

Applications and solutions

- Exchanges are differentiated from brokerages, because they typically offer more real-time currency exchange capabilities. In contrast, brokerages have more latency in transaction movements.
- Wallets are simply divided into soft vs. hard. Not all soft wallets are the same—some allow a user to keep the cryptocurrency in a smartphone vs. others use a smartphone to unlock access via password or cryptographic keys.
- Capital markets are where a lot of activity is happening—from venture capital firms and startups trying to solve the challenge of clearing-to-settlement post trade.
- Money services primarily target the multibillion-dollar business of global remittances.
- ATMs are developing additional services to become more than Bitcoin money withdrawal machines.

Middleware and services

This category aims at developers who want to build applications and innovate on top of the underlying blockchain and consensus protocols. All of the groupings in this category offer various entry points—including interacting with APIs, overlay technologies, integrated development environments, and a choice of software languages.

Infrastructure and base protocols

This category represents the infrastructure and base protocols that are still evolving, and the public mining infrastructure—for Bitcoin—that validates and secures the network. This category is typically in the space of core developers that are well versed in cryptology-based software technologies.

Considerations when evaluating a blockchain solution

There are many ways in which the blockchain model could be used to streamline current business practices, such as cross-border payments, remittances, and trade settlements, or enable new business opportunities such as smart contracts for insurance claims settlements. Despite the significant promise that blockchain presents, the technology is still rapidly evolving.

As previously noted, many financial institutions and technology companies are in the exploratory stage, experimenting with the technology, and participating in proofs of concept to better understand its possibilities and limitations. Given the hype of the media coverage about blockchain, at this stage it is easy to get lost in the allure of the technology. Many new and interesting blockchain-based solutions emerge every day.

Organizations should evaluate the technology through a technical lens, and from a holistic business perspective, considering a number of key issues:

Regulatory and compliance implications—In the aftermath of the financial crisis of 2008, government regulators have pushed for stronger oversight and control over financial institutions in an effort to provide safety mechanisms to prevent future occurrences. Governments now also have a heightened sensitivity to any significant developments in the industry. It is likely that any significant new innovations related to core functions in the banking industry will face stringent regulatory scrutiny.

Data privacy—One of the fundamental tenets of blockchain is the immutability of the data in the distributed ledger. Data cannot be changed once it is validated and bound to the ledger. In addition, data in the ledger will persist for as long as the system exists. With the ledger being distributed across the network and openly available to all participants, it is imperative to carefully consider any potential privacy concerns with the data that is being stored in it. Will there be any personally identifiable information in the ledger? Will that data be encrypted?

Operational concerns—As with any production system, a blockchain solution must be considered from an operational perspective. Depending on how the solution is integrated with a financial institution's legacy applications, there are potential impacts in the areas of technology operations and systems support. As technology or business process issues arise, how will incident root-cause analysis and resolution be handled? Will there be new staff training requirements? How will capacity planning, from a technology and staffing perspective, be done? How will business continuity be addressed?

Data standards—Depending on the applications, various types of data may be stored in the distributed ledger. Solutions are emerging that will use blockchain technology beyond the payments realm. As noted earlier, blockchain solutions can be deployed in open, "permissionless" networks, such as Bitcoin, or in private, "permissioned" networks where participants are known to each other. In either case, for such solutions to be successful, network participants must agree on standards for formatting, structure, and taxonomy of the stored data. Those standards must be clearly defined, communicated, and enforced within the inherent rule-based structure of the network.

Data analytics and actionable insights—In a constantly growing blockchain ledger, organizations will need ways to look up the history and make sense of it—essentially blockchain business intelligence and analytics. Without robust blockchain-oriented analytics, valuable actionable insights could be lost, reducing potential return on investment.

Network governance—Blockchain is by nature a decentralized solution with no single controlling authority. Some form of governance structure will need to be in place, however, particularly for permissioned or private blockchain solutions likely to be used by financial institutions. Governance is needed to provide and maintain an agreed-on set of rules for participation, onboarding, issue resolution, and other activities. Participants must understand the network rules, and also how they are established, enforced, and maintained.

Scalability—The current most popular implementations of blockchain solutions on the market—Bitcoin and Ethereum—rely on different validation speeds. Bitcoin verifies a block in 10 minutes, on average, and a record is assumed to be confirmed after 6 validations. So it takes a full 60 minutes to have cryptographic proof that funds were successfully and securely transferred. In contrast, Ethereum currently needs 17 seconds on average per block to do the same. While this is a great achievement in speed of value transfer for individuals, it might not fulfill the needs and requirements for interbank payments and high-volume transactions. Different use cases will require different blockchain-based solutions.

Security—It is essential to secure your digital wallets when considering the use of blockchain technology in combination with any cryptocurrency—an existing one like Bitcoin or your own. Any digital funds are assigned to a public key, and the corresponding private key is stored in digital wallets protected with a passphrase. A digital wallet could be considered as a traditional account, and it is likely that banks might have many accounts to fulfill business needs. There are different forms for different types of devices available. Even paper wallets are available to avoid the necessity to have any digital device at all. To access funds, a strategy for managing and maintaining access is crucial. There needs to be means of recovering lost or forgotten passphrases, and a strategy of where and how to store private keys securely—digital online, digital offline, or paper.

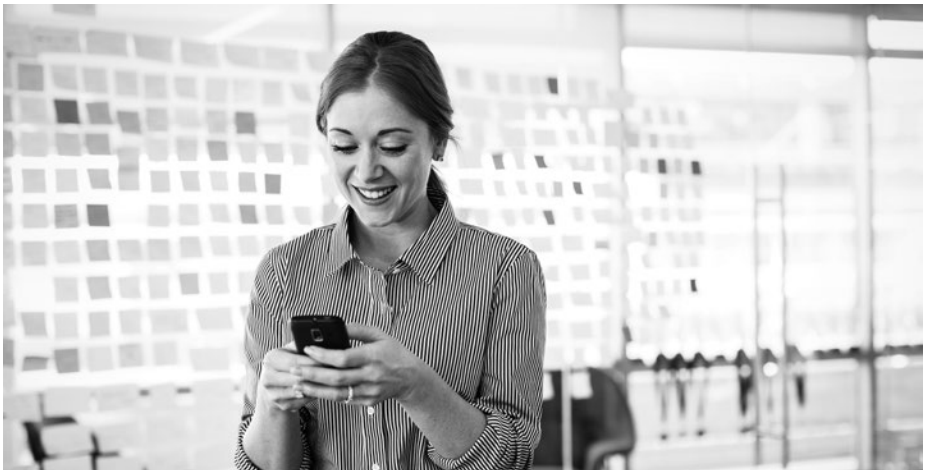
The potential is there—take the next steps

Blockchain has the potential for significant disruption in multiple areas within a business. If properly harnessed, it can create significant opportunities. Forward-looking organizations will foster a culture that is open to adopting blockchain.

Financial institutions should understand the threat that blockchain poses, and also look at it as a possible strategic enabler to transform the way they do business. Don't look at the existing business as an inhibitor to agility. Rather, consider your loyal customer base, deep domain experience, and considerable knowledge of industry regulatory requirements as a strategic advantage over emerging competitors. Determine ways to leverage these advantages in combination with blockchain and other new technologies to create a sustainable competitive edge.

The key steps for blockchain adoption include:

- Prepare your organization to accept disruption and fluidity across the business and economy.
- Adopt a management style focused on agility, innovation, and self-reliance.
- Plan for and test nonhierarchical organizational models as part of work decentralization.
- Evaluate potential blockchain use cases for your financial institution or ecosystem. Look for opportunities to streamline existing business processes or create new offerings.
- Create an investment plan to fund hackathons, proofs of concept (POCs), and/or partner with blockchain specialized companies—including start-ups.
- Start POCs for blockchain development and test specific use cases relevant to your financial institution. Adopt a "fail-fast" approach to encourage rapid learning.
- Share the results with your stakeholders and continue with an iterative approach to refine your POC.



Help is available

DXC Technology has a rich heritage of working with game-changing technologies. Innovation is in our DNA. We have a 35-plus year history in the financial services industry and a significant presence in all of the top 200 banks, top 50 brokerages, 130 of the world's major stock and commodity exchanges, and top 50 insurance carriers. Drawing on that knowledge and experience, we can help you at all points along your blockchain journey, from initial strategy through to implementation and ongoing operations. Work with DXC to:

- Facilitate strategy and planning workshops
- Rapidly prototype and develop a POC
- Host, manage, and operate a blockchain environment
- Partner with blockchain solution providers

Get proven expertise and a worldwide presence with DXC. Let us help you formulate, develop, and execute an innovative blockchain strategy to transform the way you do business.

About DXC

DXC Technology (NYSE: DXC) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner alliance combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.

DXC_4AA6-5864ENW. July 2016