American Bankers Association

Understanding Blockchain

Blockchain—a distributed ledger technology that facilitates payments—has the potential to transform banking. Although the emergence of bitcoin originally put blockchain into the spotlight, it's the integration of the technology into mainstream financial services that has grabbed the attention of banks, regulators and venture capitalists from around the world.

The blockchain enables multiple parties to trade assets without a trusted third-party to clear transactions. The technology has yet to see mainstream adoption, but it could substantially reduce operational costs and increase transactional efficiency in payments, trade finance and securities settlement. Globally, banks and regulators are researching blockchain use cases and acknowledging the financial services implications. It is uncertain today what the full impact of blockchain integration will be, but it has the potential to transform banking.

It is important for banks of all sizes to learn how the blockchain works, its possible applications and how it could affect their business. By participating in discussions and collaborating with stakeholders, banks can play a significant role in shaping the future of blockchain technology.

Virtual Currency vs. Blockchain

It is easy to get confused by the differences between virtual currencies and the underlying blockchain that facilitates the transaction.

Virtual currencies—of which bitcoin is the most prominent—are digital representations of value. They are marketed directly to consumers and used in place of government-issued money. A virtual currency stores value, as traditional currencies have for centuries. Although few merchants accept them, they have a market value based on demand and limited supply. While not recognized as fiat money, owning a virtual currency is similar to owning a foreign currency. There is an exchange rate (often volatile) and it can be traded for dollars. Virtual currencies are also often pseudonymous, granting users a degree of privacy.

For a virtual currency to be effective, it must be difficult to counterfeit and prevent individuals from spending the same unit of currency twice, referred to as double-spending. To solve these problems—amongst other goals—Satoshi Nakamoto, the alias of the anonymous originator of bitcoin, developed the blockchain in 2008 to power the virtual currency.

Blockchain is the underlying technology that powers most virtual currencies. The blockchain is the "ledger" (a permanent summary of all accounts) that keeps track of virtual currency transactions allowing users to establish ownership of their virtual assets. Much like the Internet enables users to navigate the World Wide Web, the blockchain

enables individuals to acquire and trade virtual currencies. However, its use is not limited to facilitating bitcoin transactions. The blockchain can be used to facilitate the exchange of **any** digital asset.

The Federal Reserve and the Current Payments System

Currently, the Federal Reserve acts as the trusted intermediary holding the master ledger for banks in the United States. Each bank has an account with the Federal Reserve, either directly or through a correspondent bank. If, for example, the customers of Bank A send $1,000,000 in payments to Bank B and the customers of Bank B send $300,000 in return over the course of the day, the Federal Reserve will debit Bank A and credit Bank B's account $700,000, respectively. However, clearing payments through an intermediary takes time, and holding an account at the Federal Reserve has a cost. The blockchain, in its simplest form, distributes this ledger to all participants. Transactions are updated and verified by all parties in unison, eliminating the need for a third party intermediary.

How it Works

The blockchain, in essence, is a shared ledger. It records transactions into "blocks" and then uses a cryptographic signature to add each block to the "chain" of preceding transactions. In order to add a new block to the chain, the transaction must first be verified by all participants in the network. This process, called *consensus*, prevents fraudulent activity.

Proof of Work vs. Proof of Stake

There are multiple ways to reach consensus on the blockchain. In a permissionless system, all parties have access to the ledger and consensus is achieved through *proof of work*. Proof of work relies on network participants to contribute computing power towards solving computationally difficult problems. This computational process, sometimes called mining, is used to validate new blocks. Participants that volunteer computing resources to the network are rewarded with virtual currency as an incentive.

Proof of work is said to be permissionless because anyone with a computer can participate. However, as transactions are added and the ledger grows, the costs of consensus rise. Increasingly more time and processing power are required to receive a virtual currency reward.[1] Any blockchain system adapted by the financial services industry must resolve this resource bottleneck in order to assure agility and scalability.

In a permissioned system, transactions are verified by *proof of stake*. Proof of stake requires the virtual currency be distributed prior to network launch. Individuals purchase a certain amount of the currency in a presale, which gives them permission to participate in the network. Instead of requiring participants to solve a computational problem, they must only prove they have a stake in the network (by owning an amount of the network's native currency) in order to validate a new block.[2]

BitFury Group's "Proof of Stake versus Proof of Work" white paper explains the rationale behind proof of stake

"[U]sers with the highest stakes in the system have the most interest to maintain a secure network, as they will suffer the most if the reputation and price of the cryptocurrency would diminish because of the attacks. To mount a successful attack, an outside attacker would need to acquire most of the currency, which would be prohibitively expensive for a popular system."

Each technique has its own strengths and weaknesses; however, permissioned systems benefit from an agility and scalability that permissionless systems lack. In adopting blockchain technology, the financial services industry will likely use a form of permissioned network.

Blockchain as Smart Contracts

The blockchain can also be used to implement "smart contracts," which are self-executing applications written in blockchain code. These smart contracts can be written to ensure that transactions are carried out in a specific manner between multiple parties to reduce counterparty risk. Smart contracts can further diminish the role of intermediaries. For example, Banco Santander, S.A., believes that smart contracts can be used to automate the payouts by the counterparties to swap contracts.[3]

An Example: Homeownership on the Blockchain

To better explain these concepts, consider homeownership as an example. Homeownership is not proven because a person possesses a key to the front door. Homeownership is proven because an individual's name is listed on the final deed of sale. This deed of sale is recorded and held in an official place, usually a local courthouse or municipal public records office, where anyone can see it and confirm ownership.

The blockchain is like the courthouse in the above example. It is the official record of all transactions, listing the current owners of all circulating assets. Unlike the local courthouse, the blockchain is a **distributed** ledger of ownership, which means there is not only one official record of ownership. Instead, every participant in the system has a copy of the official record, and whenever a transaction is made, agrees in near-real time on the revision to the ownership record.

By distributing ownership of the ledger, ownership can be quickly and efficiently transferred. No need to visit the local courthouse—or the central bank—waiting for a transaction to be recorded and confirmed, because recording and confirming happens in real time. Another benefit of a distributed ledger is its transparency. The public nature of the ledger enhances payment transparency, which prevents fraud, counterfeiting and double-spending.

Blockchain Use Cases

The blockchain has the potential to substantially reduce operational costs in the delivery of financial services. The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services, a World Economic Forum report,[4] details many of the benefits blockchain can bring to the financial sector. The immutable nature of the blockchain enables asset origination and transaction history to be permanently recorded within a single shared ledger, dramatically reducing the propensity of fraud. The distributed ledger disintermediates central clearinghouses to provide transaction verification and validation while significantly reducing settlement times. Faster settlement would improve bank liquidity by freeing up capital. Moreover, smart contracts coded on the blockchain automate the manual processes required to perform settlement and resolve disputes, and reduce human error. Smart contracts also mitigate counterparty risk because conditional obligations can be programmed to execute automatically. These benefits have potential to improve efficiencies in several sectors—particularly payments, trade finance and securities settlement.

Payments

The first and best known blockchain application addresses inefficiency in payments. Virtual currencies are strong proofs-of-concept demonstrating the blockchain already can facilitate payments reliably and securely.

Financial institutions began to take notice of the technology underlying bitcoin in 2013, focusing on costly and time-consuming cross-border payments. Costs arise from fees paid to correspondent banks and other intermediaries, and several days can be required for verification and validation to take place. Furthermore, routing payments through intermediaries presents more potential failure points and lead to a higher rate of false positives.[4] This delayed settlement time also leads to higher amounts of idle capital at financial institutions.

A single, shared ledger eliminates the need for redundant validation steps and enables direct communication between sending and receiving institutions. The necessity, and resulting cost and time, of intermediaries is removed. Moreover, the speed of blockchain transactions and confirmation frees up capital. As costs evolve and blockchain becomes customary, new services may become viable, such as micropayment consumer services.[4]

Micropayments: A financial transaction involving a very small payment. Micropayments generally occur online. Users pay each time they access a service. (example: Making a $0.01 payment to read a news article online)

Trade Finance

Blockchain also can improve efficiencies in trade finance, an industry valued annually in the U.S. at more than $10 trillion.[5] Known for being particularly complex, trade finance has numerous stakeholders and intermediaries, and processes require multiple legal contracts, complicated global logistics, uncertainty, and significant time from initiation to completion of a transaction.

Exporters rely on invoice factoring, selling their accounts receivable at a discount to receive short-term financing, a practice that compounds default risk if delivery fails.[4] Banks have

difficulty verifying the authenticity of the bills of lading, conclusive receipts serving as title to goods.[4] Tracking the flow and quality of goods is further complicated by inconsistencies among intermediaries, which may use incompatible platforms and data reporting. Payments may require weeks for settlement.

A shared ledger would enable import and export banks to communicate directly—circumventing correspondent banks, and reducing the potential for delivery failure. It could also standardize reporting structures, and allow tracking of goods in transit by all stakeholders. Blockchain would decrease fraud risk as goods pass through global checkpoints. This transparency would assist banks in tracking invoices, viewing complete financing history, and verifying bills of lading. Once goods are delivered and conditional contract terms are fulfilled, the blockchain-enabled smart contract can be programmed to automate settlement. As a result, settlement time is reduced significantly, and pledged capital is freed.

Securities Settlement

By enabling faster settlement, Blockchain also presents an opportunity to reduce credit and market risk in securities transactions. Securities settlement generally occurs three days after a transaction is executed, known as t+3, which restricts the use of investor funds until the transaction clears. Parties must account for the risk that a counterparty is unable to fulfill their contractual obligation. The multiple parties to a transaction can lead to inconsistencies needing time to reconcile. These inconsistencies can cause incorrect settlement. Similar to other complex transactions, the fees owed to various intermediaries are costly.

As distributed ledgers allow new operational efficiencies, settlement time could be reduced to almost t+0.[4] As in the trade finance use case, smart contracts used in securities settlement could automate validation, reduce manual errors and settlement risks, and funds can be available to customers instantly, which allocates a more efficient use of investor resources. In fact, Banco Santander, S.A., estimates that banks could save up to $20 billion annually by 2022 by adopting blockchain technology.[3]

Market Activity and Blockchain Investments

Banks and technology companies are experimenting with various use cases of blockchain, and will invest more than $1 billion on blockchain technology in 2016,[6] an investment equal to the aggregate venture capital investment in blockchain over the last four years.[7] Below are some additional blockchain developments that have taken place in the financial services industry.

Ripple—In September 2016, Ripple, a global provider of enterprise blockchain solutions that includes fifteen of the top 50 global banks, founded the Global Payments Steering Group to focus on interbank global payments based on blockchain technology. The group will oversee the creation and maintenance of Ripple payment transaction rules, formalize standards for activity and promote implementation of Ripple payment capabilities. Ripple also has 10 banks in commercial deal phases, and has completed more than 30 bank use case pilot programs.

R3CEV—In September 2015, nine founding financial institutions launched the blockchain consortium R3CEV. In April 2016, the consortium, now with more than 60 members, released Corda, a distributed ledger platform for financial services. In October 2016, R3CEV announced that it would make the Corda code publicly available.

The Corda platform is part of R3CEV's Concord project, a more comprehensive blockchain product. Concord is designed to streamline back office functions to address operational challenges, such as governance and internal record-keeping.

Hyperledger Project—In December 2015, the Linux Foundation announced the Hyperledger Project, a collaborative open-source effort to advance blockchain technology by developing a cross-industry open standard. In February 2016, they announced 30 founding members, including Accenture, IBM, JP Morgan, R3CEV, SWIFT and Wells Fargo. The Hyperledger Project has grown to more than 80 members and continues to accept code contribution proposals on its open source blockchain standard.

Bank Developed Virtual Currencies—In August 2016, Swiss bank UBS partnered with Deutsche, Santander, BNY and ICAP on a new blockchain-based virtual currency. The currency will enable financial institutions to trade securities without a clearing house. The group is educating central banks and aims for a restricted low-risk commercial launch by early 2018. In October 2014, Goldman Sachs filed a patent for a securities settlement system based on its virtual currency, SETLcoin. In July 2015, Citigroup was revealed to be experimenting with its own blockchain-based currency, Citicoin.

Visa—In October 2016, Visa announced a partnership with Chain, a blockchain technology firm, to deploy Visa B2B Connect, a platform Visa is developing to enable financial institutions to process international business-to-business (B2B) payments.

Regulators

Much of the regulatory activity related to blockchain has been focused on the legal designation of virtual currencies. However, regulators are also learning about blockchain and its financial services implications. Below are important regulatory developments that have taken place regarding blockchain and related virtual currencies.

FinCEN: Bitcoin as Money Service Business, Money Transmitter. The first announcement by a government agency related to blockchain was by the Financial Crime Enforcement Network (FinCEN) in March 2013. The guidance required some virtual currency intermediaries to register as money service businesses (MSB), or money transmitters, which are required to comply with state licensing laws. FinCEN later clarified that an intermediary mining bitcoin "for themselves" does not need to register as an MSB.[8]

In October 2014, FinCEN released new guidance for virtual currency exchanges and payment processors, establishing such companies may be considered MSBs. In May 2015, FinCEN fined Ripple Labs $700,000 for "willfully violating several requirements of the Bank Secrecy Act." FinCEN stated that Ripple operated as an MSB without proper authorization and issued its own currency without sufficient anti-money laundering (AML) compliance. In August 2015, FinCEN announced that companies using blockchain technology to transfer commodities qualify as money transmitters.

IRS: Bitcoin as property. In May of 2014, the IRS announced that, for tax purposes, virtual currencies are property, not currency. Therefore, the rules used to govern stocks and barter transactions will apply to blockchain-based currencies. Consider the purchase of real estate with bitcoin, a volatile virtual currency, as an example. If Bank A purchases $10 million in bitcoins and then uses all of those bitcoins to make an $18 million real estate purchase, the resulting capital gains would be $8 million. Some have speculated that the ruling would lead to a decrease in bitcoin transactions due to the complicated nature of calculating capital gains on each virtual currency-based purchase.

SEC: Bitcoin as securities. In November 2013, in response to a Senate hearing on bitcoin, SEC Chairman Mary Jo White issued a statement saying virtual currencies may be considered securities in certain circumstances. A virtual currency may be considered a security if packaged and sold as an investment. In enforcement, the SEC has taken action against Ponzi Schemes trading bitcoin.

CFTC: Bitcoin as commodity. In September 2015, the CFTC charged bitcoin startup Coinflip Inc. and CEO Francisco Riordan with engaging in activities related to commodity options without registering with the CFTC. In the enforcement action, the agency wrote:

> Section 1a(9) of the Act defines "commodity" to include, among other things, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in." 7 U.S.C. § 1a(9). The definition of a "commodity" is broad. See, e.g., Board of Trade of City of Chicago v. SEC, 677 F. 2d 1137, 1142 (7th Cir. 1982). Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.

FSOC: Blockchain and systemic risk. In June 2016, the Financial Stability Oversight Council (FSOC) discussed the potential risks posed by new financial products and delivery mechanisms, such as blockchain technology. While distributed ledgers are viewed by many in the financial industry as a secure way to reduce third-party transaction costs and risk exposures, FSOC warned that "operational vulnerabilities associated with such systems may not become apparent until they are deployed at scale" and that some systems may be vulnerable to fraud executed through collusion among a significant fraction of participants in the system." The council said:

> Risks embedded in new products and practices may be difficult to foresee. Financial regulators will need to continue to be vigilant in monitoring new and rapidly growing financial products and business practices, even if those products and practices are relatively nascent and may not constitute a current risk to financial stability.

Federal Reserve: Blockchain Working Group. In October 2016, speaking at the Institute of International Finance Annual Meeting, Federal Reserve Board Governor Lael Brainard said that the Fed has convened a working group on blockchain to review its uses for financial services.[10] They expect to publish a report on their findings by the end of 2016. Brainard said the working group is looking at how blockchain can improve the efficiency of the payments system without compromising public confidence.

SEC: Blockchain in the securities market. At the Fintech Forum, an event hosted by the SEC in November 2016, chair Mary Jo White said that it was an ideal time to discuss the role of fintech in the securities market. Regarding blockchain, White said the "technology could greatly simplify the trading, settlement and clearing processes, making transactions faster, more efficient, and less expensive."[11] The SEC has put together a Distributed Ledger Working Group to evaluate when and how blockchain will be on-boarded within the securities market.

Take-Away for Banks

Today the challenges facing widespread adoption of blockchain lie in creating a robust infrastructure that can leverage the technology while safely facilitating real-world transactions. Essential regulatory and ecosystem matters must be addressed before the technology becomes a mainstream operational framework.

Transparency and security. The pseudonymous nature of blockchain transactions fosters privacy, but also raises Bank Secrecy Act (BSA), Antimoney Laundering (AML), and Know-Your-Customer (KYC) concerns. Lawmakers, regulators, consumers and other stakeholders need to determine the appropriate level of transparency while guaranteeing the security and privacy of sensitive information.

Reversibility. The decentralized nature of blockchain enables faster transactions, but also raises Regulation E concerns, which allows customers to have unauthorized transactions reversed. It is uncertain how disputes would be resolved in a decentralized network.

Smart contracts. Smart contracts can automate transactions to reduce counterparty risk; however, unforeseen issues may arise regarding the specific language and code of the agreement. Regulators, and the US court system, need to determine how, and to what extent, smart contracts are legally enforceable.

Standardization. Standards need to be adopted to ensure interoperability among institutions, as much of the promised value of blockchain requires ubiquity and scale.

As the industry works to tackle these issues, it is important that bank senior management have a rudimentary understanding of blockchain and its applications in order to determine how blockchain-enabled processes could improve internal efficiencies. This understanding can be reflected in the bank's strategy plan, which can be written with an openness to blockchain technology, innovation and fintech. By participating in discussions and collaborating with stakeholders, banks of all sizes can play a significant role in evolving blockchain opportunities and realizing operational efficiencies.

---

[1] "Proof Of Stake Versus Proof Of Work Whitepaper". *The BitFury Group.* N.p., 2016. Web.
[2] Williamson, Nick. "Permissionless Vs Permissioned Consensus & Tradeoffs". Credits.vision. N.p., 2016. Web. 26 Sept. 2016.
[3] "The Fintech 2.0 Paper: Rebooting Financial Services". Finextra. N.p., 2016. Web.
[4] "The Future Of Financial Infrastructure: An Ambitious Look At How Blockchain Can Reshape Financial Services". *World Economic Forum.* N.p., 2016. Web.
[5] "Improving The Availability Of Trade Finance In Developing Countries: An Assessment Of Remaining Gaps". *World Trade Organization*. N.p., 2015. Web.
[6] Johnson, Richard. "Blockchain Adoption In Capital Markets | Greenwich Associates". *Greenwich.com.* N.p., 2016. Web.
[7] "Blockchain Startup Investment Bounces Back". *CB Insights – Blog.* N.p., 2016. Web. 26 Sept. 2016.
[8] "Application Of Fincen's Regulations To Persons Administering, Exchanging, Or Using Virtual Currencies | Fincen.Gov". *Fincen.gov.* N.p., 2013. Web. 2 Nov. 2016.
[9] "Financial Stability Oversight Council 2016 Annual Report". *https://www.treasury.gov.* N.p., 2016. Web. 2 Nov. 2016.
[10] "FRB: Speech – Brainard, Distributed Ledger Technology: Implications For Payments, Clearing, And Settlement – October 7, 2016". Federalreserve.gov. N.p., 2016. Web. 29 Nov. 2016.
[11] "SEC.Gov | Opening Remarks At The Fintech Forum". Sec.gov. N.p., 2016. Web. 26 Nov. 2016.