Preparing for Blockchain

CHALLEGES AND ALTERNATIVES FOR FINANCIAL REGULATORS

BY RITT KEERATI

Prepared with financial support from:

Center for Technology, Society and Policy (CTSP)
University of California, Berkeley

Table of Contents

I. Executive Summary

Blockchain—a distributed ledger technology that maintains a continuously-growing list of records—is an emerging technology that has captured the imagination and investment of Silicon Valley and Wall Street. The technology has propelled the invention of virtual currencies such as Bitcoin and now holds promise to revolutionize a variety of industries including, most notably, the financial sector. Accompanying its disruptive potential, blockchain also carries significant implications and raises several questions for policymakers. How will blockchain change the ways financial transactions are conducted? What risks will that pose to consumers and the financial system? How should the new technology be regulated? What roles should the government play in promoting and managing the technology?

This project seeks to help U.S. financial regulators and policymakers address some of these questions. It also seeks to enhance their understanding of blockchain and its challenges for the financial industry. Through a series of literature reviews and expert interviews, the project identifies major trends in the blockchain and distributed ledger space, determines potential risks and challenges facing financial regulators, and proposes potential policy alternatives to address these issues. Below are key takeaways of the project:

- Blockchain and distributed ledger technology hold the power to disrupt the financial sector and other industries. It enables parties lacking pre-existing trust to transact with one another without the need for intermediaries or central authority. This has the potential to revolutionize how financial transactions are conducted, eliminate certain roles of existing institutions, improve transaction efficiencies and reduce costs.

- Despite its massive potentials, blockchain is still in its early innings in terms of deployment. So far, the adoption of blockchain within the financial industry has been to facilitate business-to-business transactions or to improve record-keeping processes of existing financial institutions. Besides Bitcoin, direct-to-consumer applications remain limited, and such applications still rely on the existing financial infrastructure. For instance, although blockchain has the potential to disintermediate banks and enable customers to transfer money directly between each other, money transfer applications using blockchain are still linked to bank accounts. As a result, financial institutions still serve as gatekeepers, helping ensure regulatory compliance and consumer protection.

- With that said, the technology is continually evolving, and new use-cases are emerging rapidly. Accompanying these developments are risks and challenges. From the regulators' perspectives, key risks include: (1) lack of clarity on compliance requirements, (2) challenges in regulating new business models, (3) potential technical glitches, (4) potential new systemic risks, and (5) challenges in controlling bad actors. To mitigate these issues, effective interaction between regulators and industry participants is crucial.

- **Currently, there is a lack of unified and effective engagement by regulators and policymakers in the development and deployment of blockchain. Soundly addressing these matters will require better collaboration among regulators and more frequent interactions with industry participants.**

- Rather than maintaining status quo, policymakers may choose among these alternatives to enhance collaboration between the regulators and industry participants: (1) adjustment to existing regulatory

frameworks, (2) issuance of regulatory guideline, (3) creation of multi-party working group, and (4) establishment of regulatory sandbox. The best solution will be a combination thereof.

- For policymakers, the most important near-term goal should be to ensure that regulators are well educated about blockchain and that they understand its trends and implications. With respect to regulatory compliance, policymakers should be attentive to the adoption of the technology by existing financial institutions, particularly in the area of money transfer, clearing and settlement of assets, and trade finance. Longer-term, Congress also ought to find ways to reform the existing financial regulatory framework and to consolidate both regulatory agencies and regulations.

The emergence of blockchain and digital ledger technology represents a potential pivot-point in the ongoing global efforts to apply technology to improve the financial system. The United States has the opportunity to strengthen its leadership in the world of global finance by pursuing supportive policies that promote financial technology innovation, while making sure that consumers are protected and the financial system remains sound. This will require a policy framework that balances an open-market approach with a circumspect supervision. The next 5-10 years represents an opportune time for U.S. policymakers to evaluate their approaches toward financial regulation, pursue necessary reform and adjustment efforts, and work together with technology companies and financial institutions to make the United States both a global innovation hub and an international financial center.

II. What is Blockchain?

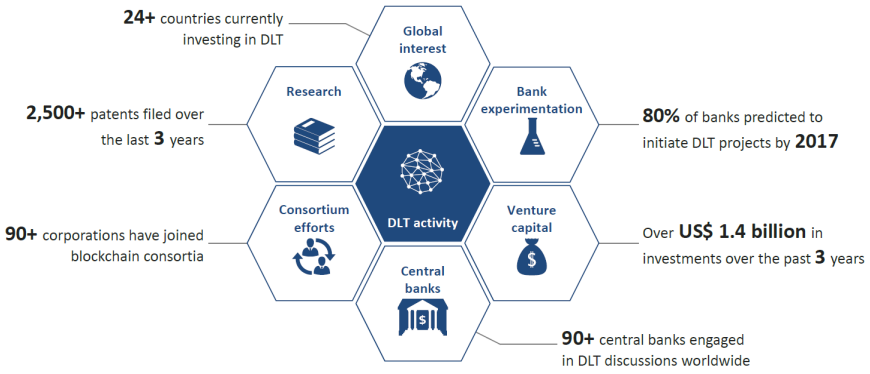
II.1. What is Blockchain?

Blockchain is a distributed ledger technology that keeps track of all transactions that have taken place across a peer-to-peer network. Best known as the technology underpinning Bitcoin cryptocurrency, blockchain takes records—such as proofs of ownerships, confirmed financial transactions, and financial contracts—and puts them into blocks, which are linked to prior blocks, forming a "chain" in linear and chronological order. The data is then verified by a **consensus mechanism**—by which various network participants work together, sometimes in a competitive manner, to verify the integrity of the data—and ultimately stored in an encrypted and decentralized fashion across the network. This results in a system of record-keeping that is maintained solely by network participants.

Blockchain is a revolutionary technology because it enables the creation and operation of a "**trustless network**" that allows unrelated parties to transact with one another without pre-existing trust, middlemen, or supervisory authorities. In the case of Bitcoin, for instance, blockchain helps create new depository and transaction mechanisms that obviate the need for banks and other intermediaries. This unique attribute, coupled with its digital infrastructure, gives blockchain the power to disrupt the existing financial system and create a new financial architecture based on computer algorithms rather on interpersonal trust. Several efforts have since emerged to use blockchain to transform the financial sector, showing promise to promote security, efficiency, and inclusion, albeit with debatable true implications.

Given this transformative potential, blockchain has garnered significant attention and investment. Greenwich Associates, a market intelligence provider, estimated that financial and technology markets invested approximately $1 billion in blockchain in 2016, and the markets will likely see exponential growth in the near future.[1] Furthermore, blockchain has also propelled the development of other **distributed ledger technologies (DLTs)**—database technologies that store data in a decentralized fashion—and other decentralized technological platforms. Together, these technologies may transform our society, potentially in ways that we have not yet imagined.

Exhibit 1: Blockchain and DLT is capturing the imaginations of entrepreneurs and investors



Source: World Economic Forum, *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services*, August 2016

[1] Yu, "What Wall Street's Obsession with Blockchain Means for the Future of Banking," in *Fortune* (July 10, 2016) and Vantiv, "Riding the Blockchain Train, Together," January 2017.

Blockchain versus Distributed Ledger Technology (DLT)

The terms "blockchain" and "distributed ledger technology (DLT)" have often been used interchangeably. Are they the same thing?

Technically, DLT is a class of database technology, among which blockchain is one implementation. There have been efforts to create other applications of DLT that share some of the key features of blockchain but are modified to make them more suitable for other purposes. Nevertheless, today there are no strict technical specification for DLT besides it being a shared ledger.

To understand why technologists want to improve upon blockchain, one must understand the value propositions and the shortfalls of the technology. On the plus side, blockchain introduces a consensus mechanism (see more on page 7) that ensures data integrity in a trustless network. On the other hand, depending on how it is used, blockchain could be a cumbersome database. The Bitcoin blockchain, for instance, copies all the data to all participants on the network, which is arguably excessive. It also requires a proof-of-work verification (see more on page 7) on all new transactions, which is costly. Hence, some developers have created new implementations of DLT—such as Corda, Ripple, and Chain—to serve other purposes. One must keep in mind that by loosening some constraints, the new implementations may lose some features as well. Appropriate implementations hence vary by use-cases and design choices.

In this report, the term "blockchain" refers to specific implementations of DLT that allow for decentralized consensus mechanisms, while "DLT" refers to any distributed database technology that may or may not contain such mechanisms.

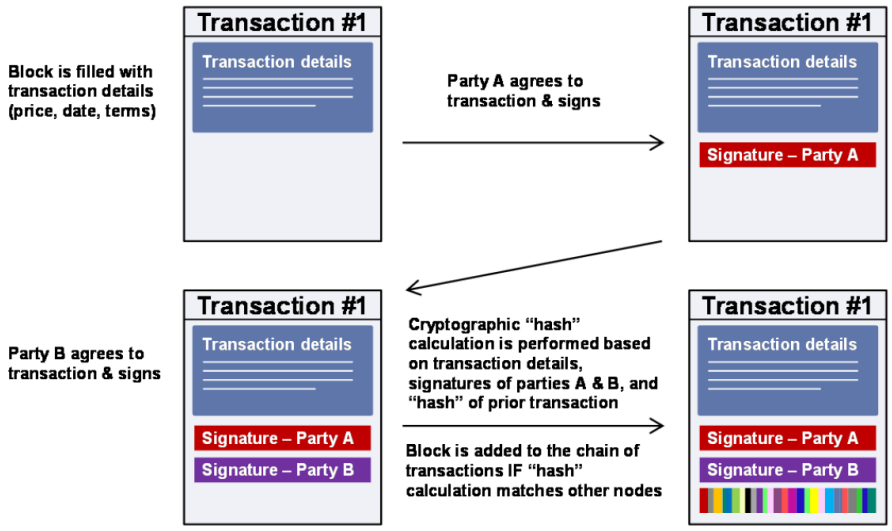
.

II.2. How Blockchain Works

Blockchain was invented by Satoshi Nakamoto (pseudonym), the technologist who introduced the concept of Bitcoin—and by extension its underlying technology, blockchain—in a white paper in November 2008. To understand how blockchain works, it is easiest to study the working of Bitcoin, blockchain's first and most well-known application.

Bitcoin uses blockchain to keep track of all transactions that have taken place among participants across a network. As new transactions occur, they are first propagated throughout the network. Certain participants in the network—called "miners"—then compete to validate the transactions and append them to the database. In the case of Bitcoin, these miners validate transactions by solving mathematical problems based on a cryptographic hash which is difficult to solved. Once the answers to those problems have been found, however, they can be easily verified by other nodes on the network. This "**proof-of-work**" process makes the database **tamper-resistant**, meaning that any efforts to manipulate existing data without others' approval would be extremely difficult to succeed. The miners are rewarded some Bitcoins for their efforts in the "mining" process, and the updated blockchain is re-propagated throughout the network to include the records of the new transactions.

Exhibit 2: Illustration of how a single block in the blockchain is built and validated



Source: Goldman Sachs Global Investment Research.

Based on the architecture described above, blockchain encompasses three core concepts: shared ledger, cryptography, and consensus.

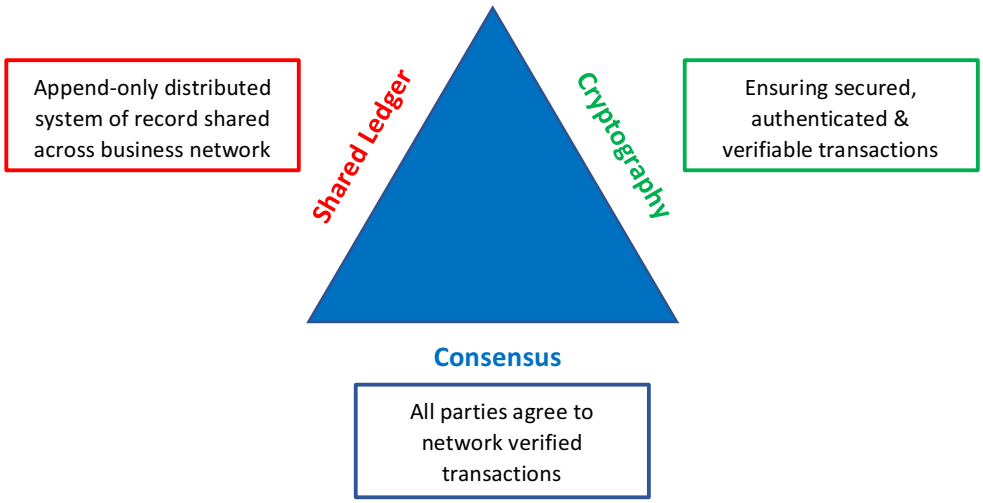
- *Shared Ledger:* Blockchain is a distributed ledger that is either open to the public (for public blockchain) or shared among private consortium (for private blockchain). It often layers on permissions for different types of users who have access to different levels of information stored on the blockchain. The fact that the ledger is shared allows several parties to access the same data, eliminating the need for data reconciliation.

- *Cryptography:* Blockchain employs cryptography to create a secured and immutable data structure. When each block of data is created, it is identified by its cryptographic hash, which is a value that is encoded through a hash function and still refers to the original data. This hash refers to the previous block of data—called the "parent block"—by including the parent block's hash in its own hash value. If the data in the parent block is modified, it will also change the hash values in the subsequent blocks. This means that the network must re-perform the consensus mechanism to re-verify all the transactions in the sequence. Any efforts to manipulate the data therefore will likely fail unless such efforts are blessed by the entire network. This feature establishes security and integrity of the data stored on blockchain.

- *Consensus:* Whereas traditional record-keeping systems depend on trusted intermediaries to verify transactions, blockchain utilizes the power of the network to achieve data integrity. Each transaction that is added to a blockchain must be verified by participants in the network who would arrive at the same consensus on the data by sharing information among each other.

These three concepts enable blockchain to create a record-keeping system that allows for broad participation and lower redundancy.

Exhibit 3: Underlying Concepts of Blockchain



Blockchain Consensus Mechanisms

Blockchain technology creates a decentralized data structure by using a "consensus mechanism." A consensus mechanism is a process by which network participants work together, sometimes in a competitive fashion, to verify the integrity of the data on the network. There are several protocols to perform this process, among which the **proof-of-work** and the **proof-of-stake** protocols are the best-known ones.

To understand how they work, consider Bitcoin's proof-of-work process. When a new Bitcoin transaction occurs, miners—which are certain participants on the network—compete to add that new transaction to the next block in the blockchain by racing to solve a difficult cryptographic puzzle. The first to solve the puzzle wins, and after other nodes on the network have checked and confirmed that solution (which is easy to do), the winner receives new Bitcoins as compensation, and the new block of data is added to the blockchain and redistributed throughout the network. This protocol essentially does two things: (1) it ensures that the next block of data being added to the blockchain is the one and only version, and (2) it prevents mischievous efforts to manipulate the data and fork the chain.

Although a proof-of-work mechanism is a powerful concept, it also carries some flaws. The main flaw is that it requires enormous amount of computational energy and therefore does not scale well. Thus, innovators have sought to improve upon this process. For instance, a distributed ledger technology company Ripple devised a consensus mechanism in which various nodes in the network perform different functions in the transaction verification process (in other words, not all network participants participate as miners to verify each transaction). Moreover, only 70% (rather than all) of the miners participate in approving a new transaction. Ripple argues that this process is sufficient to ensure the integrity of the data, particularly among trusted participants, while improving performance.

Blockchain Consensus Mechanisms (Continued)

Furthermore, other ideas have also emerged as alternatives to provide the consensus mechanism. For instance, a **proof-of-stake** concept works by allowing validators (rather than miners) on the network to validate transactions. These validators are owners of coins in the system, and they take turns validating transactions in exchange for transaction fees, with validation frequency depending on how many coins each validator owns. To discourage validators from creating two blocks simultaneously and thereby forking the chain, the system creates an enforcement procedure, for instance, by requiring validators to lock their coins in a virtual vault, which will be forfeited if these validators behave badly. Ethereum is an example of a blockchain architecture that plans to move from the proof-of-work to the proof-of-stake protocol in early 2018.

Other alternatives also include **proof-of-activity** (which combine both proof-of-work and proof-of-stake), **proof-of-burn** (in which network participants spend their coins to increase their chance of being selected as miners), **proof-of-capacity** (in which participants contribute their storage space to increase their chance of being selected as miners), **proof-of-storage** and **proof-of-space** (which are derivatives of proof-of-capacity), and **proof-of-elapsed-time** (which relies on an algorithm running in a specific trusted execution environment). As the technology continues to evolve, we will likely see more consensus mechanisms designed for specific purposes and constraints.

Source: Coindesk, "A (Short) Guide to Blockchain Consensus Protocols," March 4, 2017.

II.3. Types of Blockchain

Blockchain can be implemented in various ways. In making appropriate design choices, developers and users of the technology select along these three dimensions: (1) public vs. private access, (2) transparent vs. nontransparent data, and (3) mutable vs. immutable data.

- *Public vs. Private Access:* As the names suggest, public blockchains (also called "**permission-less** blockchain") and private blockchains (also called "**permissioned** blockchain") differ in the levels of permission required for participants to access and modify the data. Public blockchains grant read and write access to all users who wish to join the network, while private blockchains only allow permitted parties to join. The choice between public versus private blockchains lies in the trade-off between access and control. While public blockchains allow for broader access, they are harder to control for privacy and harder to apply in a specialized fashion. Private blockchains on, the other hand, could be designed for specific purposes, thereby enhancing efficiency, but they also limit access, turning permitted parties on the network into intermediaries for those outside the network.

- *Transparent vs. Nontransparent Data:* While all the data on blockchain is encrypted, blockchain can still be designed for different levels of transparency and degrees of privacy. Some blockchains—such as Bitcoin—are designed so that one can still identify the parties engaging in transactions through pseudonyms. In certain instances, one can then use network analysis to decipher the pseudonyms and reveal the actual identities of the parties engaging in transactions. On the other hand, other blockchains—such as Z-cash—allow parties to engage in transactions with "**zero-knowledge security,**"

which means that the identities of the parties and the nature of the transactions are completely concealed.

- *Mutable vs. Immutable Data:* Blockchain databases could be designed such that existing records on the blockchain are either modifiable or permanent. For example, Bitcoin is an "**immutable**" blockchain, and once a transaction has been committed, it cannot be reversed or changed. In other words, one can only append new transactions to the Bitcoin blockchain. However, other blockchains—such as Accenture's blockchain—allow modifications of existing data, which must still be approved in a consensus process. Hence, an immutable blockchain offers more security given its data rigidity, while a mutable blockchain offers more efficiency instead.

Note that although these attributes describe different aspects of a blockchain, in practice, some of these attributes are mutually exclusive. For instance, while private blockchains can be either mutable or immutable, only immutable public blockchains exist. This is because allowing data modification on a public blockchain will expose the blockchain to more risks of data manipulation, and therefore no one has deployed both features together. Similarly, a nontransparent private blockchain does not exist since only pre-approved participants are allowed on a private blockchain already and therefore hiding the identities of these participants is pointless. As a result, most industry participants tend to focus on choosing between *private* versus *public* blockchains. Exhibit 4 provides examples of blockchains under each category, and Exhibit 5 provides a comparison of public versus private blockchains.

Exhibit 4: Examples of Blockchains by Category

	Public		Private	
	Immutable	**Mutable**	**Immutable**	**Mutable**
Transparent	Bitcoin, Ethereum		Ripple, R3 Corda	Accenture
Nontransparent	Z-cash		(case not found)	(case not found)

Exhibit 5: Comparison of Private vs. Public Blockchains

	Public	**Private**
Scope of Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Consensus Mechanism	Consensus Mechanism + Pre-Approved Participants
Identity	Anonymous / Pseudonymous	Known identities
Control	Harder	Easier
Asset	Native assets	Any asset
Examples	Bitcoin, Ethereum, Dash, Lisk	Ripple, R3 Corda, Chain

Source: BlockchainHub, augmented by the author.

Based on the current trend, financial institutions generally deploy *private* blockchains because they fit with existing systems and regulatory structures. In a typical transaction scheme where financial institutions serve as intermediaries, these institutions can utilize private blockchains to facilitate interaction among themselves without the need to open the network to the public. Private blockchains therefore serve as a better choice as they offer more control over data access. Moreover, this system also

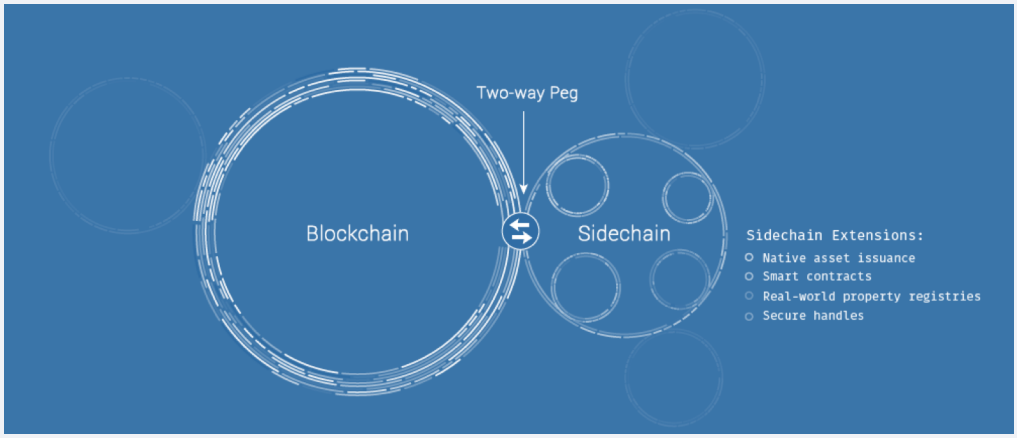
fits squarely with the existing regulatory regime in which regulators simply monitor these intermediaries to ensure their compliance and the compliance of their customers.

On the other hand, startups and communities of developers are enthusiastic about using *public* blockchains to create trustless networks that enable direct peer-to-peer transactions. This approach has the potential to change the ways people do business and create trillion dollars' worth of business opportunities. Unsurprisingly, technologists and entrepreneurs are competing to devise new business models based on the public blockchain concept.

Not only do these design choices affect how entrepreneurs and developers deploy the technology, they also create regulatory implications. With limited number of participants, a private blockchain is presumably easier to regulate, and any potential damages that could occur would likely be limited in scope (although not necessarily in scale). This stands in contrast to a public blockchain which anyone can join, and as a result the regulators will likely have a harder time controlling activities on the network and limiting any potential damages. With that said, a public blockchain also offers more transparency by allowing regulators to see everything that takes place on the networks, whereas the regulators will require permissions to monitor activities on a private blockchain. Ultimately, these design choices will be used in different applications and yield different outcomes in terms of performance, scalability, accessibility, and stability.

Linking Blockchains Together Through "Sidechains"

Blockchain can be applied under different technical specifications. For instance, firm A could create blockchain A for its internal usage, while firm B could also create blockchain B for a similar purpose. So how would blockchain A communicate with blockchain B? We do so via a pegged "sidechain."



Let us say firm A wants to send a block of data to firm B. Firm A first sends that block of data to a specific address on its own blockchain that is completely *immobilized*. Confirming the immobilization, firm B then creates a new block of information on its own network with the same data as that contained in the immobilized block on blockchain A. This makes blockchain B a "sidechain" of blockchain A. This process is also symmetrical, so firm B can also send its data on blockchain B to firm A running blockchain A by the same process.

Linking Blockchains Together Through "Sidechains" (continued)

Sidechains allow multiple blockchains to transfer data among each other without breaking the immutability property imposed by the underlying technology. The concept can be applied to both private and public blockchains. Most importantly, it allows one to dissect a generic blockchain into multiple sidechains, each serving particular purposes. The most discussed use-case for sidechains is with Bitcoin, where firms can create internal Bitcoin networks that are carved out from the public network, allowing for internal privacy.

Sidechains are not only interesting from a technical standpoint, they also raise questions from a regulatory perspective. For instance, how should regulators monitor and regulate transactions occurring through side-chains between companies? Should they regulate intra-firm activities, such as inter-departmental billings? Would a system with multiple side-chains be more or less stable than one with one inclusive blockchain structure? How should regulators deal with the complexity of monitoring activities on multiple sidechains? Ultimately, sidechain is merely one example of technical derivatives of blockchain. As other derivative technologies emerge, regulators would need to deal with new issues related to them as well.

II.4. Benefits of Blockchain

Blockchain has the potential to revolutionize various industries based on several benefits that the technology has to offer, including:[2]

- *Removal of transaction intermediaries:* The most unique benefit of blockchain is its ability to facilitate secure, de-centralized transactions among unrelated parties without going through intermediaries. For instance, blockchain can facilitate a transfer of money between parties that bypasses banks, or a purchase of financial securities that bypasses brokers. This has the effect of reducing transaction costs and expanding the system's reach. For instance, customers can use a blockchain-based system to transfer money between each other cheaply relative to using money transfer networks (such as Western Union) or banks (which may not be accessible to the "unbanked").

- *Reduced transaction time:* Blockchain can reduce transaction time, particularly for clearing and settlements. Consider the current financial system: while trading of stocks and bonds is often conducted in nanoseconds, settlements still take days or even weeks. The delay lies in the time it takes for both parties to reconcile and confirm their transactions. Blockchain could eliminate these lags since the transaction is conducted on a shared ledger visible to both counterparties, undoing the need for transaction reconciliation. As it stands today, Bitcoin transactions can be settled within minutes.[3]

[2] Note that these benefits are present regardless of the design choices, although such choices could affect the extent of such benefits. For instance, although both private and public blockchains could remove transaction intermediaries, a private blockchain used by banks will eliminate intermediaries for banks, while a public blockchain used by consumers will eliminate intermediaries completely, including the banks themselves.

[3] Oliver Wyman, *Blockchain in Capital Markets: The Prize and the Journey*, February 2016.

- *Reduced record-keeping costs:* Blockchain reduces record-keeping costs by eliminating the need for reconciliation process and the risks of a "double-spending." Since participants in a blockchain network share the same distributed ledger and since transactions occur practically in real-time, there is no need to reconcile records among counterparties, and these parties also need not worry that their counterparties will engage in multiple transactions using the same assets. Blockchain can also enhance the auditing process and facilitate contract compliances with the use of **smart contracts**.

- *Reduced risk of fraud and information leakage:* Because blockchain database is encrypted and immutable, writing and accessing data require a "public key" and a "private key" which help ensure data security. More importantly, any changes to the data requires verification by participants in the network, making any attempts to manipulate the data on a blockchain virtually impossible. This makes blockchain fraud-proof, unlike the existing system where anyone that can hack into the database of centralized intermediaries can alter records. As an example, the Bangladesh Central Bank lost $100 million after its network was hacked in March 2016.[4]

- *Elimination of single point of failure:* Because blockchain reduces the role of intermediaries, relying instead on the network of participants, it eliminates potential risks of failure at intermediary nodes, either due to mass demand, security attack, or other technical glitches. If some nodes on the blockchain network fail, other nodes can still maintain the records of and verify all the transactions on the network. This enhance the overall stability and security of the system.

Is Blockchain Really Safe?

On August 2, 2016, Bitfinex—a Bitcoin exchange based in Hong Kong—was hacked, resulting in $65 million worth of Bitcoins being stolen from customers' accounts. Isn't Bitcoin (and blockchain) supposed to be fraudproof? Does this signal the impending collapse of Bitcoin (and blockchain)?

Not really. In fact, this unfortunate event ironically highlights the strength of blockchain, if it is implemented correctly. In this case, the hack demonstrates the weakness of a system whereby centralized intermediaries facilitate transactions. Effectively, the intermediary, i.e. the exchange, mishandled customers' wallets, resulting in a significant loss. In a completely decentralized system enabled by blockchain whereby intermediaries are no longer necessary, such risks of significant losses due to security breaches at the intermediaries will be minimized or eliminated.

In the end, losing a wallet is difficult to avoid in any types of systems, but blockchain would allow one to be responsible for one's own wallet, rather than trusting it to the intermediaries.

[4] Wall Street Journal, "Bangladesh Central Bank Found $100 Million Missing After a Weekend Break," https://www.wsj.com/articles/bangladesh-central-bank-found-100-million-missing-after-a-weekend-break-1457653764

II.5. Applications of Blockchain

Blockchain provides several potential use-cases within the financial sector, ranging from facilitating payments to enforcing financial contracts. Exhibit 6 lists potential use-cases of blockchain and DLT, as compiled by the Blockchain Working Group at the World Economic Forum in 2016. These use-cases can be grouped into three categories as follows.

- *Facilitating Global Transfers of Assets:* Blockchain improves upon the existing mechanisms to transfer assets by allowing transactions to take place directly between parties without going through banks or transfer agents. This has the potential to reduce cost, increase speed, and enhance security. Currently, several banks—such as Citi, Bank of America, and Barclays —are exploring methods to use blockchain to enable transfers of money among themselves or with customers in a more expedited manner (See Exhibit 9 for a list of banks using blockchain for various applications).

- *Improving Clearing, Settlement, and Record-Keeping Processes:* Using a shared ledger, blockchain can assure the integrity and uniformity of data by allowing parties to overcome the risks of "double-booking," whereby a particular asset is transfer to two different parties at the same time. This can improve clearing and settlement processes by eliminating the need to reconcile records. Today, brokerages and exchanges are working on improving slow clearing and settlement processes for certain assets, such as private shares and commodities. In fact, it is estimated that blockchain could deliver cost savings of nearly $20 billion per year by 2022 by eliminating the manual processes of reconciliation with customers, trading partners, and exchanges.[5]

- *Enabling Smart Financial Contracts:* Blockchain enables automation of transactions, as business terms can be recorded in computer language embedded in blockchain databases. As a result, transaction terms and events can be executed automatically without engagement with accountants and lawyers. For instance, a loan default can automatically trigger a process specified in the default clause of the contract. This reduces contracting, enforcement and compliance costs and increase efficiency, although it may also raise concerns regarding bypassing of a dispute settlement process and due-process rights.

In terms of priority, a survey conducted by IBM in September 2016 shows that financial institutions that are leading technological trends identify the following key areas where blockchain could provide the biggest benefits: record-keeping, retail payments, and consumer lending. Other literature also suggests that trade finance represents another key area which could see up to $17 billion in new value by integrating blockchain solutions.[6] Exhibit 7 provides a more extensive list of blockchain deployment in the financial sector.

[5] Yu, Howard, "What Wall Street's Obsession With Blockchain Means for the Future of Banking," *Fortune*, July 10, 2016.
[6] Vantiv, *Riding The Blockchain Train, Together*, January 2017.

Case Study: Applying Blockchain to Capital Markets

One key area in which blockchain could be deployed to enhance transaction efficiency is the capital markets. In an ideal scenario, the record of each security would be kept in a single shared ledger, eliminating the need for data normalization, reconciliation of internal systems, and agreement on exposures and obligations. This would allow for standardized processes and services, near real-time data, and improved visibility in counterparty worthiness. Specifically, transactions could be conducted as follows:

- *Securities Transaction:* Client A and B are matched on an execution venue, upon which their means to complete the transaction are verified. Client A and B then jointly "sign" the transaction by applying their private keys to unlock their asset or cash, and then applying their public key to transfer ownership in their assets to the recipients. The signed transaction is subsequently broadcasted to the network to be validated and recorded.

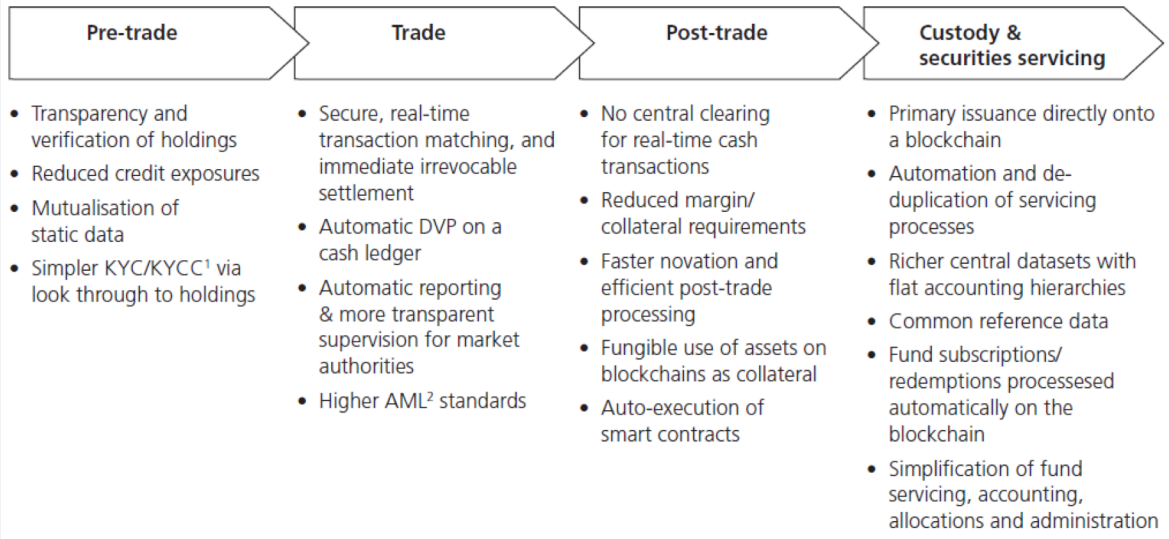
- *Asset Servicing:* Mandatory events and distributions can be managed via smart contracts, with complex events structured via "Delivery Versus Payment (DVP)" transactions. With a shared ledger, multiple custody layers are shrunk to a single function, giving asset managers more transparent command over their pool of investments as well as the ability to manage investors' holdings in the funds themselves.

- *Derivative Transactions:* Derivative transactions could be unbundled and financed by issuers selling their own instruments that match the cash flows they expect to achieve, effectively creating swaps without the need for balance sheet intermediation. Derivative contracts could also be created as smart contracts, which could automatically re-compute exposures and trigger payment instructions. Dealers could continue to net their exposures to various derivative contracts that may offset each other. At the same time, posting of collateral could be done either by escrowing cash on the cash ledger or allocating assets to the collateral ledger.

Currently, several companies are working on applying these concepts in their operations. For instance, investment banks such as Credit Suisse Group, Bank of America, Goldman Sachs are exploring securities transaction mechanisms and smart contract applications using blockchain. NASDAQ is also exploring the use of blockchain in IPO and private securities transactions. Finally, DTCC is developing a distributed ledger solution for derivatives processing and building the next generation trade information warehouse.

Note that these changes will not only change how companies operate, they will also affect the market structure. Clients will likely accrue the most benefit from reduced costs in capital markets dealing and securities servicing. Dealers will still play a valuable role in the market as a price setter, adviser, and liquidity provider. On the flip side, this could affect the functioning of market makers and High-Frequency Traders (HFT), since they will have to wait for transaction settlement cycles (even for a few seconds). While this system will keep execution venues in their existing roles, it will eliminate the need for Central Counterparty Clearing houses (CCPs) and custodians. A number of related use-cases is presented in the accompanying feature detail and in Exhibit 6 below.

Potential Benefits for Capital Markets



Potential Use-cases and Adoption Steps

Type	Use case	Capital markets examples	Other industry examples	Rationale for adoption
First order adoption – works as standalone	• Tokenising assets not currently on a common ledger (new blockchains or tokens on Bitcoin)	• Pre-IPO equities • Syndicated loans • Depository receipts	• Physical objects e.g. diamonds, paintings	• Proof of ownership/ provenance • Settlement efficiency
	• New blockchains to share data between participants	• KYC data sharing • Collateral ledger to support efficient margining • Reference and market data	• Supply chain data invoicing • Trade finance	• Efficiency of information collection
	• New blockchains to process transactions	• Corporate finance bookrunning • Fund portfolio management	• Inter-bank blockchain to support cross-border banking payments • Intra-bank blockchain to support cross-bank accounting	• Disintermediation of actors • Simplified data and infrastructure
Second order adoption – reliant upon critical mass of assets on blockchains	• Monitoring of richer datasets	• Concentration monitoring • Market surveillance • Pricing data	• Trade flows, transit data	• Powerful understanding of data
	• Processing using blockchains	• Securities servicing • Regulatory reporting		• Efficient processing capabilities

Source: Oliver Wyman, *Blockchain in Capital Markets: The Prize and the Journey*, February 2016.

Exhibit 6: Use-cases for Blockchain and DLT

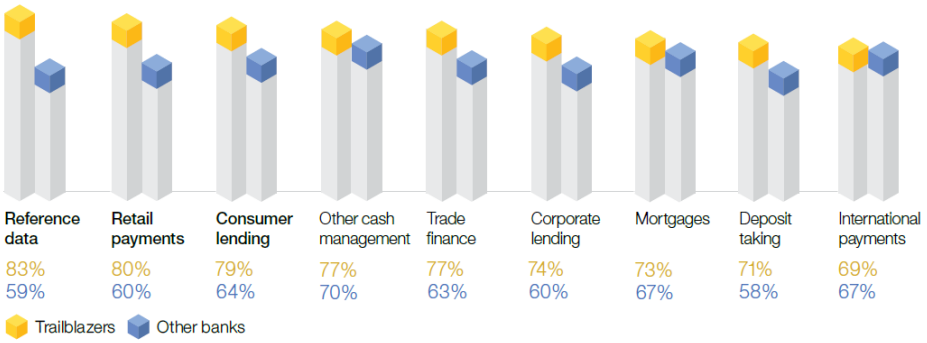
Use Case	Summary	Implications for FIs	Critical conditions for implementation
Global Payments	Conducting international money transfers through DLT could provide real-time settlement and reduce costs, enabling new business models (e.g. micropayments), and institute newer models of regulatory oversight	• Real-time settlement of international money transfers can increase profitability by reducing liquidity and operational costs • Utilizing DLT will enable direct interaction between sender and beneficiary banks, and eliminate the role of correspondents • Smart contracts can capture obligations and drive reporting, minimizing operational errors and accelerating outcomes	• Ensuring compliance via standard KYC processes • Binding legality of cryptographic hash to exchange value • Adopting standards and ensuring interoperability
Insurance	Facilitating claims management for property and casualty (P&C) insurers on DLT can automate processing through smart contracts, improve assessment through historical claims information and reduce potential for fraudulent claims	• Smart contracts can automate claims processing through third-party data sources and codification of business rules • DLT can drive reductions in operating costs through process simplification • Storing historical claims information on the ledger will enable insurers to identify suspicious behaviour and improve assessment	• Building a comprehensive set of asset profiles and history • Adopting standards for relevant claims data • Providing a legal and regulatory framework
Deposits & Lending — Syndicated Loans	Utilizing DLT to automate syndicate formation, underwriting and the disbursement of funds (e.g. principal and interest payments) can reduce loan issuance time and operational risk	• Forming syndicates through smart contracts can increase speed and provide regulators with a real-time view to facilitate AML/KYC • Performing risk underwriting through DLT can substantially reduce the number of resources required to perform these activities • Smart contracts can facilitate real-time loan funding and automated servicing activities without the need for intermediaries	• Building risk rating framework for syndicate selection • Standardizing diligence and underwriting templates • Providing access to financial details on the distributed ledger
Deposits & Lending — Trade Finace	Utilizing DLT to store financial details can facilitate the real-time approval of financial documents, create new financing structures, reduce counterparty risk and enable faster settlement	• Storing financial details on the ledger can automate the creation and management of credit facilities through smart contracts • DLT can improve real-time visibility to the transaction to better institute regulatory and customs oversight • Utilizing DLT will enable direct interaction between import and export banks, and eliminate the role of correspondent banks	• Providing transparency into trade finance agreements • Enabling interoperability with legacy platforms • Rewriting regulatory guidance and legal frameworks

Use Case	Summary	Implications for FIs	Critical conditions for implementation
Capital Raising — Contingent Convertible ("CoCo") Bonds	Utilizing smart contracts to automate regulator reporting can minimize the need for point-in-time stress tests, reduce market volatility and, ultimately, increase "CoCo" bond issuance	• Tokenizing bond instruments when soliciting capital from investors can enable them to make informed, data-driven decisions • Smart contracts can alert regulators when loan absorption needs to be activated, minimizing need for point-in-time stress tests • Providing investors with transparency into loan absorption can reduce uncertainty currently associated with "CoCo" bonds	• Standardizing attributes for soliciting investments • Streamlining trigger calculations across FIs • Developing processes to act on real-time trigger notifications
Investment Management — Automated Compliance	Utilizing DLT to store financial information can eliminate errors associated with manual audit activities, improve efficiency, reduce reporting costs and, potentially, support deeper regulatory oversight in the future	• Storing financial information on the ledger provides immutable, real-time updates and facilitates automated review • Executing reporting activities through smart contracts can facilitate the automated creation of quarterly and annual findings • In the future, DLT can seamlessly execute and automate compliance activities (e.g. Comprehensive Capital Assessment Review)	• Providing compartmentalized access to data • Automating faster and efficient enforcement of regulations • Enabling interoperability with legacy platforms
Investment Management — Proxy Voting	Distributing proxy statements via DLT and counting votes via smart contracts may improve retail investor participation, automate the validation of votes and, potentially, enable personalized analyses in the future	• Distributing proxy statements via the distributed ledger can reduce costs associated with printing and mailing • Smart contracts can automate the validation of votes and increase the transparency of counting votes (e.g. end-to-end confirmation) • Storing proxy statements on the ledger may enable investors to conduct personalized, automated analyses in the future	• Storing investment records on a distributed ledger • Integrating legacy voting mechanisms into tokens • Collaborating across actors to ensure success
Market Provisioning — Asset Rehypothecation	Utilizing DLT to track and manage asset rehypothecation via smart contracts can enable the real-time enforcement of regulatory control limits across the financial system and reduce settlement time	• Rating counterparties based on transaction history stored on DLT can enable investors to improve investment decisions • Smart contracts enable the real-time reporting of asset history and the enforcement of regulatory constraints • Facilitating clearing and settlement processes via smart contracts can eliminate need for intermediaries and reduce settlement time	• Tokenizing assets using a shared standard • Fostering engagement among the financial ecosystem • Architecting solution to manage over-the-counter (OTC) templates

Use Case	Summary	Implications for FIs	Critical conditions for implementation
Market Provisioning — Equity Post-Trade	Utilizing DLT and smart contracts to facilitate post-trade activities can disintermediate processes, reduce counterparty and operational risk and, potentially, pave the way for reduced settlement time	• Conducting clearing activities through the ledger can automate processes, reduce settlement time and lower counterparty risk • Smart contracts can simultaneously transfer equity and cash in real time, reducing the likelihood of errors impacting settlement • Disintermediating clearing, settlement and servicing processes can reduce costs and enable capital & liquidity management efficiencies	• Incorporating "net transaction" benefits within settlement • Achieving multistakeholder alignment across participants • Standardizing reference data utilized to match trades

Source: World Economic Forum, *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services*, August 2016.

Exhibit 7: Use-cases of DLT



Source: IBM Institute for Business Value, *Leading the pack in blockchain banking: Trailblazers set the pace*, September 2016.

Note that although some use-cases of blockchain technology could transform how financial transactions are conducted, today financial institutions are primarily deploying blockchain merely to upgrade their infrastructure. Many financial institutions are working with technology partners to deploy permissioned blockchains to facilitate record-keeping and transaction mechanisms, either internally or with other financial institutions. By applying blockchain solutions, these institutions aim to save costs and gain efficiency, potentially passing these benefits onto consumers. Consumers may only observe minimal changes in their experiences, however. An example of such applications is the financial institutions' effort to create money transfer mechanism that would replace the SWIFT network. Exhibit 8 lists some of the technology partners, and Exhibit 9 lists some adoptions of blockchain and DLT by major financial institutions around the world today.

Emerging Use-cases of Blockchain: Digital Token and ICO

One use-case of blockchain which has garnered significant attention recently is the use of a "**digital token**" to facilitate transaction between enterprises. Digital token represents a token of value that one company may issue to another either as a medium of exchange or as compensation for services provided. For example, in 2014, Ripple created a digital currency, dubbed XRP, to allow financial institutions to transfer money across currencies with negligible fees and wait-time. The idea is that for some thinly traded currencies, XRP could serve as a reference currency to facilitate a transfer across countries.

Another emerging use-case of blockchain is the issuance of new securities based on blockchain technology to raise money. Through a process called **Initial Coin Offering (ICO)**, several companies have recently issued new "coins" in exchange for capital. This process is equivalent to an Initial Public Offering of a publicly-traded company, and after the ICO process, these coins also trade like traditional securities. As an example, Ethereum was the first company to do an ICO and raised $17.3 million in August 2014.

These examples illustrate that more use-cases of blockchain will be invented in the coming future. Regulators have to be aware of these innovations and be prepared to engage when necessary.

Exhibit 8: Major Companies Developing Blockchain and DLT

Company	Founded	HQ	Funding	Description
r3	2014	US (NY)	$ 200	"R3 CEV is a financial innovation firm that leads a consortium partnership with over 75 of the world's leading financial institutions to design and deliver advanced distributed ledger technologies to the global financial markets. Corda, the consortium's open-source distributed ledger platform, enables financial institutions to handle more complex transactions and maintain securities. Corda aims to provide a platform with common services to ensure that any services built on top are compatible between the network participants, while fostering innovation and faster time to market as the underlying infrastructure would be accepted and understood by at least the founding firms."
ripple	2012	US (CA)	$ 93	"Ripple is the creator of Ripple Transaction Protocol (RTXP), a real-time gross settlement system (RTGS), currency exchange and remittance network. Built upon a distributed open source Internet protocol, consensus ledger and native currency called XRP (ripples), RTXP purports to enable secure, instant and nearly free global financial transactions of any size with no chargebacks. At its core, RTGS is based around a shared, public database or ledger, which uses a consensus mechanism that allows for payments, exchanges and remittance in a distributed process."
Blockstream	2014	Canada	$ 76	"Blockstream is a bitcoin-focused company that works to accelerate innovation in cryptocurrencies, open assets, and smart contracts. The company's core area of innovation is focused around an idea called "sidechains", bitcoin-like ledgers that operate independently of, but are pegged to, bitcoin. It allows its users to build a separate platform for a specific use, but still have access to the bitcoin blockchain. Blockstream's products include Elements, an open-source platform for building and testing applications; and Liquid, which is designed for bitcoin exchanges and high-speed transactions."
Digital Asset Holdings	2014	US (NY)	$ 60	"Digital Asset is a software company that develops distributed ledger technology solutions for the financial services industry. The company employs the blockchain technology to facilitate settlements between digital and traditional currencies. Its software maps business logic and legal processes into cryptographic signature flows as well as commits transactions to private or public distributed ledgers and traditional databases, depending on the requirements. It offers its software to various market segments such as loans, securities, derivatives, and foreign exchange. The company maintains strategic partnerships with Accenture, Broadridge, and PwC."
Chain	2014	US (CA)	$ 40	"Chain is a technology company that partners with financial firms to build and deploy blockchain networks which transform markets. Its solutions enable institutions to design, deploy, and operate blockchain networks that can power any type of asset in any market. The company offers Chain Open Standard, an open-source blockchain protocol for high-scale financial applications. It includes Chain Core, an enterprise-grade production node; and Chain Sandbox, a prototyping environment. Chain maintains strategic partnerships with financial services firms such as NASDAQ, Visa, Citi, Capital One, and Fiserv."
SETL	2015	UK	$ 40	"SETL is an inititive to deploy a multi-asset, multi-currency institutional payment and settlements infrastructure based on blockchain technology. The SETL system will enable market participants to move cash and assets directly between each other, facilitating the immediate and final settlement of market transactions. The SETL system maintains a permissioned distributed ledger of ownership and transaction records, simplifying the process of matching, settlement, custody, registration and transaction reporting."
ethereum	2014	US / Switzerland	$ 15	"Ethereum is a platform and a programming language that makes it possible for any developer to build and publish next-generation distributed applications. Ethereum can be used to codify, decentralize, secure and trade just about anything: voting, domain names, financial exchanges, crowdfunding, company governance, contracts and agreements of most kind, intellectual property, and even smart property thanks to hardware integration. Ethereum borrows the concept of decentralized consensus that makes bitcoin so resilient, yet makes it trivial to build on its foundation."
HYPERLEDGER	2014	US	--	"Hyperledger is a new technology to allow banks to clear and settle in real-time without the need for a central party via distributed ledgers. By removing the need for these intermediaries, Hyperledger reduces costs, delays, and settlement risk. For the first time, financial institutions can create private shared databases among known entities. By providing an open standard for value transfer, Hyperledger can integrate with existing systems to break down silos and increase liquidity. Hyperledger is the only platform of its type not to have a built-in cryptocurrency or singular public network."

Source: Crunchbase, other news sources; compiled by the author. Funding stated in millions of dollars.

Exhibit 9: Engagement with Blockchain / DLT by Major Financial Institutions

Financial Institutions	Timeline	Partners	Use Cases	
fidor BANK	Oct-13	Ripple, Kraken, bitcoin.de	• Money transfer • Digital currency exchange • P2P bitcoin trading	*
LHV pank	Jun-14	ChromaWay, coinfloor, coinbase	• Builds Cuber Wallet in partnership with Chromaway • Money transfer services • Digital security applications	
cross river	Sep-14	Ripple	• Risk management • Cross-border payments	*
Rabobank ING ABN·AMRO	Dec-14	Ripple	• Faster transactions • Other banking services	
BBVA Compass	Jan-15	coinbase	• Investment in series C round	
	Mar-15	IBM	• Explores digital payment system and digital currency in partnership with IBM	*
	Mar-15	Safello	• Runs innovation labs & accelerators focused on blockchain and partnered with Safello • Have 45 experiments that Barclays plan to conduct internally	
UBS	Apr-15	Clearmatics	• Builds an alliance for an industry-wide product "utlity settlement" • Builds smart bonds on the Ethereum platform • Partners with BNY Mellon for specific blockchain projects	*
USAA®	May-15	coinbase	• Creates a pilot program that will let some of its customers view their Coinbase bitcoin balances through their USAA online and mobile accounts	*
Commonwealth Bank	May-15	Ripple	• Partners with Ripple to adopt DLT for payments settlement	*
Nasdaq	May-15	Chain, Linq	• Partners with Chain to create a blockchain platform that enables pre-IPO trading • Uses Linq blockchain technology to complete and record private securities transactions	*
DBS	May-15	Coin Republic	• Runs a blockchain hackathon in Singapore in partnership with Startupbootcamp and Coin Republic	
Santander	Jun-15	Ripple	• Introduces blockchain technology for international payments • Have 20-25 other use cases under exploration	
	Jun-15	Ripple	• Partners with Ripple to develop low-cost, cross-border payments platform	

Financial Institutions	Timeline	Partners	Use Cases
	Jun-15	Ripple	• Partners with Ripple to develop low-cost, cross-border payments platform • Invests in coinbase through its VC arm
citibank	Jul-15		• Have 3 separate systems within Citi that deploy blockchain technology • Develops an equivalent to Bitcoin called Citicoin
	Jul-15		• Starts staffing employees with BTC, blockchain, and cryptocurrency expertise
	Sep-15	In-house	• Files a patent on "System and Method for Wire Transfers using Cryptocurrency"
Deloitte.	May-16		• Launches Smart Identity proof-of-concept to support banks' regulatory client onboarding and Know Your Customer (KYC) processes
Crédit Mutuel ARKEA	Jun-16	IBM	• Announced the completion of their first blockchain project
Goldman Sachs	Sep-16	In-house	• Files a patent on "Systems and Methods for Updating a Distributed Ledger-Based on Partial Validations of Transactions"
Standard Chartered	Sep-16	Ripple	• Implements a blockchain solution for payment
WELLS FARGO	Oct-16	R3	• Uses blockchain technology for a "proof of concept" test on international trade to buy a cotton shipment
VISA	Oct-16	Chain	• Introduces international B2B payment solution built on Chain's blockchain technology
BNP PARIBAS	Dec-16		• Conducts live blockchain payments based on "Cash Without Borders" proof-of-concept
DTCC	Jan-17	Axoni, IBM, R3	• Develops Distributed Ledger Solution for Derivatives Processing and to build the next generation Trade Information Warehouse
Deutsche Bank HSBC KBC Rabobank	Jan-17		• Participates in a new project—called Digital Trading Chain (DTC)—aimed at increasing global trade among small and medium-sized businesses using blockchain, or distributed ledger, technology • Partners include Deutsche Bank, HSBC, KBC, Natixis, Rabobank, SocGen, Unicredit
	Feb-17	Bitfury	• The National Agency of Public Registry, the Republic of Georgia, is working with BitFury on a pilot project that will use a transparent, secure ledger to manage land titles

Note: * denotes deployment in the United States
Source: Let's Talk Payment, "Know more about blockchain: Overview, Technology, Application Areas and Use-cases"

Other Use-cases of Blockchain outside the Financial Sector

Outside the financial realm, there have also been efforts to adopt blockchain for other uses. One area of adoption deals with document retention. For instance, the State of Delaware is currently undertaking the **Delaware Blockchain Initiative**, which will streamline recordkeeping for private and public companies registered in the state. It is also working on legislation that would establish a legal basis for using the technology for this purpose. Specifically, the new law will amend the state's General Corporation Law to account for blockchain usage, such as in keeping records of share issuance. The state also plans to enable filers to have the opportunity to use smart-contract versions of UCC documents on a distributed ledger.

Internationally, there are also efforts to utilize blockchain for record-keeping purposes. For instance, the Republic of Georgia's National Agency of Public Registry (NAPR) has been working with Bitcoin company Bitfury to pilot a blockchain land-titling project and to develop projects for other governmental departments. Also, ID2020—a public-private partnership based in the United Kingdom—has been working with the United Nations High Commissioner for Refugees (UNHCR) to develop solutions that would help governments digitize national card systems and provide legal identity, including birth registration, to everyone, including refugees. These use-cases illustrate examples of how blockchain could help "import governance" into areas where the functioning of local governments could be improved.

In addition, there are also efforts to create other blockchain-type architecture for new types of deployment, such as software execution and data storage. For instance, Ethereum is a decentralized platform that runs smart contracts. Ethereum essentially creates a virtual machine linking various computers on the network together without the need for existing trust among machines on the network. This allows software to run on the computing power of various computers on the network. As another example, Filecoin is developing a data storage network and electronic currency based on blockchain. Filecoin allows users to share storage space and earn filecoin—a digital currency—as compensation for the storage space provided by the users. The platform effectively applies blockchain concepts of a shared ledger, cryptography, and consensus mechanism to create a storage application built on a trustless network. These applications illustrate the potential of blockchain to transform technological landscapes in various industries.

.

III. Blockchain and the Current Regulatory Environment

Given its potential to transform the financial industry, blockchain has garnered significant attention from lawmakers and financial regulators. These officials are eager to understand how they should manage the emergence of blockchain, whether existing laws are sufficient to provide consumer protection and safeguard the financial system, what they should do to ensure compliance and promote innovation, and what problems they should anticipate in their efforts to manage the technology. Seeking to address these questions, this section starts by providing an overview of how the regulators are dealing with the emergence of blockchain and what problems that they are witnessing today. This will serve as a lead-in to the discussion on key policy problems and potential solutions in the subsequent sections.

III.1. Engagement by U.S. Regulators

The U.S. financial system is governed by several regulatory agencies. Different applications of blockchain hence require engagement by different sets of regulators. So far, regulators have been applying existing framework with minimal problems. However, this may soon change as the industry develop more products challenging prevailing schemes. In cases where new applications of the technology do not easily fit within the existing laws, or where there is ambiguity, regulators have been pursuing *ad hoc* approaches to handle such situations.

As an example, since most of the deployment of blockchain within the financial sector to date has been to upgrade existing transaction infrastructure—such as modernizing clearing and settlement mechanisms, or modifying money transfer processes—financial institutions that deploy these technologies must remain compliant with existing laws, such as the Bank Secrecy Act of 1970 (which includes the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) provisions) and the USA Patriot Act of 2001 (which includes the Know-Your-Customer (KYC) provisions). Moreover, technology partners must satisfy third-party vendor requirements (such as the OCC's third-party provider guidance) and pursue a roll-out process that meets certain standard (such as the Information Technology Infrastructure Library (ITIL) framework). Hence, in most cases, the existing regulatory framework provides sufficient mechanisms to oversee the deployment of the technology.

Moreover, the regulators have so far been accommodative to new use-cases of the technology. For instance, in 2015, the Securities and Exchange Commission (SEC) approved online vendor Overstock's plan to issue securities on its own custom-built blockchain stock exchange. The commission is also working with two separate exchanges competing to be the first to host a Bitcoin exchange traded fund (ETF). In cases where new applications challenge existing laws, the regulators have also responded judiciously. For instance, reacting to Ripple's issuance of its digital currency XRP, the Financial Crimes Enforcement Network (FinCEN) fined the company for failing to register as a money services business (MSB) and for failing to implement appropriate anti-money laundering (AML) procedures. Additionally, the Commodity Futures Trading Commission (CFTC) also took action in September 2015, ordering an unregistered Bitcoin options trading platform to cease operations. These regulatory actions have so far helped ensure compliance and promote consumer safety.

Besides these engagements, several regulators have also undertaken efforts to understand and encourage the development of blockchain. For instance, seven regulatory agencies—including the Department of Justice, the Department of Homeland Security, the Federal Bureau of Investigation, and Secret Service, the Department of Immigration and Customs Enforcement, Marshals Service, and the CFTC —are all parts of the Blockchain Alliance, a public-private partnership aimed at promoting dialogue between industry

and regulators to help combat criminal activity on blockchain. Furthermore, the SEC has also established a distributed ledger working group within the commission to educate their peers about the technology and to coordinate cross-agency regulatory efforts with federal, state and local law enforcement. In addition, the SEC's Specialized Working Group on Equity Market Structure has also established its own Blockchain Taskforce with the responsibility of analyzing the impacts of blockchain on investment management, trading, and markets.

Lastly, some regulatory agencies have also issued statements urging more engagements by regulators in the development of blockchain. Most-often cited is the statement by CFTC Commissioner J. Christopher Giancarlo in January 2017, in which he outlined practical steps that the CFTC and other financial regulators should take to promote DLT and other financial technology. (see the box below for more details). Other agencies have also published reports or issued statements on blockchain and digital currencies. Exhibit 10 lists such engagement by U.S. federal regulators.

CFTC's Proposed "Practical Steps" for Financial Regulations

On January 18, 2017, CFTC Commissioner J. Christopher Giancarlo delivered a speech before SEFCON VII (Swap Execution Facilities Conference), during which the commissioner suggested practical steps that would allow the CFTC and other financial regulators to promote usages of distributed ledger and other financial technology. The suggestion centers around the "do no harm" approach and includes five steps as follows:

1. *Putting Our Best Foot Forward:* Financial regulators should designate dedicated, technology savvy teams to work collaboratively with technology companies to address issues of how existing regulatory frameworks apply to new, digital products, services and business models derived from innovative technologies, including DLT;
2. *Allowing "Breathing Room":* Financial regulators should foster a regulatory environment that spurs innovation similar to the FCA's sandbox, where financial technology businesses, working collaboratively with regulators, have appropriate "space to breath" to develop and test innovative solutions without fear of enforcement action and regulatory fines;
3. *Getting Involved:* Financial regulators should participate directly in financial technology proof of concepts to advance regulatory understanding of technological innovation and determine how new innovations may help regulators do their jobs more efficiently and effectively;
4. *Listening and Learning:* Financial regulators should work closely with financial technology innovators to determine how rules and regulations should be adapted to enable 21st century technologies and business models; and
5. *Collaborating Globally:* Financial regulators should provide a dedicated team to help financial technology firms navigate through the various state, federal and foreign regulators and regimes across domestic and international jurisdictions.

This suggestion has often been cited by industry experts as an appropriate framework that would promote innovations in the financial industry. The commissioner also encourages regulators to cultivate a regulatory culture of forward thinking, refocusing the agencies to get ahead of the curve of changes taking place in global trading markets.

Source: J. Christopher Giancarl, "Keynote Address of CFTC Commissioner J. Christopher Giancarlo before SEFCON VII," January 18, 2017.

Exhibit 10: Engagement by federal regulators on virtual currencies and distributed ledgers (as of 2016)

Agency	Country	Position	Format	Topic	Summary
US Senate	USA	~	Letter to regulators	Virtual Currencies / Distributed Ledgers	"Request to regulators for guidance on these technologies US House of Representatives USA Neutral Non-binding resolution Virtual Currencies / Distributed Ledgers Resolution calling for a national technology innovation policy including digital currencies and blockchain technology"
US House of Representatives	USA	~	Non-binding resolution	Virtual Currencies / Distributed Ledgers	"Resolution calling for a national technology innovation policy including digital currencies and blockchain technology"
Congress	USA	+	Study group set-up	Virtual Currencies / Distributed Ledgers	"Creation of a caucus (study group) dedicated to bitcoin and blockchain"
FinCEN	USA	~/-	Report	Virtual Currencies	"Guidance to avoid illicit activities through the use of virtual currencies CFPB USA Neutral to Negative Report Virtual Currencies Statement about big issues have yet to be solved regarding virtual currencies"
CFPB	USA	~/-	Report	Virtual Currencies	"Statement about big issues have yet to be solved regarding virtual currencies"
FINRA	USA	+	Report	Distributed Ledgers	"Statement highlighting key applications being explored in the securities industry, potential impact of the technology, and discussion of key implementation and regulatory considerations for broker-dealers."
OCC	USA	+	Report	Distributed Ledgers	"Statement about how DLT has the potential to transform how transactions are processed and settled CFTC USA Positive Declaration Distributed Ledgers Statement about how blockchain may give regulators transparency"
CFTC	USA	+	Report	Distributed Ledgers	"Statement about how blockchain may give regulators transparency"
SEC	USA	~	Declaration	Distributed Ledgers	"Statement about the commitment of the agency in actively exploring blockchain regulation Federal Reserve USA Positive Declaration / Report Virtual Currencies / Distributed Ledgers Statement about how blockchain may represent the most significant development in many years in payments, clearing, and settlement. In the context of payments, DLT has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography"
Federal Reserves	USA	+	Declaration	Virtual Currencies / Distributed Ledgers	"Statement about how blockchain may represent the most significant development in many years in payments, clearing, and settlement. In the context of payments, DLT has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography"

Source: BBVA, *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*, December 2016.

Besides engagement by federal regulators, some states have also taken initiatives both to regulate and to utilize blockchain and digital currencies. The degrees of engagement vary from observatory (California), to participatory (Delaware and Illinois) and assertive (New York). Most states participate through legislative efforts, although some states—such as Delaware and Illinois—also plan to utilize blockchain for record-keeping. Exhibit 11 summarizes such efforts by various states.

Exhibit 11: Engagement by various states on virtual currencies and distributed ledgers (as of 2016)

State	Topic	Summary
New York	Virtual Currencies	"The New York Department of Financial Services (NYDFS) published BitLicense regulations for virtual currency businesses in June 2015. According to these regulations, firms engaged in "Virtual Currency Business Activity" that involves New York or a New York resident are required to apply for a BitLicense within 45 days of the effective date of the regulation. Applicants for a license are required to have, among other things, Anti-Money Laundering/Know Your Customer, Consumer Protection and Cybersecurity programs."
Vermont	Distributed Ledgers	"In May 2016, Vermont adopted legislation to recognize blockchain data in the court system. The relevant provision is part of Bill H868 (An act relating to miscellaneous economic development provisions). In essence, the bill harmonizes blockchain data with Vermont's state law on the kinds of evidence admissible in court. Any document notarized using blockchain technology is to be considered legally admissible in court and have full legal bearing. The bill also establishes how the veracity of that certification can be challenged in court. However, Rep Bill Botzow, Chair of the Vermont House Committee on Commerce and Economic Development has emphasized that the bill is to apply "only to documents as opposed to financial transactions"."
North Carolina	Virtual Currencies / Distributed Ledgers	"The North Carolina Money Transmitter Act was recently extended to cover bitcoin traders with House Bill 289, signed in July 2016 by State Governor Pat McCrory. The revised act is a Bitcoin-Friendly 'Virtual Currency Law.' It updates the existing laws to define the term "virtual currency" and the activities that trigger licensure. Virtual currency miners and blockchain software providers will not require a license for multi-signature software, smart contract platforms, smart property, colored coins, and non-hosted, non-custodial wallets."
Delaware	Distributed Ledgers	"Through its Delaware Block Initiative, launched in April 2016, the state plans to engage technology vendors to help businesses and state agencies use blockchain technology to distribute, share, and save ledgers and contracts. The Initiative will first work on using blockchain technology to store contracts and other essential corporate data on a distributed ledger. It will also use distributed ledger techology to store the Delaware Public Archives."
California	Virtual Currencies	"In late 2015, Bill 1326 was introduced to license virtual currency businesses (the Initial Bill) but it was discontinued. The revised bill, which was re-submitted to the legislature, will establish the Californian Digital Currency Business Enrollment Program (CDCBEP)—an equivalent of a regulatory sandbox—to help the state learn more about the technology."
Illinois	Distributed Ledgers	"The State of Illinois announced a consortium of Illinois state and county agencies, known as the Illinois Blockchain Initiative, who will collaborate to explore innovations presented by Blockchain and distributed ledger technology. The Department of Innovation and Technology (DoIT) is actively engaged in this effort. The goal of the initiative is to determine if this groundbreaking technology can be leveraged to create more efficient, integrated and trusted state services, while providing a welcoming environment for the Blockchain community. As part of this effort, the Illinois Blockchain Initiative recently published on the Illinois Procurement Bulletin (IPB) a Request for Information (RFI) to invite participants to submit non-price information about Blockchain and distributed ledger technology."

Source: BBVA, *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*, December 2016. Augmented by the author.

As Exhibit 10 and Exhibit 11 illustrate, regulators and lawmakers have been eager to understand the potential impacts of blockchain on the financial industry. In most cases, policymakers are optimistic about the technology and supportive of blockchain deployment. In certain cases, federal regulators have also begun to clarify how the existing laws will be applied to some blockchain applications, especially virtual currencies. Some states have also enacted new legislation to regulate virtual currencies (such as New York) or undertaken initiatives to use blockchain themselves (such as Delaware and Illinois). Nevertheless, more and better engagement by regulators will likely be required, as shall be discussed further in Section IV.

III.2. Engagement by Foreign Regulators

Outside the United States, several countries have also taken proactive approaches to promote the development and deployment of blockchain. Among the forefronts are the United Kingdom, Singapore, and Australia. According to some experts, these financial centers pursue proactive measures with hopes to become leaders in international finance by staying at the forefront of financial innovation. Some countries hinted that they learned their lessons from the internet revolution in the 1990s during which they either failed to engage with the industry more actively or imposed restrictive regulation too soon, which drove innovation away. Exhibit 12 provides examples of engagement by foreign regulatory agencies.

Exhibit 12: Engagement by foreign authorities on virtual currencies and distributed ledgers (as of 2016)

Authority	Region	Position	Format	Topic	Summary
European Parliament	Europe	~/+	Report / Taskforce	Virtual Currencies / Distributed Ledgers	"Hands-off approach to regulating blockchain technology. Creation of a task force to analyse it."
European Commission	Europe	~	Directive / Taskforce	Virtual Currencies / Distributed Ledgers	"Inclusion of virtual currencies players in the AML Directive. DLT workstream inside the Financial Technology Task Force."
EBA	Europe	-	Reports	Virtual Currencies	"Recommendation to banks not to deal at all with virtual currencies, and amendments to the EC decision to include virtual currencies players in the AMLD ESMA EU Positive Public Consultations Virtual Currencies / Distributed Ledgers Consultations on investment using virtual currency or DLT and on DLT applied to securities markets."
ESMA	Europe	+	Public Consultations	Virtual Currencies / Distributed Ledgers	"Consultations on investment using virtual currency or DLT and on DLT applied to securities markets."
FCA	UK	+	Declaration / Sandbox Initiative	Distributed Ledgers	"Statement about considering approving blockchain-based firms into their Sandbox Initiative (finally, 9 out of 16 approved firms use DLT)."
ECB	Europe	+ on DLT - on VC	Reports / Declaration	Virtual Currencies / Distributed Ledgers	"The ECB has analyzed virtual currencies and identified potential risks. In fact, it has warned the EC not to encourage the use of virtual currencies in order to keep controlled money issuance. On the other side, it sees potential benefits in the use of distributed ledgers in post-trading activities. And it has started a joint project with Bank of Japan to analyze potential use of DLTs."
National Central Banks	Several countries	+	Declaration / BoE report	Virtual Currencies / Distributed Ledgers	"A number of central banks have stated serious interest in the issuance of their own currencies. The Bank of England have published a paper on this topic."

Source: BBVA, "Blockchain in financial services: Regulatory landscape and future challenges for its commercial application," December 2016.

Note that one of the reasons that some countries have been able to be more proactive compared to the United States is the fact that their regulatory regimes are more consolidated. These countries generally have either one or a couple of regulatory bodies. For instance, the United Kingdom has only the Financial Conduct Authority (FCA), Singapore has only the Monetary Authority of Singapore (MAS), and Australis has Australian Prudential Regulation Authority (APRA) and Australian Securities and Investments Commission (ASIC). In contrast, the United States has more than ten federal financial regulators, coupled with state-federal complexity. This makes it more difficult for different U.S. regulatory agencies to engage with the industry in a more unified and proactive manner.

One of the most popular forms of engagement by various countries is through the concept of **regulatory sandbox**. Several countries—including the United Kingdom, Singapore, Australia, Canada, Hong Kong, Malaysia, and the United Arab Emirates, among others—are exploring or have launched their versions of the sandboxes. In some of these sandboxes, companies that utilize blockchain and DLT represent a majority of their participants. For instance, 9 out of the 18 companies that have begun testing their products in the FCA's sandbox in the first cohort are developers of blockchain or DLT applications. See Exhibit 13 for a complete list of companies in the FCA's sandbox.

Exhibit 13: List of Companies in the FCA's Sandbox (First Cohort)

Firm	Description	
Billon	An e-money platform based on distributed ledger technology that facilitates the secure transfer and holding of funds using a phone based app.	*
BitX	A cross-border money transfer service powered by digital currencies / blockchain technology.	*
Blink Innovation Limited	An insurance product with an automated claims process, which allows travellers to instantly book a new ticket on their mobile device in the event of a flight cancellation.	
Bud	An online platform and app which allows users to manage their financial products, with personalised insights, on a single dashboard. Bud's marketplace introduces relevant services which users can interact with through API	
Citizens Advice	A semi-automated advice tool which allows debt advisers and clients to compare the key features of available	
Epiphyte	A payments service provider that aims to provide cross-border payments using blockchain technology.	*
Govcoin Limited	A technology provider that has partnered with the Department for Work and Pensions (DWP) to determine the feasibility of making emergency payments using means other than cash or the Faster Payments Scheme. The payments platform will use blockchain to allow the DWP to credit value to a mobile device to transfer the value	*
HSBC	An app developed in partnership with Pariti Technologies, a FinTech start-up, to help customers better manage	
Issufy	A web-based software platform that streamlines the overall Initial Public Offering (IPO) distribution process for investors, issuing companies and their advisors.	
Lloyds Banking Group	An approach that aims to improve the experience for branch customers which is aligned with the online and over the phone experience.	
Nextday Property Limited	An internet-based property company that will provide an interest free loan for a guaranteed amount to customers if they are unable to sell their property within 90 days.	
Nivaura	A platform that uses automation and blockchain for issuance and lifecycle management of private placement	*
Otonomos	A platform that represents private companies' shares electronically on the blockchain, enabling them to manage shareholdings, conduct bookbuilding online and facilitate transfers.	*
Oval	An app which helps users to build up savings by putting aside small amounts of money. These savings can then be used to pay off existing loans early. Oval will be working with Oakam, a consumer credit firm, and a number of their customers during the test period.	
SETL	A smart-card enabled retail payment system based on their OpenCSD distributed ledger.	*
Tradle	An app and web-based service that creates personal or commercial identity and verifiable documents on a distributed ledger. In partnership with Aviva they will provide a system for automated customer authentication.	*
Tramonex	An e-money platform based on distributed ledger technology that facilitates the use of "smart contracts" to transfer donations to a charity.	*
Swave	A micro savings app that provides an across-account view; enables a round-up service every time a user spends money and calculates an affordable savings amount based on the user's spending behaviour.	

Note: * denotes use of blockchain or DLT; Note also that six additional companies were granted access to the FCA's sandbox but were not ready to begin testing and will be part of cohort two instead.

Source: FCA, "Financial Conduct Authority unveils successful sandbox firms on the second anniversary of Project Innovate," November 7, 2016.

Fundamentally, regulatory sandbox provides a "safe space" for businesses to test products with less risk of being punished in case of noncompliance. In exchange for more flexible standards, regulators often require applicants to incorporate appropriate safeguards in their testing models, ranging from customer protection measures (such as requiring informed consent), financial limits (such as limiting the amount of money that can be invested by a customer), and various risk controls (such as fraud detection and cyber security). See more discussion on the regulatory sandbox concept in Section V.4.

Besides these efforts by foreign regulators, several international consultative bodies have also issued statements expressing their interests in the topic. Nevertheless, most of them have only provided preliminary education about the technology. Exhibit 14 lists the engagement by international agencies.

Exhibit 14: Engagement by international consultative bodies on virtual currencies and distributed ledgers

Authority	Region	Position	Format	Topic	Summary
FATF	Global	~ / -	Report	Virtual Currencies	"Recommendations for avoiding illicit activities related to virtual currencies."
FSB	Global	~ / +	Declaration	Distributed Ledgers	"Statement including distributed ledger technology among their priorities for 2016 OICV-IOSCO Global Neutral Declaration Distributed Ledgers Committed to analyse the impact of blockchain in the framework of their Securities Markets Risk Outlook."
OICV-IOSCO	Global	~	Declaration	Distributed Ledgers	"Committed to analyse the impact of blockchain in the framework of their Securities Markets Risk Outlook."
BIS	Global	~ / -	Report	Virtual Currencies	"Statement about the effect of digital currencies in reducing role of central banks IMF Global Positive Report Virtual Currencies / Distributed Ledgers Publication of specific reports on virtual currencies and distributed ledgers (considering them as "The Internet of Trust")."
IMF	Global	+	Report	Virtual Currencies / Distributed Ledgers	"Publication of specific reports on virtual currencies and distributed ledgers (considering them as "The Internet of Trust")."
World Bank	Global	+	Article	Distributed Ledgers	"Article analysing how blockchain technology redefines trust in a global digital economy."
WEF	Global	+	Report	Distributed Ledgers	"Statement about how blockchain will become "beating heart" of the global financial system."

Source: BBVA, *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*, December 2016.

III.3. Case Study: Regulations Related to Money Transfer

III.3.A. Background on Money Transfer Regulations

One key area in which blockchain and DLT are being used is the money transfer business. This section explores regulatory background as it relates to money transfer in the United States and how blockchain and DLT interplay with the existing regulatory framework.

In the United States, companies that transfer funds are considered **money transmitters** engaging in **money services businesses (MSBs)**.[7] FinCEN—a regulatory body under the U.S. Department of the Treasury—regulates money transmitters pursuant to the Bank Secrecy Act ("BSA"), which also includes elements of the Patriot Act. Under this framework, money transmitters must:[8]

- Register with FinCEN;
- Undergo an initial risk assessment and adopt an anti-money laundering policy based on those risks;
- Appoint a qualified compliance officer with specific qualifications;
- Train employees in the operationalization and implementation of the compliance program; and
- Undergo regular independent testing and review of the business' compliance program.

Money transmitters must also report to FinCEN personal information of their customers as well as transactional data, particularly those that are above a certain amount or imply suspicious activities. In case of high risk clients, the business must take measures to mitigate such risks or deny services to customers.

Beside federal registration, most states also require licensure. Whereas the federal requirements imposed by FinCEN aim to prevent money laundering, state regulators aim to protect consumers. In some cases, this includes the exercise of "extraterritorial jurisdiction," whereby any business servicing or soliciting the state's citizens must satisfy that state's licensing requirements even without any physical presence in that state. Hence, a money transmitter wishing to operate across states must obtain licenses in all the states that it wishes to operate. Licensure typically includes disclosure requirements, which may encompass: audited financial statement of the business, financial records of control persons, list of all lawsuits and criminal complaints against control persons, criminal and civil background checks, among others. Additionally, some states also require money transmitters to carry surety bond—in some cases of at least $500,000—and to satisfy minimum capitalization requirements.

Companies engaging in money transfer may also choose to become a federally chartered bank instead, circumventing state licensing requirements. However, this subjects them to a different set of regulations, which could be even stricter. Specifically, a company may obtain a federal banking charter from the Office of Comptroller of Currency (OCC). Doing so, the company becomes subject to federal regulation by either the Federal Reserve and/or the Federal Deposit Insurance Corporation (FDIC).[9] Moreover, federal banks also remain subject to regulation by FinCEN and the Office of Foreign Assets Control, as well as various other regulatory and prosecutorial agencies. This is compounded further by the volume of banking regulations, including the Bank Secrecy Act, the USA Patriot Act, and Dodd-Frank Wall Street Reform and Consumer Protection Act, and more.

[7] According to the Internal Revenue Services, a Money Services Business (MSB) generally refers to any person offering check cashing; foreign currency exchange services; or selling money orders, travelers' checks or pre-paid access (formerly stored value) products; for an amount greater than $1,000 per person, per day, in one or more transactions. A person who engages as a business in the transfer of funds is an MSB as a money transmitter, regardless of the amount of money transmission activity.

[8] Source: Coin Center, "What is Money Transmission and Why Does it Matter?," April 7, 2015.

[9] Alternatively, a company may instead become registered as a credit union—either by states or at the federal level by the National Credit Union Administration, although they are still subject to regulation by the Federal Reserve and in some cases the FDIC.

This shows that becoming a money transmitter is neither easy nor cheap. Nevertheless, both federal and state legislature create these safeguards to ensure the safety of consumers and soundness and solvency of the banking system.

III.3.B. Issues for Blockchain/DLT Deployment

With the introduction of Bitcoin and blockchain, questions arose whether digital currencies and technology companies that enables the transfer of money via blockchain should be subject to the same regulatory requirements as traditional money transmitters.

Initially, digital currency businesses assumed that they were software companies operating largely in an unregulated space. Even though the services provided by some of these companies resemble those provided by traditional money transmitters, these companies assumed that they should not be subject to the existing regulations.

This changed in March 2013 when FinCEN published a guidance, announcing that digital currencies such as Bitcoin shall be treated in the same fashion as fiat currencies with respect to the money transmission laws. This means that any businesses that facilitate the transmission of Bitcoin (or other digital currencies) from one person to another, and those that exchange fiat currencies for Bitcoin, as well as payment processors who accept Bitcoin are all money transmitters. However, businesses that accept Bitcoin as a form of currency are not considered money transmitters. As a result, Ripple, which uses its own digital currency, XRP, as a medium of money transfer, became subject to money services business regulations, and the company was subsequently fined for its failure to register as a money transfer agent.

Despite the additional clarity provided by FinCEN, state-level regulations remains ambiguous. Except for a few states, most state regulators have taken a "wait and see" approach and offered little guidance related to digital currencies and blockchain. Those that have offered guidance are also treating digital currencies differently. For instance, while Texas and Kansas have published official guidance concluding that digital currencies shall be treated the same way as fiat currencies, New York proposed digital currency-specific license, dubbed "BitLicense," to govern companies dealing with digital currencies in the state.

Additionally, new applications for blockchain, particularly those related to digital tokens, add more complexity to the equation. For instance, Filecoin—a shared storage company which utilizes blockchain to enable users to share their data storage space—issues its own digital token as a compensation for users who provide their data storage to the network. Since the company issues digital tokens (called "filecoins") in exchange for services provided by its customers, Filecoin is not considered a money transmitter. However, if it allows users to trade filecoins with one another, will they then become a money transmitter? Also, should this digital token be treated differently from digital assets issued by companies such as Ethereum, which issued ethereum coins (ETH) as securities to raise money? What should be the process of making this determination? Who should have the authority to do so? As the industry invents more applications for blockchain, more questions like these will likely emerge.

The biggest challenge facing regulators however lie in the difficulty in managing the distributed financial architecture enabled by blockchain. In the current system whereby financial institutions and companies serve as intermediaries in a transaction, financial regulators can simply monitor the activities of these intermediaries and entrust them to monitor their clients. In a blockchain-enabled world where these actors are disintermediated, this approach will no longer work. The problem is further exacerbated by the

fact that blockchain offers user anonymity. This makes any efforts to regulate the actual parties more difficult. Finally, blockchain also allows transactions to occur globally, making regulation in one jurisdiction ineffective. In the Unites States, we are already seeing U.S. residents opening Bitcoin accounts overseas and engaging in transactions that fall outside the purview of U.S. regulators.

Last but not least, the unwieldiness of the existing regulatory framework also poses the risk that regulation will stifle innovation. Although it is difficult to prove this claim, some experts point to the fact that several leading blockchain and digital currency companies are domiciled overseas. For instance, Ethereum, the most-recognized distributed platform that runs smart contract, is invented by a Russian programmer residing in Canada, and the organization supporting the technology is based in Switzerland. Others also suggest that several startups have exited New York after BitLicense came into effect.[10] Additionally, among the top 20 cryptocurrency exchanges, only 7 are located in the United States (see Exhibit 15 for the list).

Exhibit 15: Top 20 Bitcoin Exchanges

#	Company	Location	#	Company	Location
1	Coinbase	San Francisco, USA	11	PAXFUL	Delaware, USA
2	Poloniex	Delaware, USA	12	Bitfinex	Hong-Kong
3	Localbitcoins	Helsinki, Finland	13	Bittrex	Las Vegas, USA
4	CEX.IO	London, UK	14	Bittstamp	London, UK
5	Kraken	San Francisco, USA	15	BTCC	China
6	Xcoins	Santa Monica, USA	16	Shapeshift	Switzerland
7	GDAX	San Francisco, USA	17	bitcoin.de	Germany
8	Yobit	Russia	18	Kcoin	China
9	Blockchain.info	Luxembourg	19	Unocoin	Bangalore, India
10	bitsquare	p2p (decentralized)	20	bitFlyer	Tokyo, Japan

Source: BestBitcoinExchange.io

III.3.C. Implications for the Financial Industry

As this case study illustrates, some of the existing regulations—including those related to money transmission—are cumbersome, unequipped to deal with new issues resulting from blockchain and virtual currencies, and unsupportive of innovation. Moreover, the current reactive engagement by regulatory agencies is also exposing consumers and the financial system to potential risks. Hence, financial regulators must find ways to fill the gap between what the existing laws can protect and what blockchain can do. The need for action is urgent, given that a "wait-and-see" approach could lead to three potential problems as follows.

First, by applying existing regulations to new technology, regulators are forcing companies to build only products that could fit within the existing regulatory framework. This could limit innovation, both in terms of technological development and commercial originality. As a result, some new businesses may choose either to ignore the existing laws, relocate overseas, or abandon certain products, none of which is positive for the United States.

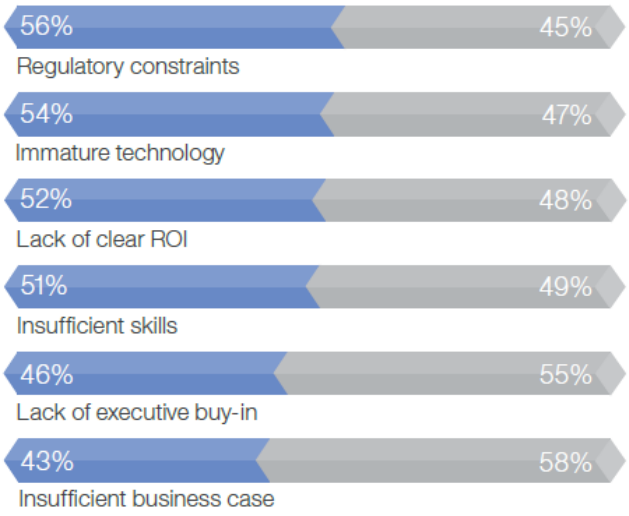
Second, for businesses that can fit within the existing framework, the cost of doing so may still prove insurmountable. In the case of a money transfer business, existing regulations have shown to be

[10] Fortune, "Behind the "exodus" of Bitcoin startups from New York," August 14, 2015.

cumbersome and ambiguous in dealing with digital currencies. This represents both a barrier to entry for startups as well as an ongoing burden for more established companies.

Finally, the ambiguity and complexity of the existing regulations will lead to noncompliance and undermine the regulators' ability to protect consumers and the financial system. All these will ultimately weaken the leadership of the United States in both the financial and technological arenas.

Exhibit 16: Barriers to Implementing Blockchains According to Banks leading the Adoption of Blockchain



Source: IBM, *Leading the pack in blockchain banking*, September 2016.

IV. Regulators' Challenges in Managing Blockchain

IV.1. The Problem of Ineffective Engagement

As the previous section illustrates, the emergence of new technology often gives rise to new policy challenges. In the case of blockchain, its applications within the existing regulatory framework and in new frontiers bring about different challenges. For instance, the use of blockchain by financial institutions to upgrade their technical backend raises questions about the robustness of the technology. On the other hand, new use-cases—such as digital token and direct money transfer—raises questions about how these use-cases should be regulated, and what the potential consequences are for consumers. In either case, the emergence of blockchain raise an important question for regulators and policymakers: How can the government best promote and facilitate blockchain-technology advancement in the public interest while also serving the equally important objectives of financial industry regulation?"

Because the technology is evolving rapidly, challenges related to blockchain are also multiplying and becoming more complicated. To be able to address these challenges effectively, regulators and legislators must engage with industry players to understand the evolution and use-cases of the technology. This leads to the main argument of this paper: based on the current dynamics, **there is a lack of unified and effective engagement by regulators and legislators in the development and deployment of blockchain technology.**

> ***"The main problem is the lack of unified and effective engagement by policymakers in the development and deployment of blockchain technology."***

This is not to say that there has been no engagement by regulators to date. In fact, as discussed in Section III, several regulatory agencies, both at the federal and state levels, have engaged with the financial and technology industries in the deployment of blockchain. Several industry players have also expressed their appreciation for the regulators' efforts to keep themselves educated about the technology and its potential risks. However, such engagement so far has been haphazard, with each regulatory agency exerting its own authority when and how it deems appropriate. There is no unified regulatory framework, guideline, or platform for technology developers and users to explore various use-cases of the technology.

The lack of proper and consistent engagement by regulators potentially leads to two potential key issues:

- *Lack of Clarity on How the Technology will be Regulated:* From the industry's standpoint, reactive and haphazard engagement by the regulators could lead to confusion around how the technology will be regulated going forward. New applications of blockchain that do not fit squarely within the existing laws will raise questions about the laws will be applied to those applications and whether new regulations will emerge. This uncertainty may lead some developers and users of the technology to take either an excessively cautious approach—which will stifle innovation—or an aggressive approach—which will lead to poor compliance—in adopting the technology.

- *Difficulty for Regulators and Policymakers in Identifying Key Areas of Risks and Providing Appropriate Responses:* As blockchain evolves and new use-cases emerge, the technology will likely introduce new

risks to the financial system. Without close and consistent interaction with the industry, regulators and policymakers could fail to recognize some potential risks and become unprepared to provide appropriate responses. Although in some cases the regulators may be able to respond quickly or address the problems as they occur, such reactive approach could still be suboptimal, especially if the risks are significant.

It is worth noting again that these problems arise partly because the regulatory regime for the U.S. financial system is cumbersome. Simplifying the regulatory and organizational structure would enhance collaboration among the regulators and the industry. However, doing so requires a massive reform. Before that happens, the regulators and legislators could still improve the ways that they engage with the financial and technology industries. Section V discusses some potential alternatives to do so.

IV.2. Specific Challenges and Opportunities from Blockchain

Blockchain offers several new use-cases for the financial industries. The mismatch between these use-cases and the existing regulatory framework, coupled with the rapid pace of the technological evolution, could lead to potential risks to consumers, financial institutions, and the financial system. Some of these challenges include:

- *Lack of Clarity on Compliance Requirements:* New use-cases of blockchain—such as digital token and decentralized payment system—raise questions about applicability of the existing regulatory requirements. For instance, how should an application created by a community of developers to facilitate transfer of digital currencies be regulated? Who should be regulated, given that the software is created by a group of independent developers? How should state-level regulations be applied, especially if the states cannot identify the actual users given blockchain anonymity? Such lack of clarity could lead to the failure to comply and/or higher costs of compliance.

- *Difficulty in Adjusting Regulations to Handle Industry Changes:* The lack of effective engagement by the regulators could prevent them from acquiring sufficient knowledge about the technology to be able to issue proper rules and responses or to assist Congress in devising appropriate legislation. For instance, there remains a disagreement on how digital tokens should be treated: as currencies, commodities, or securities?

- *Risks from Industry Front-running Policymakers:* The lack of clarity on the existing regulatory framework, coupled with possible emergence of new regulations, could incentivize some industry players to "front-run" the regulators by rolling out their products before new guidelines emerge in hope of forcing the regulators to yield to industry demand. The most evident comparison is Uber, in which the application continues in violation of labor laws.

- *Challenges arising from New Business Models:* Blockchain will propel several new business models, some of which could pose regulatory challenges and unknown consequences. For instance, the emergence of a decentralized transaction system raises questions about how such a system should be regulated, how to confirm the identities of relevant parties, how to prevent fraud and money laundering, who to be responsible in the case of fraud and errors, and more.

- *Potential Technical Issues:* Blockchain is a new technology—it has been in existence for less than a decade. Therefore, the robustness of the technology has not yet been proven. In fact, there remain several issues to be resolved even with Bitcoin—the most recognized blockchain application—such as scalability, lag time, and other technical glitches. Moreover, features such as identity verification, privacy, and security also have not been fully integrated. Finally, the use of blockchain to upgrade the technical infrastructure also raises questions about interoperability, technology transition, and system robustness.

- *Potential New Systemic Risks:* Blockchain has the potential to transform the nature of the transaction network from a centralized to a decentralized system. In addition, it enhances the speed of transaction settlement and clearing and improves transaction visibility. Questions remain whether these features will increase or undermine the stability of the financial system. For instance, given the transaction expediency enabled by blockchain, will the regulators be able to analyze transactional data in real-time, and will they be able to respond quickly to prevent a potential disaster?

- *Risks from Bad Actors:* Any financial system is exposed to risks from bad actors; unfortunately, frauds, pyramid schemes, and scams are bound to happen. Because blockchain and digital currencies are new, such risks are potentially heightened as consumers, companies, and regulators are less familiar with the technology. The fact that blockchain changes the way people do business also raise questions about who should be responsible in the case of frauds, whether the damaged parties should be protected and compensated, and who should bear the responsibility of preventing such events and safeguarding consumers.

- *Other Potential Challenges and Opportunities:* Blockchain's revolutionary potential could unveil other policy and societal challenges, not only in the financial industry but also to the society at large. For instance, blockchain could alter the roles of some financial intermediaries, such as banks and brokers, leading to job shrinkage and displacement. At the same time, it could provide other opportunities that would benefit society.

Besides the aforementioned challenges, there are also potential opportunities for the regulators to capture with regards to the emergence of blockchain, such as:

- *Opportunities to Reap Potential Benefits of the Technology by the Government:* Blockchain has the potential to benefit not only businesses and consumers but also the government. For instance, blockchain could allow regulators to monitor financial transactions in real time, improve record-keeping processes, reduce costs of monitoring and regulation, and enhance regulatory enforcement. To reap these benefits, however, the government must be willing to deploy blockchain-based applications itself.

- *Opportunities to Collaborate with Foreign and International Agencies:* Blockchain's potential to transform the financial sector and other industries has captured the attention of policymakers, not only in the United States but also overseas. Several countries have undertaken efforts to capitalize on this trend (see Section III.2 for more details). There have also been collaborative efforts across countries to manage cross-border activities, share best practices, and establish international standards. The United States has the opportunity to a part of such efforts to help set international

rules and standards going forward. Note that so far, the United States has been left out of such engagement, however.

- *Opportunities to Maintain Global Leadership Positions in Finance and Innovations:* Blockchain could transform the financial system, and several countries view this as an opportunity to become leaders in innovation and finance. The United States has the opportunity to take an assertive role in the development of blockchain and other financial technology in order to maintain its leadership positions in both arenas.

International Regulatory Collaboration in Financial Technology

In September 2016, the International Organization of Standardization (ISO) has selected Standards Australia—an independent, not-for-profit organization recognized by the Australian government—to spearhead a technical committee to develop standards for blockchain technology. The committee consists of leading standards organizations from 35 countries, including Canada, France, the United Kingdom, and the United States, among others.

In addition, there have been efforts to establish cross-country partnerships among regulators to share lessons and best practices. Exhibit 17 lists some of the cross-border governmental partnerships on blockchain and financial technology that have been announced to date.

Exhibit 17: International Regulatory Partnerships in Financial Technology

Date	Party	Party	Announcement
03/23/16	United Kingdom	Australia	British and Australian financial regulators sign agreement to support innovative businesses
05/11/16	United Kingdom	Singapore	UK and Singapore to establish 'fintech bridge'
09/13/16	Singapore	Switzerland	Singapore and Switzerland forge fintech pact
09/27/16	Russia	South Africa	CSDs to Collaborate in Distribute Ledger First
10/21/16	Australia	Kenya	Kenyan and Australian Regulators sign agreement to support fintech innovation
10/22/16	Singapore	India	Singapore and the Government of Andhra Pradesh ink FinTech cooperation agreement
10/24/16	Singapore	South Korea	Singapore and South Korea sign up for fintech co-operation
12/06/16	ECB	Bank of Japan	Speech by Yves Mersch, Member of the Executive Board of the ECB
12/09/16	Hong Kong	United Kingdom	Co-operation Agreement between HKMA and FCA
01/13/17	Brussels	United Kingdom	Brussels and London form 'fintech bridge'
02/22/17	United Kingdom	Canada	FCA and OSC sign Co-operation Agreement to support innovative businesses
03/08/17	Singapore	Abu Dhabi	MAS and Abu Dhabi Global Market Collaborate
03/10/17	United Kingdom	Japan FSA	Financial regulators of Japan and UK announce Exchange of Letters

Source: Various news sources.

IV.3. Striving for a Balanced Solution

Because blockchain has the potential to transform several industries and because the technology is evolving rapidly, unified and consistent engagement by financial regulators is crucial. The regulators must find proper ways to interact with the financial and technology industries, balancing between (1) regulating too loosely and thereby introducing risks into the financial system, and (2) regulating too tightly and thereby stifling innovation. Such engagement should aim to help the government monitor activities within industry, learn about the technology and its use-cases, collaborate with industry players, and lead the industry to produce public benefits. Policy alternatives that would facilitate such engagement should aim to achieve the following three objectives:

- *Engage Policymakers in Discussions on Blockchain in Unified and Effective Manners:* The policy should promote collaboration between the regulators and industry participants as well as coordination across regulatory agencies. It should create a platform that allows the regulators to (1) convey clear and consistent messages to industry participants, (2) learn from such interaction and use the lessons learned to adjust their rules and responses, (3) provide appropriate recommendations to legislators to help them adjust the policy frameworks, if necessary.

- *Allow Policymakers to Ensure Regulatory Compliance and Maintain Stability of the Financial System:* Second, the policy should enable the regulators to ensure industry compliance. More importantly, it should preserve the stability of the financial system. This means that the policy should allow the regulators to anticipate and respond quickly to potential risks that may be introduced by the technology into the financial system.

- *Promote Technological Innovation in Blockchain / DLT:* Finally, while the policy should aim to enhance the regulators' understanding of the technology, it should refrain from undermining the industry's incentives to innovate and utilize the technology. While regulatory compliance and consumer protection are crucial, they should not come at the price of innovation.

V. How to Improve Regulators' Engagement

This section lists five potential policy alternatives: (1) Status Quo, (2) Modified Status Quo, (3) Issuance of Regulatory Guideline, (4) Creation of Multi-Party Working Group, and (5) Establishment of Regulatory Sandbox. Aiming to help financial regulators achieve the three aforementioned goals, these alternatives differ in the nature of engagement by the regulators, ranging from decentralized and limited (in the case of status quo) to centralized and interactive (in the case of regulatory sandbox). Note that the regulators could apply these alternatives to manage the emergence of blockchain as well as other financial technology. Below is the description and analysis of these alternatives.

V.1. Status Quo

Under status quo, financial institutions and technology companies develop and deploy blockchain applications under the existing regulatory framework with limited engagement from financial regulators. This means that companies must comply with the existing laws, and the regulators will monitor compliance and pursue actions when necessary.

This is the current approach that most U.S. regulators have been pursuing, and therefore it requires no changes to the regulators' courses of actions. Moreover, so far it has proven effective in ensuring compliance and preventing harm to consumers, as evidenced by the limited number of media reports on consumer damages related to digital currencies and blockchain, although this is partly due to limited adoption of the technology to date.

Despite these advantages, most industry participants have voiced the following concerns. First, the existing regulatory framework is cumbersome. The often-cited example is the money transfer regulation (see Section III.3) which requires money transmitters to be registered with FinCEN and to comply with state laws governing money services business. These requirements have proven costly, and as a result only companies with sufficient funding can engage in money services business.

Second, status quo provides limited clarity on the applicability of existing laws on new technology or new application, which could result in unintentional noncompliance. For instance, in May 2015, Ripple was fined $700,000 for "willful violations" of the Bank Secrecy Act for failing to register with FinCEN as a money transmitter prior to selling XRP, a digital token used to settle payments on its network. Ripple argued that its noncompliance was due to the ambiguity in FinCEN's registration requirement, which was subsequently clarified in FinCEN's ruling in 2015. Note that although Ripple was able to continue its operations despite the fine, such penalty could spell financial doom for smaller companies.

In summary, although financial regulators have been able to manage new blockchain applications to date, industry participants argue that the "reactive engagement" by the regulators imposes unnecessary costs on the industry in terms of the ambiguity of the existing laws and their incompatibility with the technology. In the long-run, this could stifle innovation in the United States and drive technology startups to seek other operating jurisdictions that are more amenable to their businesses.

The European Union's Handoff Approach to Blockchain

The United States is not the only country that is adopting a status quo approach to blockchain regulation. At the moment, the European Union is doing so as well. In February 2017, the European Securities and Markets Authority (ESMA) issued a reported on DLT, in which it outlines ESMA's view on DLT and indicates its position that "regulatory action is premature at this stage, considering that the technology is still at an early stage." Below is an excerpt from the report:

> *"ESMA, as well as identifying the benefits, also points to some important challenges for DLT in terms of interoperability, governance and privacy issues and risk creation. These challenges would require further attention before any large-scale use of DLT across the financial services sector. An important point for the technology's advocates and developers to be aware of are the existing rules and their application to DLT. The development of a new technology, such as DLT, does not liberate users from complying with the existing regulatory framework, which provides important safeguards to ensure the stability and proper functioning of financial markets.*
>
> *However, drawing on the responses to its Discussion Paper, ESMA's view is that the current EU regulatory framework does not represent an obstacle to the use of DLT in the short-term. Meanwhile, a number of concepts or principles, such as the legal certainty attached to DLT records or settlement finality, may require clarification. In addition, ESMA points out that beyond pure financial regulation, broader legal issues, such as corporate law, contract law, insolvency law or competition law, may affect the deployment of DLT."*

Source: ESMA, *The Distributed Ledger Technology Applied to Securities Markets*, February 7, 2017.

V.2. Modified Status Quo

Under this approach, the regulators either modify the existing laws or issue new laws to facilitate the emergence of the new technology. Examples of this approach include (1) the plan by the Office of the Comptroller of the Currency (OCC) to issue fintech charter to technology companies offering financial services and (2) the enactment of BitLicense regulation by the State of New York.

In the first instance, the OCC announced in December 2015 its plan to consider applications from financial technology (fintech) companies to become special purpose national banks. The charter allows fintech firms that provide similar services as those offered by traditional banks—such as taking deposits, paying checks or making loans—to enjoy the same benefits as traditional financial institutions that have the OCC charter. This means that fintech companies engaging in money services business, for instance, can apply for the OCC charter and operate in states without needing state licenses. Companies seeking the charter will be evaluated based on their reasonable chance of success, appropriate risk management, effective consumer protection, and strong capital and liquidity. The OCC has recently concluded its commenting period and received support from industry participants and opposition from state regulators. The OCC

also established a stand-alone Office of Innovation to serve as a clearinghouse for innovation-related matters and a central point of contact for OCC staff, banks, and nonbanks.[11]

In the second instance, New York Department of Financial Services (DFS) in August 2014 enacted a new regulation—23 NYCRR Part 200 Virtual currencies—governing companies conducting businesses related to virtual currencies in New York or involving a New York resident. (See more details about BitLicense in the box below.) As of January 2017, out of the initial 22 applicants, three companies have received the license (Circle, Ripple, and CoinBase). Although several companies have also exited the New York State as the cost to obtain the license proved too prohibitive, many experts still believe that BitLicense represents an appropriate first step by policymakers to embrace blockchain and virtual currencies.

Essentially, this policy alternative allows financial regulators to create a "derivative framework" based on existing regulations. In both cases, the regulators modify the existing regulatory framework to control fintech companies in a more proactive fashion. It allows the regulators to leverage their expertise to manage the new technology. On the other hand, while convenient, this approach may still be suboptimal. For instance, the OCC's fintech license may prove too costly for companies wishing to engage in micro-transactions using digital currencies. In any case, industry participants generally welcome more clarity from the regulators in both instances. They also prefer having a "choice" (OCC's approach) rather than facing a "requirement" (DFS's approach) and also favor a federal framework rather than a state-level solution. Nevertheless, most experts recognize that the outcomes will ultimately depend on actual implementations.

New York State's "BitLicense" and Industry's Reaction

On June 24, 2015, the New York Department of Financial Services (DFS) published the final rules for virtual currency business activity—23 NYCRR Part 200 Virtual Currencies—commonly known as "BitLicense". BitLicense is the first comprehensive virtual currency regulatory regime proposed and enacted in the United States, and it governs businesses engaging in "virtual currency business activity" defined as any one of the following activities involving New York or a New York Resident:

- Virtual currency transmission
- Storing, holding, or maintaining custody or control of virtual currency on behalf of others
- Buying and selling virtual currency as a customer business
- Performing exchange services as a customer business
- Controlling, administering, or issuing a virtual currency.

A business that engages in these activities must apply for a license and satisfy certain requirements, including maintenance of required capital, AML/KYC compliance, annual reports to DFS, disclosure of risks/terms/conditions to consumers, among others (see Exhibit 18 for more details).

[11] Office of the Comptroller of the Currency (OCC), *OCC Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies*, March 2017.

New York State's "BitLicense" and Industry's Reactions

Some of these conditions overlap with FinCEN's requirements, and a business that has obtained a BitLicense will still need to comply with federal, other states' and other countries' virtual currency laws. In addition, some businesses may require a BitLicense even when MSB registration with FinCEN is not needed—for example, a company that holds virtual currency for others. On the other hand, BitLicense relaxes some of FinCEN's requirements; for instance, companies are required to obtain information for counterparties to comply with AML/KYC requirements only to the extent practicable, and some companies are also allowed 2-year conditional licenses for with more tailored requirements.

Exhibit 18: BitLicense Requirements

Topic	Requirements
Covered Activities	• Most business activities, excluding mere merchant/consumer/investor activities; software developers, miners • Involving centralized or decentralized virtual currencies (excluding in-game / rewards points / prepaid cards) • Involving New York or New York customers
Cyber Security Program	• Board-approved cyber security policy & program to protect electronic systems and sensitive data • Qualified Chief Information Security Officer • Annual reports to NYDFS • Annual penetration testing/audits • Maintain business continuity and disaster recovery plan, to be independently tested annually
Consumer Protections	• Initial and per-transaction disclosures of risks, terms and conditions • Complaint policies & disclosures • Advertising and marketing requirements (e.g., no false, misleading or deceptive representations or omissions)
BitLicense Application / Revocation	• Must submit detailed applications to NYDFS & become licensed before undertaking covered activities • Existing businesses will have transition period to apply; if denied, must cease activities • NYDFS has broad discretion to approve/deny, revoke/suspend licenses • Material change of activities or change of control requires application to NYDFS (can ask NYDFS if proposed change is material or if person would gain control from proposed transaction)
On-Ramp	• Startups and new businesses may receive a 2-year conditional license with more tailored requirements and examinations • Numerous factors will be taken into account when determining whether to grant a conditional license
Safeguarding Assets	• Licensed entity must hold required capital in the form of cash, virtual currency, or high-quality, highly liquid, investment-grade assets • Surety bond / trust account at NYDFS's discretion • Full reserves for custodial assets — selling / encumbering prohibited • Books and records requirements (seven years) • Capital requirements at NYDFS's discretion
Exams, Reports, and Oversight / Anti-Money Laundering	• Largely consistent with federal AML requirements • Initial & annual risk assessments to inform AML program. Board-approved policy • Records of all transactions for seven years. • Office of Foreign Assets Control ("OFAC") compliance • Report within 24 hours to NYDFS ? $10,000 virtual currency to virtual currency one-day transactions by one person (unless fed reporting) • Suspicious Activity Reports ("SARs") required (unless fed reporting) • Customer Identification Program • Annual internal / external audit. No structuring to evade reporting, or obfuscating identity

Source: Davis Polk, *New York's Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal*, June 5, 2015.

New York State's "BitLicense" and Industry's Reaction (Continued)

Industry responses to BitLicense have been mixed. Some argue that BitLicense will create barriers to entry and impose costs on companies, as evidenced by the fact that many companies had exited the New York State after BitLicense came into effect. Others also question the need for BitLicense requirements considering that "virtual currency business activities … already fit within the New York [Money Transmitter statues]". On the other hand, many suggest that that BitLicense will promote investment in the industry and consumer trust, and that BitLicense-regulated companies will find it easier to establish banking relationships. In any case, BitLicense represents an example of efforts by regulators to embrace the new technology, as reflected in DFS Superintendent Maria Vullo's statement below:

> *"New York is committed to fostering and encouraging the long-term growth of new industries throughout the state while enforcing all necessary safeguards to protect our markets and consumers." (January 17, 2017)*

V.3. Issuance of Regulatory Guideline

Because some regulations are ambiguous when applied to blockchain-based businesses, regulatory agencies may choose to provide preliminary perspectives on how they plan to regulate the new technology. This may come in the form of a statement specifying how the regulators plan to manage blockchain applications, how active or passive the regulators will engage with industry players, how strict or flexible the rules will be, what the key priorities are, and how the regulators plan to use the technology themselves. Such a guideline will provide industry participants with added clarity, while offering them flexibility and autonomy for self-regulation.

The often-cited example of this approach is President Bill Clinton's declaration of "do no harm" approach to internet commerce regulation (see box on the next page). Following the recommendation from a President's task force, the president in July 1997 announced his intention to make the internet a "global free-trade zone." The framework called for a hands-off approach to regulating business transactions on the internet. It encompassed 13 specific objectives, such as international agreement to make the internet a global tariff-free trade zone, federal procurement of items online, and the development of industry codes of conduct and technology tools to protect privacy online.[12] The framework has been hailed by many as helping secure the leadership position in internet commerce for the United States.

Aiming to provide additional clarity to industry participants, a regulatory guideline embraces a "**principle-based**" approach to regulation in which regulators manage the actions of industry participants pursuant to a set of principles. This is in contrast to a "**rule-based**" approach in which regulators follow specific rules set forth in the agencies' statutes. While the rule-based approach is more precise, the principle-based approach allows for more flexibility for the regulators to interpret the legislation and enforcing the law. This presumably will enable the regulators to respond more quickly to any potential challenges that may emerge from the technology. On the other hand, a principle-based approach also requires more

[12] "Clinton Issues 'Hands Off' Policy on Internet Commerce," New York Times, July 2, 1997.

engagement by the regulators to interpret the laws on a case-by-case basis which may prove too demanding, particularly in a large market such as the United States.

President Clinton's "Hands Off" Policy on Internet Commerce

At the dawn of internet commerce in the late 1990s, U.S. regulators sought to ensure that technology companies build a secured online marketplace for American consumers. Some of the key issues under consideration for the regulators were consumers' privacy, protection of patents and copyrights, taxes, and other protection for consumers. Recognizing that existing regulatory framework might have been inept to manage the emergence of the new technology and that a comprehensive regulatory reform might have also been too politically challenging to pursue, President Bill Clinton—under the guidance of a taskforce led by his chief policy advisor Ira Magaziner—declared a guideline on how the administration planned to regulate the emerging industry. Proclaiming that the Internet "should be a place where government makes every effort … not to stand in the way, to do no harm," the guideline embraced a "hands off" paradigm which encompassed a few key principles, including:

- *Avoid undue restriction:* "Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention."

- *Pursue a light-touch approach:* "Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce."

- *Recognize the unique qualities of the internet:* "Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the need of the new electronic age."

- *Pursue a global approach:* "The legal framework supporting commercial transactions should be consistent and predictable regardless of the jurisdiction in which a particular buyer and seller reside."

President Clinton's declaration essentially welcomed industry self-regulation, which stood in contrast to other countries' approaches, such as the "comprehensive legal framework" preferred by Germany. The United States' approach was subsequently embraced by the European Union, and a similar set of principles was later announced in the Bonn Declaration. Despite some criticisms at the time, President Clinton's framework has often been credited by industry experts for helping secure the leadership position for the United States in the development of internet commerce.

Source: "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," *Forbes*, February 12, 2012. (https://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/#2ad95ecb7170) and "Clinton Issues 'Hands Off' Policy on Internet Commerce," New York Times, July 2, 1997. (https://partners.nytimes.com/library/cyber/week/070297commerce.html)

As with other policy alternatives, the effectiveness of this policy approach depends on execution. An encompassing statement by the president on the one-hand would create coherence across multiple regulatory agencies, but it may also prove too broad for actual implementation and ultimately fail to provide additional clarity to industry participants. On the other hand, specific guidance by each regulatory agency would be easier for industry players to follow, but it may also lack consistency across agencies and therefore fail to address interagency issues.

Furthermore, this policy alternative presumes that the regulators have sufficient understanding of the technology to devise an appropriate guideline. It also indicates a one-sided interaction, whereby the regulators guide industry players how to behave with limited inputs from the industry itself. It often also implies reduced engagement by the regulators, which may, or may not, be the direction that the United States wishes to pursue. Finally, it may not solve some complexities within the existing regulatory framework, such as state-federal intricacy.

V.4. Creation of Multi-Party Working Group

A multi-party working group represents an effort by regulatory agencies and industry participants to collaborate and arrive at a standard framework or shared best practices for technology development and regulation. Under this approach, various regulatory agencies would work together to formulate and issue a single policy framework for the industry. They may also collaborate with industry participants to learn from their experiences and take their feedbacks to adjust their policies accordingly. A multi-party working group essentially aims to solve a coordination problem across agencies to come up with a coherent regulatory solution for the blockchain industry.

An example of a multi-party working group is the **Federal Financial Institutions Examination Council (FFIEC)**. Established on March 10, 1979, the council is a formal interagency body empowered "to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions."[13] Members of the council include the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). FFIEC is also responsible for developing uniform reporting systems for federally supervised financial institutions and their holding companies and subsidiaries and for making recommendations to promote uniformity in the supervision of financial institutions.

To understand how a multi-party working group such as the FFIEC may help regulators, one may observe the council's **Cybersecurity Awareness** effort in which the council members pursued a number of initiatives "to raise the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats."[14] With this effort, the FFIEC created the Cybersecurity and Critical Infrastructure Working Group in June 2013 "to enhance communication among the FFIEC member agencies and build on existing efforts to strengthen the activities of other interagency and private sector groups."[15] The council also work to enhance the industry preparedness to deal with potential cybersecurity issues.

[13] FFIEC website About Us (http://www.ffiec.gov/about.htm)
[14] FFIEC website, Cybersecurity Awareness (http://www.ffiec.gov/cybersecurity.htm)
[15] Ibid.

The FFIEC and its Cybersecurity Awareness represent only one example of how regulatory agencies may create a multi-party working group to handle issues related to emerging technologies. In this example, the council serves as a coordinating body to standardize monitoring and reporting processes of depository institutions. In the case of blockchain, a multi-party working group may include various regulatory agencies, ranging from FinCEN, SEC, CFTC, CFPB, FINRA, and the Federal Reserves, which would work together to promote effective interaction with financial institutions and technology companies. The working group may also pursue other initiatives besides standardizing reporting procedure, such as issuing a common regulatory framework for dealing with blockchain-related issues, serving as a point of contact for industry participants, or serving as a representative in negotiating with regulatory bodies of other countries or international agencies.

While the creation of a multi-party working group may help solve coordination issues and promote uniform engagement with the industry, it may add additional layers of bureaucracy, leading to organizational inefficiencies. Depending on how the working group is form and what authority it has, it may also lack the power to decide on cross-agency issues or to correspond with foreign counterparties. Furthermore, an effective working group requires constant interaction among its members to allow for idea sharing, which may prove challenging in an environment where different regulatory agencies have historically been operating autonomously. Finally, the ability of various regulatory agencies to collaborate will also depend on the extent to which their interests and objectives are unifiable (as in the case of the FFIEC). This will also have implication on the long-term viability of the working group itself.

Industry Advocacy on Blockchain and Digital Currency

Despite limited collaboration among U.S. financial regulators so far, industry participants have been collaborating to promote the understanding and the adoption of blockchain. In the United States, such efforts come in the form of trade associations and research and advocacy organizations, such as the Chamber of Digital Commerce and Coin Center.

The Chamber of Digital Commerce (digitalchamber.org) is a trade association representing the digital asset and blockchain industry. With membership including several key industry players, ranging from technology companies, venture capital firms, to financial institutions, the association has a mission of promoting the acceptance and use of digital assets and blockchain-based technologies through education, advocacy and working closely with policymakers, regulatory agencies and industry.

Coin Center (coincenter.org) is a non-profit organization focusing on research and advocacy of policy issues related to cryptocurrency and decentralized computing technologies like Bitcoin and Ethereum. The organization publishes research from academics and experts and educates policymakers on important issues related to blockchain. The organization is funded by several blockchain and distributed ledger technology providers and investors.

Besides working with their members and sponsors, these organizations have also formed **Blockchain Alliance** (blockchainalliance.org), a public-private forum created to promote better understanding of blockchain technology. The alliance aims to promote open dialogue between industry and regulatory agencies to enable better enforcement and prevent criminal activities.

Industry Advocacy on Blockchain and Digital Currency (Continued)

Outside the United States, there are also similar efforts by industry participants to promote the technology. For instance, in Japan, the **Blockchain Collaborative Consortium (BCCC)** (bccc.global) was formed in 2016 to promote the spread of blockchain in the country. As of March 2017, the consortium comprises 109 members, ranging from technology companies to financial institutions. The consortium plans to host seminars and educational programs for the media and the public going forward.

Based on the aforementioned examples, regulators should continue to engage with these organizations while at the same time consider forming their own regulatory working group to enhance their understanding of various regulatory issues and share best practices.

V.5. Establishment of Regulatory Sandbox

A popular approach that several foreign regulators have adopted to manage the emergence of blockchain is the establishment of regulatory sandbox. Several countries—such as the United Kingdom, Singapore, Australia, Hong Kong, France, and Canada—have established regulatory sandboxes to promote innovation while protecting consumers and preventing risks to the financial system.

One often-cited example is the FCA's sandbox in the United Kingdom (see box on the next page). Established as a part of Project Innovate—an initiative stated in October 2014 to encourage innovation in the interests of consumers and to promote competition through disruptive originality—the FCA's sandbox provides "a 'safe space' in which businesses can test innovative products, services, business models and delivery mechanisms while ensuring that consumers are appropriately protected."[16] Essentially, it creates a well-defined space in which companies can experiment with new technology and business models in a relaxed regulatory environment and in some cases with support of the regulators for a period of time. This leads to several potential benefits, including: reduced time-to-market of new technology, reduced cost, better access to financing for companies, and more innovative products reaching the market. The first cohort of the FCA's regulatory sandbox closed to applications on July 8, 2016, in which it received applications from 69 firms, and 24 were accepted into the sandbox to develop products toward testing.[17]

Besides the United Kingdom, other countries such as Singapore, Malaysia, Australia, and Hong Kong have also launched similar initiatives, albeit with different implementations and details. For instance, while the FCA only issued a guidance on an appropriate timeframe for a firm to be in the sandbox, Malaysia imposes a maximum limit. Furthermore, Singapore and Malaysia also require applicants to show that they intend to deploy their products in the respective countries upon exit from the sandboxes. Also, while Australia proposes a conditional, industry-wide exemption for new businesses to test certain financial services for six months without holding an Australian Financial Services ('AFS') license, the Hong Kong sandbox is open

[16] Financial Conduct Authority, *Regulatory Sandbox*, November 2015.
[17] Financial Conduct Authority, "Financial Conduct Authority unveils successful sandbox firms on the second anniversary of Project Innovate," July 11, 2016. (https://www.fca.org.uk/news/press-releases/financial-conduct-authority-unveils-successful-sandbox-firms-second-anniversary)

only to institutions authorized under the Banking Ordinance and under the supervision of the Hong Kong Monetary Authority, which include mainly banks and depository institutions.

Compared to other alternatives, regulatory sandbox is popular for a couple of reasons. First, a sandbox allows for deeper engagement between regulators and industry participants, enabling the regulators to gain more insights into the technology and its adoption trends. For example, in the case of the United Kingdom, industry participants must submit plans of how they will test their technology, the results of the tests, and potential implementations of the solutions. Second, sandbox allows regulators to strike a balance between promoting innovation and preventing harms to consumers and the financial system. A "controlled environment" approach reduces the cost of compliance for companies wanting to experiment on new ideas and also limits potential damages if they occur. Finally, a sandbox creates a streamline process for testing innovation and ideas, providing clarity to both industry participants and regulators on how the technology will be developed and deployed.

On the other hand, a regulatory sandbox also carry some disadvantages. First, a regulatory sandbox is difficult to implement. Regulators must create a detailed process that specify the criteria with which companies will be evaluated, the process to monitor these companies' progresses, and the criteria to approve a full-scale roll-out. Furthermore, since the United States has several financial regulatory, coupled with the state-federal intricacy, a regulatory sandbox may prove even more challenging to implement.

Second, given the complexity in setting up and operating a regulatory sandbox, this alternative may be difficult to scale. Since each company must be admitted to the sandbox and their business plans must be evaluated individually, the process could require significant manpower. Lastly, although a regulatory sandbox provides a safe pathway for companies wishing to roll out their solutions to the broader market, there is no guarantee that such solutions would still be able to operate safely in the real world. It is possible that other risks to consumers or to the financial system may emerge once the products are rolled out in a wider scale.

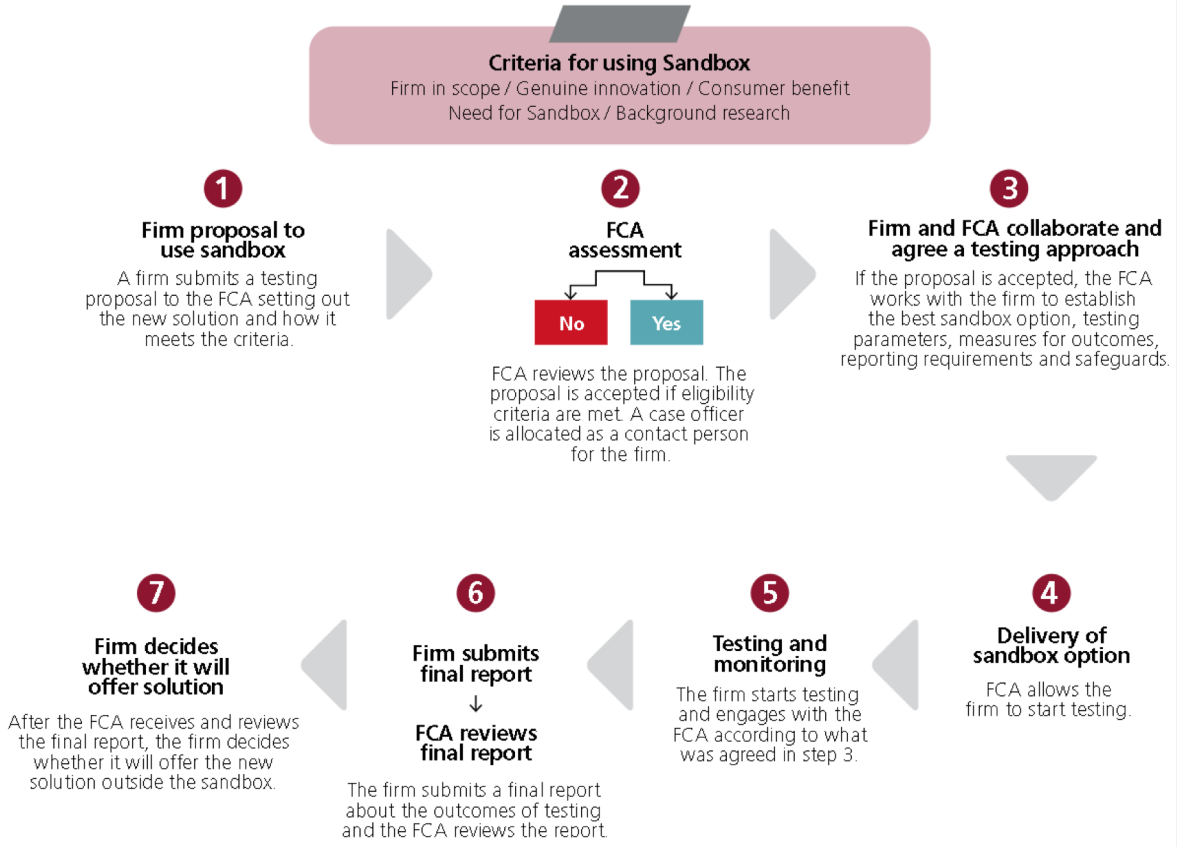
Note that in the United States, a derivative of regulatory sandbox is the safe harbor concept. A **safe harbor** provides exemptions, deeming certain conduct not to violate a given rule. A notable example is the Digital Millennium Copyright Act (DMCA), which has safe-harbor provisions protecting Internet service providers from the consequences of their users' actions. For instance, content owner cannot sue YouTube if an infringer posts pirated content on YouTube's website as long as YouTube has "adopted and reasonably implemented a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[18] While a safe harbor provides regulatory leniency, allowing companies to pursue certain business ideas without massive costs or fear of repercussions, it also involves limited interaction between regulators and industry participants, reducing the levels of learning for the regulators in the process. It also presumes that the regulators know the risks that would be carved out by the safe harbor in advance and therefore is not equipped to accommodate other potential risks.

[18] 17 U.S. Code § 512 - Limitations on liability relating to material online.

How the U.K.'s Regulatory Sandbox Works

Started in October 2014, the FCA's regulatory sandbox was the first of its kind to establish a safe space for companies to test their innovation. The FCA's sandbox focuses on addressing two main challenges: (1) how to lower barriers to technological testing within the existing regulatory framework, and (2) how to ensure that risks from testing novel solutions are not transferred from firms to consumers. To achieve these goals, the sandbox works as follows.

Exhibit 19: How the FCA's Regulatory Sandbox works



Source: Financial Conduct Authority, *Regulatory Sandbox*, November 2015.

The FCA, working together with the Prudential Regulation Authority (PRA), first introduced the criteria for firms wishing to join the sandbox. Similar to the criteria for requesting support from the FCA's Innovation Office, the criteria ask whether a firm (1) provides solutions for the financial services industry, (2) delivers genuine innovation, (3) offers consumer benefits, (4) has a need for the sandbox, and (5) has completed sufficient background research. Companies that apply and satisfy the aforementioned criteria based on the FCA's assessment then may join the sandbox.

Next, the firm and the FCA collaborate and agree on a testing approach, and the firm begins its testing process. Upon completion of the testing (with monitoring by and engagement with the FCA), the firm must submit an outcome report to the FCA. If the firm wishes to pursue a further roll out

How the U.K.’s Regulatory Sandbox Works (Continued)

of the product outside the sandbox, it needs to provide an additional report on the roll out process and must remain compliant with the existing regulations outside the sandbox. Different thresholds for testing ideas and for a full roll-out allow firms to reduce their costs of experiment, while recognizing the potential for wider use of the product.

VI. Solving for the Best Solution

The policy alternatives discussed in Section V should be evaluated based on specific criteria. This report proposes three criteria: (1) effectiveness (will the alternative help policymakers achieve the objectives set forth in section IV.3), (2) efficiency (will the alternative achieve these objectives in an efficient manner), and (3) feasibility (can the policy be implemented in the current regulatory regime and political environment). These criteria will help ensure that the chosen policy will allow policymakers achieve their goals in the most practical and effective manner.

VI.1. Choosing the Right Criteria

VI.1.A. Effectiveness

The policy alternatives should be evaluated based on whether they enable the federal government to achieve the objectives discussed in Section IV.3. Specifically, an effective solution should (1) engage policymakers in discussions on blockchain with industry participants in a unified and effective manner, (2) allow policymakers to ensure regulatory compliance and maintain stability of the financial system, and (3) promote technological innovation in the blockchain and DLT space.

VI.1.B. Efficiency

The policy alternatives should allow policymakers to achieve their policy objectives in an efficient manner. Specifically, the best alternative should be cost efficient, easy to implement and scale, and flexible to address unanticipated challenges. In a nutshell, an efficient policy should promote innovation without compromising consumer protection and the stability of the financial system.

VI.1.C. Feasibility

Finally, the policy alternatives should be feasible within the context of the current regulatory framework and political environment. Specifically, a feasible policy can be implemented in an environment with multiple regulatory agencies as well as with state-federal complexity. One must also consider feasibility in terms of policy design, execution, and viability.

VI.2. Comparing Alternatives

The table on the next page analyzes the five policy alternatives based on the criteria mentioned above. Although policy effectiveness, efficiency, and feasibility will ultimately depend on actual policy designs and implementations, the table below provides a preliminary analysis of the trade-offs of these alternatives.

As the table illustrates, each policy alternative has different advantages and disadvantages. For instance, while status quo is clearly the easiest to implement, it fails to solve many policy problems arising from the existing regulatory framework. On the other hand, although a regulatory sandbox will be the most effective in promoting innovation while protecting consumers, it will also be the most difficult to implement and the costliest to scale.

Alternatives	Evaluation Criteria		
	Effectiveness	**Efficiency**	**Feasibility**
1. Status Quo: Continue to regulate blockchain technology and digital currencies under the existing regulatory framework	+ So far has proven effective in promoting innovation and limiting harms to consumers and the financial system — Offer limited clairty to industry players on how regulations will be applied to blockchain technology and virtual currencies, which could lead to high compliance costs and hence stifle innovation — Difficult for regulators to anticipate potential challenges arising from the new technology; potential risks in the financial system remain	— Existing regulaory framework is cumbersome in providing effective regulations	+ Easy to implement (nothing to do)
2. Modified Status Quo: Create additional legislation to deal specifically with the application of the technology	+ The supplemental law presumably will be better equipped to manage the new technology + The law will provide additional details on how the regulators will regulate the new technology, giving more clarity to industry participants — Depending on how the supplemental law is drafted, it may impose significant compliance costs on the industry	— New laws may add more complexity to the already complicated regulatory framework — Presupposes sufficient knowledge amont regulators and legislators to enact an ffective new regulations	— A federal approach, while will be the most effective in addressing existing regulatory complexity, will be the most difficult to implement, given resistence from states
3. Issuance of a Regulatory Framework: Issue a regulatory framework to provide a guideline on how the regulators plan to regulate the technology	+ The issued statement will provide additional clarity on how the regulators will regulate the new technology, which could reduce the cost of compliance to — One-way communication which offers limited opportunity for interaction between regulators and industry players	+ Relatively inexpensive to implement (primarily only requires the president or the heads of regulatory agencies to announce the framework) — Presupposes sufficient knowledge amont regulators and legislators to issue a coherent framework	+ Issuance of statement should face minimal resistance — Compliance could be difficult to enforce
4. Creation of a Multi-Party Working Group Create a working group to coordinate across regulatory agencies and to serve as a central point of contact with industry players	+ Mitigate cross-agency coordination issues, resulting in a more coherent regulatory framework	— Create additional layers of bureaucracy	— Depending on how the taskforce is created and what authority it has, the taskforce could lack the necessary power to act or make decision
5. Establishment of a Regulatory Sandbox Establish a "safe space" for companies to experiment new ideas and interact with regulators	+ Increase engagement between regulators and industry participants + Allows regulators to have more exposure to the technology and better understanding of its use cases + The scope of the sandbox can limit harms to consumers and to the financial system + Encourage innovations, particularly within the safe space of the sandbox	— Could be costly and difficult to scale	— Difficult to implement, particularly given the current complex regulatory structure in the United States

VI.3. Adopting a Multi-Pronged Approach

Given the trade-offs between these alternatives and the fact that these alternatives are not mutually exclusive, the best solution will likely be a combination of some or all of the above approaches. Specifically, this report recommends a three-prong approach, including:

- *Issuance of Regulatory Guideline:* Financial regulators should provide a general guideline of how they plan to regulate blockchain-based applications. Such guideline should include details such as: key priorities from the regulators' perspectives (such as consumer protection and overall financial stability), the nature of engagement between the regulators and industry players (such as how active the regulators plan to monitor companies' activities and how much leeway the industry will have for self-regulation), how the regulators plan to address potential issues that may arise (such as those arising from the incompatibility between the new business models and the existing regulations), and how industry players may correspond with the regulators to avoid noncompliance. To the extent that such an indication could come from the President, it would also provide consistency in the framework across agencies.

- *Creation of Public-Private Working Group:* The regulators should establish a public-private working group that would allow various financial regulatory agencies and industry players to interact, share insights and best practices, and brainstorm ideas to promote innovation and effective regulation. Participants in the working group will include representatives from various financial regulatory agencies as well as industry players. The working group will aim to promote knowledge sharing, while the actual authority will remain with each regulatory agency. It will also serve as a central point of contact when interacting with foreign and international agencies. Note that although similar working groups, such as the Blockchain Alliance, exist currently, they are typically spearheaded by the industry and geared toward promoting industry's preferences. The regulators should instead create their own platform that would allow them to learn about the technology, discuss emerging risks and potential options, and explore potential policy options in an unbiased fashion.

- *Enactment of Suitable Safe Harbor:* Although blockchain may expose consumers and the financial system to some risks, regulators may not need to regulate every minute aspect of these new use-cases, particularly if the risks are small. Hence, under certain conditions, the regulators may consider creating safe harbor that would allow industry players to experiment with their ideas without being overly concerned with the regulatory burden while also limiting the risks to consumers and the financial system. For instance, with respect to money transfer applications, FinCEN may consider creating safe harbor for transactions below a certain amount.

This recommendation essentially aims to promote a prudent and flexible market-based solution. The recommendation affords industry players the freedom to operate within the existing regulatory environment, while also giving them greater clarity on the applicability of the regulations and enabling productive interaction with the regulators. It also allows the regulators to protect consumers and the financial system without stifling innovation. Lastly, this solution is viable within the existing political context and despite the complex regulatory regime that exists currently. Note that ultimately, policymakers should also seek comprehensive reform of the existing regulatory structure in order to reduce cross-jurisdictional complexity and promote innovation and efficiency.

VII. What Should Policymakers Do Now?

Blockchain is a revolutionary technology that hold promises to disrupt the financial industry. Although the technology holds promises to improve the financial system—such as by increasing transaction efficiency, reducing cost, and enhancing security—the transition from the current financial infrastructure to the blockchain-enabled world introduces potential risks to both consumers and the financial system. At the same time, it also represents an opportunity for the United States to strengthen its leadership positions, in both technology and financial arenas. U.S. policymakers and regulators therefore have the responsibility to ensure that this transition occurs smoothly, and that the country remains both an innovation hub and a financial center. To achieve this goal, this report suggests the following actions and priorities for both the regulators and the legislators.

For Regulators:

- For the regulators, the most important near-term goal is to become educated about the technology and its consequences. Each regulatory agency should appoint key persons to serve as experts on the technology, who would understand the trends and potential policy issues and to help ensure that the agency remain effective to ensuring compliance and protecting consumers and the financial system.
- In regards to compliance, the regulators should focus their attention on the adoption of technology by financial institutions, particularly in the area of money transfer, clearing and settlement of assets, and trade finance. The regulators should also be vigilant of new use-cases that are emerging, especially those with direct-to-consumer applications.
- Lastly, the regulators should actively engage with other actors, including industry players, other regulatory agencies, and foreign and international entities, in order to be informed about the technology and emerging trends, to share insights and best practices, and to work together to ensure compliance and consumer safety.

For Legislators:

- Similar to the regulators, the legislators should also strive to be informed about the technology and its implications. The legislators should also caution against issuing more regulations too soon, as doing so will likely stifle innovation and perhaps even bring more risks to the financial system (for instance, with companies front-running new regulations, or actors trying to conduct their activities outside the purview of the regulators).
- In the medium-term, Congress should also seek ways to promote collaboration among regulatory agencies and establish partnerships with international regulators. This would allow for better knowledge sharing and more effective regulation. After all, blockchain operates across jurisdictional boundaries, and regulatory cooperation is therefore highly important.
- Finally, Congress should consider ways to reform the existing financial regulatory framework, both in terms of consolidating regulatory agencies, resolving state-federal redundancies, and simplifying existing regulations. Ultimately, this will provide a long-term solution that will help ensure system stability and keep the United States in the leading positions in innovation and finance.

With blockchain technology gaining momentum globally, the United States has the opportunities to capitalize on this shift in the technology and financial industry landscape. It is crucial for regulators, policymakers, and industry players to continue working together to utilize this technology and to ensure consumer safety and stability of the financial system.

Bibliography

BBVA. (2016) *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*, December.

Bitfury. (2016) "Digital Assets on Public Blockchains," March 15.

Vallabhaneni, Pratin, Fauvre, David, Shipe, Andrew. (2016) "Overcoming Obstacles to Banking Virtual Currency Businesses," *Coin Center Report*, May.

Coindesk. (2017) "A (Short) Guide to Blockchain Consensus Protocols," March 4.

Davis Polk. (2015) *New York's Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal*, June 5.

Ernst & Young. (2016) *UK FinTech on the cutting edge: An evaluation of the International FinTech sector*, December.

ESMA. (2017) *The Distributed Ledger Technology Applied to Securities Markets*, February 7.

Federal Reserve Board. (2016) "Distributed ledger technology in payments, clearing, and settlement," Finance and Economics Discussion Series.

FINRA. (2017) *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*, January.

Giancarlo, J. Christopher. (2017) "Keynote Address of CFTC Commissioner J. Christopher Giancarlo before SEFCON VII," January 18.

Goldman Sachs. (2016) *Profiles in Innovation: Blockchain — Putting Theory into Practice*, May.

Government Office for Science. (2015) *Distributed Ledger Technology: beyond block chain*, December.

IBM. (2016) *Leading the pack in blockchain banking: Trailblazers set the pace*, September.

Nakamoto, Satoshi. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System."

Oliver Wyman. (2016) *Blockchain in Capital Markets: The Prize and the Journey*, February.

UBS. (2016) *Building the trust engine: How the blockchain could transform finance (and the world)*.

Underwood, Sarah. (2016) "Blockchain Beyond Bitcoin," *Communications of the ACM*, 59:11, November.

Vantiv. (2017) *Riding the Blockchain Train, Together*, January.

Walch, Angela. (2017) "The Path of the Blockchain Lexicon (and the Law)" Review of Banking & Financial Law, 36, March 24.

World Economic Forum, *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services*, August 2016.

Appendix A: List of Companies in the Blockchain/DLT Space

#	Company Name	Industry	Location	Funding ($mm)	Description	Products
1	Backfeed	Tech	Israel	???	Developer of opensource infrastructure for decentralized organization	• Blockchain Platform
2	Bitcoin News	News	US	--	News on bitcoin	• News
3	Bitfoo	Exchange	China	???	Hong Kong-based bitcoin trading company	• Bitcoin Exchange
4	BitPagos	Financial	US (CA)	$2	Provider of digital wallet and online payment solutions	• Payment
5	Bitpay	Financial	US (GA)	$30	Bitcoin payment solution	• Payment
6	Blockstack	Tech	US (NY)	5.45	Blockstack is a new decentralized internet where users own their data and apps run on their devices. Get a Blockstack identity today.	• Blockchain Identity
7	Bitcoin Magazine	News	US (TN)	--	News on bitcoin and blockchain	• News
8	BitFurry	Tech	Netherlands	$60	BitFurry develops and delivers both the software and the hardware solutions necessary for businesses, governments, organizations and individuals to securely move an asset across the Blockchain.	• Bitcoin mining
9	Blockstream	Tech	CAN	$76	Blockstream is the leading provider of blockchain technologies, on the forefront of work in cryptography and distributed systems.	• Blockchain Middleware
10	Chain	Tech	US (CA)	$40	Chain partners with leading organizations around the world to build, deploy, and operate blockchain networks that enable breakthrough financial products and services.	• Blockchain Middleware
11	CoinDesk	News	US (NY)	--	CoinDesk is the world leader in news and information on digital currencies such as bitcoin, and its underlying technology – the blockchain.	• News
12	ConsenSys	Tech	CAN	???	The ConsenSys "hub" coordinates, incubates, accelerates and spawns "spoke" ventures through development, resource sharing, acquisitions, investments and the formation of joint ventures.	• Incubator
13	Digital Asset Holding	Startup	US (NY)	$60	Digital Asset builds distributed, encrypted straight through processing tools.	• Blockchain Middleware
14	Digital Currency Group	Investment	US (NY)	--	DCG makes investment in Blockchain companies.	• Incubator
15	Ethereum	Organization	US/ Switzerland	$15	Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.	• Smart Contract Platform
16	Guardtime	Tech	Estonia/ Japan	$8	Provider of blockchain-based products and services to enterprises and governments including Ericsson AB and the country of Estonia	• Cryptographic Middleware
17	Hyperledger	Organization	US	--	The Hyperledger project is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology.	• Blockchain Platform
18	Nasdaq	Financial	US (NY)	Public	Nasdaq OMX is partnering with infrastructure provider Chain to use blockchain to issue and transfer the shares of privately held companies.	• Distributed Ledger
19	PeerNova	Tech	US (CA)	$9	PeerNova has developed a technology platform that provides immutability and data integrity for use in financial services applications, such as compliance and audit.	• Blockchain Middleware

#	Company Name	Industry	Location	Funding ($mm)	Description	Products
20	R3 CEV	Financial	US (NY)	$200	R3 is a financial innovation firm that leads a consortium partnership with over 75 of the world's leading financial institutions to to design and deliver advanced distributed ledger technologies to the global financial markets.	• Distributed Ledger Consortium • Smart Contract
21	Ripple	Financial	US (CA)	$93	Provider of financial settlement solutions . Ripple Labs has built a distributed trustless exchange system around a consensus ledger as opposed to a blockchain, although there are several similarities.	• Real-time Payment
22	SETL	Tech	UK	$40	SETL provides real-time blockchain settlement and scalable payments solutions	• Blockchain Middleware
23	Symbiont	Financial	US (NY)	$7	Symbiont is bridging the gap between the emerging blockchain ecosystem and Wall Street, with the first issuance and trading platform for Smart Securities.	• Distributed Ledger Consortium • Smart Contract
24	Abra	Financial	US (CA)	$12	Abra is the world's first digital cash peer-to-peer network. Users can send or receive money or pay for things instantly, privately, and securely with or without a bank account. Abra Tellers represent a global, shared network of people facilitating the movement of money.	• Payment
25	AlphaPoint	Tech	US (NY)	$1	A financial technology company that powers digital asset networks and provides institutions a Distributed Ledger Platform to digitize, trade, and manage any asset	• Distributed Ledger Consortium
26	BlockCypher	Tech	US	$3	Infrastructure fabric for blockchain applications	• Blockchain Middleware
27	Bloq	Tech	US	???	Bloq delivers enterprise grade blockchain technology to leading companies worldwide.	• Blockchain Middleware
28	Coinbase	Exchange	US (CA)	117.21	Bitcoin and ethereum exchange	• Bitcoin Exchange
29	Coinmetrics	News	--	--	Provider of institutional-level Bitcoin data & research	• News
30	Cointelegraph	News	UK	--	News on bitcoin and blockchain	• News
31	Earthport	Tech	UK	Public	Earthport is a regulated Financial Institution under the auspices of the UK's Financial Conduct Authority, transforming the future of cross-border payments.	• Payment network
32	Epiphyte	Tech	UK	???	Epiphyte provides a blockchain powered SaaS service that delivers instant settlement and DVP (delivery versus payment) for financial trades.	• Blockchain Platform
33	itBit	Exchange	US (NY)	25	Bitcoin trading exchange	• Bitcoin Exchange
34	Kraken	Exchange	US (CA)	6.5	A fully-compliant digital asset trading platform (bitcoin exchange) positioned for FX trading	• Bitcoin Exchange
35	KYC-Chain	Tech	HK	???	KYC-Chain is a novel platform built over the convenience and security of Distributed Ledger technology, allowing users to manage their digital identity securely, while businesses and financial institutions are able to manage customer data in a reliable and easy manner.	• KYC Platform
36	Microsoft	Tech	US (WA)	Public	Microsoft is providing Blockchain as a Service through Azure Cloud Services. It is also partnering with R3 to accelerate the use of the blockchain technologies.	• Blockchain as a Service
37	Monax	Tech	US	$1	Monax builds and maintains the market-leading, free, and open-source Universal Blockchain Platform known as Eris. Eris allows anyone to build their own secure, low-cost, run-anywhere applications using blockchain and smart contract technology.	• Blockchain Platform
38	Multichain	Tech	--	--	MultiChain helps organizations to rapidly build applications on blockchains and shared ledgers	• Blockchain Middleware
39	Noble Market	Financial	US	???	Noble is a non-fractional reserve bank that focuses solely on enabling clients to clear, net and settle FX & OTC transactions in real-time	• Prime Broker

#	Company Name	Industry	Location	Funding ($mm)	Description	Products
40	Norbloc	Tech	Sweden	???	norbloc enables intelligent KYC platforms	• KYC Platform
41	Openchain	Organization	--	???	Openchain is an open source distributed ledger technology. It is suited for organizations wishing to issue and manage digital assets in a robust, secure and scalable way.	• Blockchain Developer Network
42	Pymnts	News	--	--	News on payment and commerce	• News
43	Scorechain	Tech	Luxembourg	0.57	We offer solutions for Bitcoin regulation and compliance.	• Bitcoin Analytics
44	Serica	Healthcare	US (CA)	???	Peer-to-Peer Payment Innovation for Healthcare	• Payment
45	ShoCard	Financial	US (CA)	$2	ShoCard is a digital identity that protects consumer privacy and is as easy to use as showing a driver's license.	• Digital Identity
46	SkuChain	Commerce	US (CA)	???	Skuchain builds blockchain based products for B2B Trade and Supply Chain Finance.	• Blockchain Middleware
47	SmartContract	Tech	US (CA)	???	SmartContract provides a middleware to plugin your data API to the Ethereum network	• Smart Contract
48	Stellar	Financial	US (CA)	3.06	Stellar is a common financial platform, designed to be open and accessible to everyone.	• Payment / Banking
49	TradeBlock	Financial	US (NY)	$3	TradeBlock is the world's leading provider of institutional trading tools for digital currencies.	• Bitcoin Trading
50	Wave	Transport	Israel	$20	Wave has created a peer-to-peer and completely decentralized network that connects all carriers, banks, forwarders, traders and other parties of the international trading supply chain. Using decentralized technologies, all communication between these parties will be direct and will not pass through a specific central entity.	• Blockchain Platform

Source: Websites; compiled by the author.

Appendix B: List of Experts Participating in Interviews

No.	Name	Organization	Title	Date
1	Pratin Vallabhaneni	Arnold & Porter	Associate	03/04/17
2	Kevin Batteh	Delta Strategy Group	--	03/06/17
3	John Edge	Identity2020	Co-Chair	03/06/17
4	Angela Walch	St. Mary's University, School of Law	Associate Professor	03/06/17
5	David Andolfatto	Federal Reserve Bank of St. Louis	Vice President	03/07/17
6	Chris Khan	R3 CEV	Project Lead	03/07/17
7	Liza Partington	Ripple	Compliance Analyst	03/10/17
8	Ryan Zaone	Ripple	Director of Regulatory Relations	03/10/17
9	Jason Thomas	Thomson Reuters	Manager of Innovation, Government Segment	03/10/17
10	Alan Cohn	Blockchain Alliance Steptoe & Johnson LLP	Partner	03/13/17
11	Andrea B. Tinianow, Esq	State of Delaware	Director of Corporate and International Development	03/14/17
12	Nitin Gaur	IBM Blockchain Labs	Director	03/16/17
13	Peter Van Valkenburgh	Coincenter	Director of Research	03/17/17
14	Brian Behlendorf	Hyperledger	Executive Director	03/17/17
15	Greg Kidd	Ripple	Chief Risk Officer	03/20/17
16	Colin Hector Duane Pozza	FTC	Attorney Assistant Director Division of Financial Practices	03/21/17
17	Aaron Wright	Cardozo School of Law	Associate Clinical Professor of Law; Founder/Director, Tech Startup Clinic	03/27/17
18	Ronen Kirsh	Blockchain at Berkeley	Head of Consulting	04/14/17

Appendix C: Glossary

Blockchain	Distributed ledger technology that enables direct peer-to-peer transaction across a trustless network
Byzantine Fault Tolerant	Characteristic of a database system that tolerates manipulation of data by untrusted parties
Consensus mechanism	Process by which various network participants work together, sometimes in a competitive manner, to verify the integrity of the data
Cryptographic hash	Hash function which takes a data and returns a fixed-size alphanumeric string, called the "hash value"
Cryptography	Method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it
Cybersecurity Awareness	An initiative by the FFIEC to raise the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats
Delaware Blockchain Initiative	Project by the State of Delaware to streamline recordkeeping for private and public companies registered in the state
Digital Token	Token of value that one company may issue to another either as a medium of exchange or as compensation for services provided
Distributed Ledger Technology (DLT)	Database technology that stores data in a decentralized fashion
Federal Financial Institutions Examination Council (FFIEC)	A formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions; members of the council include the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB)
Immutability	Property by which existing data in the database cannot be modified
Merkle Tree	Tree data structure in which every non-leaf node is labelled with the hash of the labels or values of its child nodes

Mining	Data verification process for the Bitcoin blockchain by which the miners perform a proof-of-work consensus mechanism to confirm new Bitcoin transactions
Miner	Participants on the Bitcoin network who perform proof-of-work consensus mechanism tp confirm new Bitcoin transactions
Money services business (MSB)	According to FinCEN, Any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities: (1) Currency dealer or exchanger; (2) Check casher; (3) Issuer of traveler's checks, money orders or stored value; (4) Seller or redeemer of traveler's checks, money orders or stored value; (5) Money transmitter; (6) U.S. Postal Service"
Money transmitter	Business entity that provides money transfer services or payment instruments
Permissioned blockchain	Blockchain that grants read and write access to all users who wish to join the network
Permission-less blockchain	Blockchain that allows only permitted parties to join
Proof-of-Stake	Consensus mechanism by which certain network participants—called "validators"—take turns validating transactions in exchange for transaction fees, with validation frequency depending on how many coins each validator owns; the system also creates an enforcement procedure—for instance, by requiring validators to lock their coins in a virtual vault, which will be forfeited if these validators behave badly—to prevent validators from behaving badly
Proof-of-Work	Consensus mechanism by which participants in the network—called "miners"—compete to validate the transactions and append them to the database
Safe harbor	Provision in a legislation that provides exemptions by deeming certain conduct not to violate a given rule
Shared ledger	Data structure in which actors share the same data stored in the same location
Side chain	Mechanism for two or more blockchains to communicate with one another
Smart contract	Automation of transactions whereby business terms are recorded in computer language embedded in blockchain databases

Tamper-resistant	Property of blockchain database whereby data is protected against any manipulation
Trustless network	Network whereby the participants do not have established relationships and trust with one another
Zero-knowledge security	Data security protocol on a blockchain network whereby the network participants know neither the identities of the transacting parties nor the details of the transactions