THE BLOCKCHAIN REVOLUTION: AN ANALYSIS OF REGULATION AND TECHNOLOGY RELATED TO DISTRIBUTED LEDGER TECHNOLOGIES

By Hossein Kakavand and Nicolette Kost De Sevres, in collaboration with Commissioner Bart Chilton*

CONFIDENTIAL DRAFT

* Dr. Hossein Kakavand is the CEO of Luther Systems, a blockchain technology company, and an active advisor to the Blockchain industry. Dr. Nicolette Kost De Sevres is a senior academic and attorney (Canada and France) specialized on the Blockchain and based in Washington DC and Paris, where she practices in International financial regulation at DLA Piper. Commissioner Bart Chilton is a Senior Policy Advisor at DLA Piper in Washington DC and previously served as CFTC Commissioner. He is active in the Blockchain and cryptocurrency space and regularly writes and speaks on the subject. The authors wish to thank Bradley Cohen, associate at DLA Piper in Washington DC, and Sam Wood, CTO at Luther Systems, for their valuable help with this article.

INTRODUCTION

"The Blockchain is an opportunity for Wall Street to streamline some operations that are pretty antiquated."

Duncan Niederauer, former CEO of NYSE Euronext

"The trust machine ... technology behind Bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto-currency ... could transform how the economy works."

The Economist, Oct 2015

Many believe Blockchain will be as impactful as the Internet, thus referring to it as the "next revolution".[1] Originally built as the infrastructure underlying Bitcoin, many now see the different applications of Blockchain technology that go far beyond currencies. Blockchain technology has indeed far reaching applications that can influence significantly the way we interact in financial markets, as well as with artificial intelligence, computers and technology.

Blockchain technology is the use of a distributed and decentralized ledger for verifying and recording transactions. The technology allows parties to send, receive, and record value or information through a peer-to-peer network of computers. Blockchain has wide-ranging applications beyond digital currency (or "cryptocurrency"[2]), including as a platform for so-called smart contracts. Smart contracts are transactions or contracts converted into code that facilitate, execute and enforce commercial agreements between two or more parties. As discussed in this article, Blockchain-based smart contracts have the potential to streamline financial transactions and operational and counterparty risk associated with monitoring or enforcing contractual obligations.

On the regulatory and legal side, many issues have been raised in terms of privacy, security and risk. It is important that the right balance is achieved between the rapid development of Blockchain technology and its legal stability, assuring that the legal and regulatory dimensions do not hinder innovation in this space.

This article identifies the technological and regulatory dimensions related to Blockchain technology. We will first review the basic concepts related to Blockchain technology and "distributed ledger technology". We will further analyze the different possible applications of Blockchain technology, especially as it relates to financial markets. Finally, we will address regulatory developments in the EU and the US as well as the legal challenges. The article concludes on the need for the adoption of a regulatory framework which is flexible enough to encourage innovation while protecting consumers and end users.

---

[1] Don Tapscott and Alec Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 2016, Portfolio, ISBN 9781101980132.

[2] Please refer to the definition of crytocurrency in the section below.

1. DEFINING THE BLOCKCHAIN AND BASIC CONCEPTS

It is important to differentiate and define the basic concepts related to Blockchain technology. The original Blockchain technology was developed as the underlying infrastructure and database for effecting and recording transactions for the digital currency Bitcoin. It was developed to create and track agreements between counter-parties involved in Bitcoin (cryptocurrency) transactions.

In this section we define, describe and differentiate digital currencies and Blockchain technology and review their related but separate evolution.

1.1 Digital Currencies vs. Blockchain Technology

1.1.1 What is Blockchain?

Blockchain, the technology underlying Bitcoin, is a type of Distributed Ledger Technology ("DLT") that has been defined as a "distributed, shared, encrypted database that serves as an irreversible and incorruptible repository of information."[3]

Blockchain is a digital platform that stores and verifies the entire history of transactions between users across the network. From a technical standpoint, Blockchain is "a database that consists of chronologically arranged bundles of transactions known as blocks," against which any proposed transaction can be checked with confidence in the integrity of any particular block.[4] Once entered, the information can never be altered or erased[5]. It has been described as both a network and a database, equipped with built-in security and internal integrity[6]. From a theoretical perspective, Blockchain technology has the potential to replace transactions rooted in trust with those based on rules that are defined mathematically and enforced mechanically[7]. It is important to note that "Blockchain" does not have one single universally agreed-upon definition as it has a number of dimensions, including technological, operational, legal and regulatory.

1.1.2 Distributed Ledger Technology (DLT)

Distributed ledger technology refers to the ability for users to store and access information or records related to assets and holdings in a shared database (*i.e.*, the ledger) capable of operating without a central validation system and based on its

---

[3] Wright, Aaron and De Filippi, Primavera, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (March 10, 2015), available at http://ssrn.com/abstract=2580664.
[4] Wessel quoting BoE.
[5] Blockchain Technology, Sutardja Center for Entrepreneurship & Technology
[6] Embracing Disruption – Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape, Deposit Trust & Clearing Corporation (January 2016), *available at* http://www.dtcc.com/~/media/Files/PDFs/DTCC-Embracing-Disruption.pdf.
[7] Pilkington, Marc, "Blockchain Technology: Principles and Applications," page 15 (citing Kwon, J. (2014). Tendermint: Consensus without Mining. White paper.).

own standards and processes.[8] DLTs differ from standard accounting ledgers in that they are maintained by a distributed network of participants (known as "nodes") rather than a centralized entity.[9] Another common feature of DLTs is the use of cryptography as a means of storing assets and validating transactions.[10]

DLTs have a large number of various applications. One important application is in the financial services arena where DLTs could allow users with access to the shared database to directly clear and settle transfers related securities and cash with one another without relying on an intermediary.[11] Since all of the information or records would be distributed among all users, transactions conducted via DLTs could clear and settle almost instantaneously. Their development could pave the way for payment systems to disintermediate banks and function in an entirely decentralized manner.[12] The following sub-section will examine the technical theories and concepts that gave rise to DLT and Blockchain technologies.

1.1.3 Digital currencies, virtual currencies and cryptocurrencies

While no universal definition exists, "digital currency" is generally understood to be a digital representation of value that typically has some characteristics of a currency, and may have characteristics of a commodity or other asset.[13] Since digital currency can refer to either "virtual currency" (*i.e.*, value not tied to a fiat currency) or e-money (*i.e.*, value attached to a fiat currency), the terms digital currency and virtual currency are often used interchangeably.[14] Unlike e-money, where the underlying value is currency issued and backed by a central bank, virtual currencies derive value from their common acceptance a medium of exchange by a large number of individuals.

As US and European regulators issue guidance and rulings concerning virtual currency, a standard definition of virtual currency has emerged. For example, the European Central Bank has defined virtual currency as "a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency, but is used by natural or legal persons as a means of

---

[8] Andrea Pinna and Wiebe Ruttenberg, European Central Bank, Occasional Paper No. 172, *Distributed ledger technologies in securities post-trading* (April 2016), *available at* https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

[9] European Securities and Markets Authority, Discussion Paper, The Distributed Ledger Technology Applied to Securities Markets, p. 8 (June 2, 2016) *available at* https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

[10] *Id*.

[11] Pinna, *supra* note 6.

[12] Wessel, David; "Hutchins Center Explains: How Blockchain could change the financial system," (quoting Bank of England economists in "Innovations in Payment Technologies and the Emergence of Digital Currencies," Quarterly Bulletin, 2014:Q3).

[13] *Digital Currencies*, Committee on Payments and Market Infrastructures, Bank for International Settlements (November 2015), *available at* http://www.bis.org/cpmi/publ/d137.pdf.

[14] Financial Action Task Force (FATF) Report, *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 2014), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

exchange and can be transferred, stored or traded electronically."[15] In the US, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has defined virtual currency "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency," such as legal tender status in any jurisdiction.[16] Similarly, the Commodity Futures Trading Commission (CFTC) has distinguished virtual currencies from other "real currencies" (*i.e.*, coin and paper money), which are circulated as legal tender and customarily used and accepted as a medium of exchange.[17]

One prominent subset of virtual currency is cryptocurrency, which uses peer-to-peer protocols and cryptography to validate transfers of value. As discussed below, cryptocurrencies such as Bitcoin use "Blockchain" protocols that allow for transactions to be validated without an intermediary such as a bank or escrow agent.

As defined by the Bank for International Settlement, digital currencies combine decentralized payments systems and new currencies.[18] They have a decentralized payments mechanism based on the use of DLT, are not typically issued or connected to a fiat currency, and are not a liability of any entity or backed by any authority.[19] A commonly known cryptocurrency is Bitcoin.

Bitcoin is the most prominent, widely accepted cryptocurrency currency in use today. It has experienced a large number of events and stresses, and has emerged as the most reliable cryptocurrency.

1.2 Blockchain Technical Concepts and Implementation

1.2.1 Technical concepts

A review of the technical concepts of Blockchain technology is necessary to understand the implications of the different architectures with respect to performance, privacy, security and regulation. A variety of different Blockchain-based technologies have been developed to solve different problems. As such, the different technologies available are more or less appropriate for different needs.

In general, a Blockchain is a digital platform that stores and verifies the entire history of transactions between users across the network in a tamper- and revision-proof way. It is also the underlying database structure for digital

[15] *EBA Opinion on virtual currencies*, European Banking Authority (July 4, 2014), p. 11 *available at* https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf p. 11; see also *Virtual currency schemes – a further analysis*, European Banking Authority (February 2015), p. 4, *available at* https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (describing virtual currencies as an alternative to money in certain circumstances).
[16] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013), *available at* https://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
[17] In re: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29, fn. 2
[18] The economics of digital currencies – Bank of England, 2014 Q3 quarterly bulletin
[19] Committee on Payments and Market Infrastructures – Bank for International Settlements - Nov 2015

currency transactions including in the Bitcoin and Ethereum networks. Transactions between users or counter-parties are broadcast across the network and are verified by cryptographic algorithms and grouped into blocks. Each block is subsequently verified by the network and added to the Blockchain. Blocks are chained to each other so one could never alter them. Each node participating in the Bitcoin network has its own copy of the Blockchain, which is synchronized with other nodes using a peer-to-peer protocol.[20] This "removes the need for a central authority and thus for participants to have confidence in the integrity of any single entity."[21] Blockchain technology enables multiple organizations and groups within an organization to efficiently process transactions and securely reach consensus without the requirement of a third party.

Related Technical Concepts

Blockchain technology can be better understood through the introduction of some of the fundamental technical concepts[22]:

i. **Node**: A Blockchain is maintained by software that runs on a computer called a node or peer. Each node is connected to the Blockchain network and can submit and receive transactions. Each node participating in the Bitcoin network, for example, has its own copy of the Blockchain, which is synchronized with other nodes using a peer-to-peer protocol.

ii. **Network**: Organizations and possibly individuals maintain computer systems called nodes, these nodes run Blockchain software to communicate with each other and form a Blockchain network.

iii. **Smart Contracts**: Transactions or contracts that are converted into code to be executed on a Blockchain are known as scripts or smart contracts.

---

[20] Proof of Stake versus Proof of Work, White Paper, Bitfury Group Limited, Sept 13, 2015, http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf.

[21] Wessel quoting BoE.

[22] **Some additional concepts include the following:**

i. Hash Function: A hash function is a one-way function that maps an input of arbitrary size to a fixed sized output called a hash. A cryptographic hash function is a hash function that includes the properties (i) easy to generate the hash given the input, (ii) infeasible to generate the original input given the hash, (iii) virtually impossible for two similar inputs to have the same output in a so called "collision". SHA256 is an example cryptographic hash function that is used in the Bitcoin and Ethereum networks.

ii. Consensus: In distributed systems, multiple processes communicate to enable system operation. Faults may occur anywhere throughout a distributed system, for example processes may crash or adversaries may send malicious messages to processes. Distributed systems use consensus protocols to achieve reliability despite faults. Processes execute a consensus protocol so that they reach agreement within a certain period of time. For example, in Bitcoin nodes execute a proof-of-work consensus protocol to reach agreement on the next valid block and blocks are generated roughly every 10 minutes. An adversary who injects malicious data into the system can trigger faults known as "Byzantine faults" where multiple processes receive conflicting information. Byazantine Fault Tolerance (BFT) refers to consensus protocols that achieve consensus in systems with Byzantine faults.. BFT is a well understood distributed systems problem within computer science and implementations have existed for several decades..
See: http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf

iv. **Submit Transaction**: Users submit transactions to the Blockchain by sending them to nodes on the network who subsequently disseminate them to all other nodes on the network.

v. **Transaction Validation**: Nodes on the Blockchain network receive, process and cryptographically validate each transaction. The network ignores invalid transactions.

vi. **Block**: Nodes collect and group valid transactions together into a bundle known as a Block. Blocks must follow a pre-determined set of rules for them to be valid. For example, they must not exceed a maximum size in bytes, contain more than a maximum number of transactions, and must reference the most recent valid block.

vii. **Blockchain**: Each new block contains a reference to the most recent valid block and is attached to that block. *i.e.*, it is placed after that block in the database, forming a "chain of blocks".

viii. **Consensus**: The process of ensuring that every node agrees on the Blockchain.

Many other technical concepts relate to the functioning of a DLT, some of which we will analyze further below.

1.2.2 Permissioned vs. Permission-Less

Distributed ledgers supporting for example Bitcoin are public ledger that any can use to interact with any individual regardless of whether they know them or not. Further, anyone can interact with such ledgers, *i.e.*, they can read from/ write to them. This feature makes public ledgers appealing for a number of applications. However, there are commercial applications where the counter-parties to transactions prefer the details of their transaction to remain private and not visible to the general network and the public. Examples of such applications include various financial transactions, exchange of medical records, the shipment of goods among many others. Private Blockchains are rather appropriate and relevant for a large number of commercial application and are likely to gain considerable traction over the coming years.

Permissioned or private Blockchains add a layer of privileging to determine who can participate in the network, with the identity of each participant known to all participants. New participants are invited to the network. The exact details of invitation are varied. Options include: unanimous agreement, core group acceptance, single user invitation and satisfaction of pre-determined set of requirements[23].

[23] http://www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf

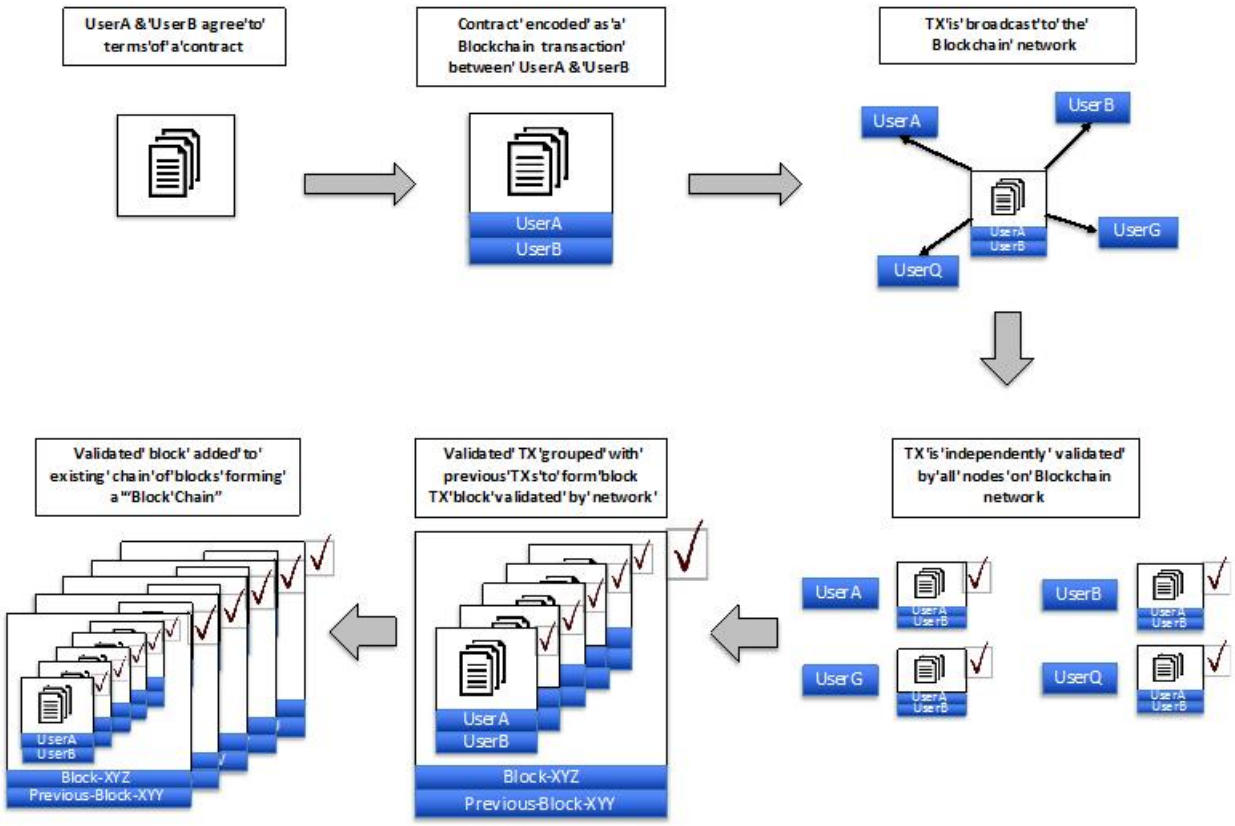

Fig.1: An overview of the Blockchain process.

1.3 Blockchain Performance Metrics & Implementations

1.3.1 Metrics

Blockchain technology has developed very quickly, with a variety of different database technologies and distributed protocols emerging. These technologies are being established for a number of different industries and applications, and as such require a myriad of different specifications. The technologies being developed are aiming to address and solve the scalability and throughput capacity of Blockchains, and ensuring their security, robustness and performance. These areas are currently being addressed by a variety of different types of distributed ledger technologies with varying degrees of decentralization.

A Blockchain node processes transactions and stores the current and past state of the entire network. The performance of a Blockchain architecture can be evaluated based on a number of qualitative and quantitative metrics described below:

i. **Submission Throughput**: maximum number of transaction submissions per second possible/ permitted by each node and by the entire network.

ii. **Maximum/Average Validation Throughput**: maximum/ average number of transactions/ blocks validated per second possible/ permitted by the network. This parameter determines the maximum/ average transaction processing speed of the network.

iii. **Average Transaction Validation Latency**: the average length of time it takes for a transaction to be validated from the time of submission. This parameter determines how long on average a user needs to wait for their transaction to be validated and placed in a block. Note that the notion of validation and block confirmations might vary for each Blockchain.

iv. **Latency Volatility**: the volatility of transaction validation latency. This is a measure of how varied the transaction processing time could be.

v. **Security**: system security evaluation requires a threat model that defines the types and scope of adversaries and attacks on the system. Threat models vary across Blockchain applications. A security evaluation may include analysis of:

    a. Transaction and block immutability

    b. Transaction censorship resistance

    c. Denial of Service (DoS) resilience

    d. Trust requirements of users and oracles

    e. Protocol governance and node membership services

    f. Transaction confidentiality and user anonymity.

vi. **Confidentiality**: Two nodes transacting on a Blockchain may not want other nodes to "know" the contents of the transaction and in some cases may not want other nodes to even "know" their identity as having participated in that transaction.

vii. **Transaction fees**: In many of the technologies users must pay a small transaction fee to the network in order to process transactions or execute smart contracts. These fees support the maintenance costs of the Blockchain and provide protection from frivolous or malicious

computational tasks such as spam transactions or infinite loops in smart contracts.

viii. **Hardware requirements**:

a. Memory/storage: total memory/storage capacity required per node

b. Processor: amount of processing resources required to validate transactions and blocks

c. Network usage over time, including throughput and latency requirements

d. Hardware requirements will change as the network scales

ix. **Scalability**

a. Number of nodes: system performance change as the number of nodes increases

b. Number of transactions: system performance change as the number of transaction submissions per second increases

c. Number of users: system performance change as the number of active users submitting transactions increases

d. Geographic dispersion: system performance change as the geographic dispersion of nodes increases

x. **Validation process**: not a performance metric but an important factor in determining the performance of the network.

xi. **Complexity**: a measure of the development, maintenance, and operation complexity of Blockchain infrastructure.

xii. **Smart-contract limitations**: what the code deployed on the Blockchain can and cannot do, this is influenced by the smart contract scripting language and the underlying consensus protocols.

There are a number of private and public Blockchain infrastructures provided by various market participants who offer different levels of performance with respect to the metrics discussed above. Some of the key market participants, products, and infrastructures are presented below.

1.3.2 Examples of DLT implementation

1.3.2.1 Bitcoin

First, Bitcoin, launched in 2009, is a decentralized digital currency designed to facilitate the transfer of value between parties without the need for third-party intermediaries, and has its own unit of value called "bitcoin". The Bitcoin network first introduced and implemented Blockchain technology, storing all transactions on a network of nodes in a distributed public ledger. The ledger records the history of every bitcoin transaction made and blocks are added to the Blockchain through a process called 'mining' that uses "Nakamoto Consensus", a proof-of-work consensus protocol[24]. It does not require a central party to facilitate transactions or confirm balances, and is an open payment system that can be accessed by anyone, anywhere. Bitcoin is a permission-less and cryptographically secure network.[25] The peer-to-peer resiliency of the network ensures that there are no central points of failure and Nakamoto Consensus ensures that all nodes are in agreement on the status of all validated transactions.

1.3.2.2 Ethereum

Second, Ethereum is an open Blockchain platform that allows building, executing, and using decentralized applications (DApps). Ethereum allows for ease of creation of applications that automate direct interaction between peers or facilitate coordinated group action across a network[26].

Similarly to Bitcoin, it has a fully customizable payment logic, allowing for the creation of payment systems without the reliance on third-party intermediaries. It has been developed with particular emphasis on situations where rapid development time, security for applications, and the ability of different applications to interact efficiently with each other are important[27]. To aid this, Ethereum employs a "Turing complete" programming language allowing for developers to create applications that run on the Ethereum system in a variety of programming languages.

The Ethereum platform has been built to have high levels of security against denial of service attacks, and relies on a proof-of-work mining process. All operations on Ethereum are executed through the Ethereum Virtual Machine "EVM", where smart contract computations are paid for using a cryptocurrency called Ether. Every node of the EVM runs all computations in order to maintain consensus throughout the Blockchain[28].

---

[24] See "Bitcoin: A Peer-to-Peer Electronic Cash System".
[25] Blockchain: A Fundamental Shift for Financial Services Institutions, Capgemini, page 9
[26] https://media.readthedocs.org/pdf/ethereum-homestead/latest/ethereum-homestead.pdf
[27] Understanding Ethereum, CoinDesk, page 6
[28] Ethereum White Paper - https://github.com/ethereum/wiki/wiki/White-Paper

Although this process provides Ethereum with extreme levels of fault tolerance, this massive use of synchronized computing across the entire Ethereum network makes computation slow and means contracts are stored publicly on every node of the Blockchain[29].

1.3.2.3 IBM Open Blockchain and Hyperledger Fabric

Third, the IBM Open Blockchain (OBC) was created on the expectation that there will be many Blockchain networks, with each network ledger serving and providing for different goals. IBM is part of the larger Hyperledger Project, a Linux foundation project, that aims to advance Blockchain technology by identifying and addressing important features for a cross-industry open standard for distributed ledgers. OBC has since been replaced and incorporated entirely into the open source Hyperledger Fabric architecture that is distributed under the Hyperledger Project. The system has no requirement for any one network ledger to rely upon another network for its core functionality[30], and is also 'Turing complete' like Ethereum. The Hyperledge Fabric therefore allows for many different uses of the Blockchain technology and the creation of distinct levels of permissioning. Through being able to encrypt all transactions on the fabric, and only providing access on how to decrypt the information to the relevant stakeholders, it is possible to conceal the identity, transaction patterns, and terms of confidential contracts from unauthorized third parties. Unlike Bitcoin, Hyperledger Fabric does not rely on proof-of-work mining to secure consensus throughout the system, and instead relies on Byzantine Fault Tolerant (PBFT) algorithm.

1.3.2.4 ErisDB / Tendermint

Fourth, ErisDB, similarly to Ethereum, is an open-source Blockchain platform for building, testing, maintaining, and operating DApps. However, unlike Ethereum, it allows for the creation of both permissioned and permission-less Blockchains. ErisDB was designed to be deployable in a variety of environments including public facing, enterprise consortiums, and private corporate environments.[31] ErisDB fully supports the EVM so that smart contract code written for Ethereum, such as code written in the Solidity programming language, can also execute on an ErisDB Blockchain. ErisDB sits at the layer in the stack between a Blockchain client[32] and the operating system, and aims to allow people to easily build DApps, and has developed its platform alongside the open source Tendermint project, using Tendermint's consensus protocol.[33] The Tendermint project includes an open source BFT consensus protocol

[29] Ethereum Homestead Documentation, Release 0.1 – page 4
[30] Architecture of the Hyperledger Blockchain Fabric, IBM research, page 2
[31] Eris Industries – Company Blog , https://erisindustries.com/components/erisdb/, 28 August 2016
[32] Eris Industries – Company Blog – 19 August 2015
[33] Tendermint: Consensus without Mining – page 1

implementation for smart contracts that is used as the consensus layer in Blockchain frameworks such as ErisDB.[34]

1.3.2.5 R3CEV

Finally, although not directly a Blockchain infrastructure itself, R3CEV, a technology firm, is leading a consortium partnership of a number of financial companies into the research and development of Blockchain usage in the financial system. R3CEV aims to improve the integration of Blockchain and to build a financial-grade ledger, where it aims to develop the base layer reference architecture underpinning a financial-grade ledger.[35] R3CEV hopes to get financial institutions and regulatory bodies involved and engaged with the initial deployment and creation of a common distributed ledger-standard.

2. BLOCKCHAIN APPLICATIONS

2.1 FINANCIAL MARKETS

2.1.1 Clearing, trading and replacing the intermediary

The clearing and settlement of financial assets is a traditional function of the banking industry. "Major markets such as the U.S., Canada and Japan still have a 3-day settlement cycle in place, while the EU, Hong Kong and South Korea have moved to" a two day settlement cycle.[36] "On January 26, 2015, the Federal Reserve issued a call to action for all stakeholders in the U.S. payments systems to increase end-to-end payment speed, among other things."[37] The lag between the time the trade is made and the time at which it settles is what drives a number of credit- and liquidity-related risks and presents substantial opportunities for improvement. Some indicate that "the Blockchain does not only move value; it also integrates several components of the trading-clearing-settlement value chain in an elegant and efficient way".[38] Thus, one of the potential applications for Blockchain is in the context of clearing and settling trades.

The lifecycle of a trade begins when a buyer and a seller agree to trade a particular security. Once the agreement is reached, "the two counterparties update their accounts and arrange for the transfer of the security and the associated monies," which is known as clearing the trade.[39] Once the process, which is made up of numerous steps, is complete, the monies and the security actually change hands, generally occurring 2 to 3 days after the original

[34] Tendermint: Cases for Tendermint, http://tendermint.com/blog/cases-for-tendermint/, 28 August 2016
[35] R3CEV - http://r3cev.com/about/
[36] Peters, Gareth W. and Efstathios Panayi, "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," page 26.
[37] Kiviat, page 585-86.
[38] Kiviat, Trevor I., "Beyond Bitcoin: Issues in Regulating Blockchain Transactions," 65 Duke L.J. 569, 587 (2015-2016).
[39] Peters, page 26.

agreement is reached. Several participants are involved in the clearing process, including: **(i) clearing members,** who have access to the clearing house in order to settle trades", and **(ii) clearing house/CCP**, which stands between two clearing members."[40]

This example of central clearing, when a middleman (called a central counterparty or CCP) becomes a counterparty to each party making the trade, is increasingly becoming more common as regulators are encouraging the shift from bilateral trading to central clearing. "This simplifies the risk management process, as firms now have a single counterparty to their transactions. Through a process termed novation, the CCP enters into bilateral contracts with the two counterparties, and these contracts essentially replace what would have been a single contract in the bilateral clearing case. This leads to some contract standardization and a general reduction in the capital required due to multilateral netting of cash and fungible securities."[41]

However, a longer settlement cycle may present two main risks: **(i) counterparty risk** between trade execution and settlement, and associated margin requirements, which leads to a requirement for clearing members to maintain a prescribed level of capital with the CCP, and **(ii) settlement risk**, which is 'the risk that one leg of the transaction may be completed but not the other'.[42]

A shorter settlement time would reduce both of these risks and result in trades being completed more reliably and clearing members being subject to lower capital requirements. By reducing the risk of purchaser default and thus lowering counterparty credit risk, this would help reduce an institution's balance sheet capital requirements under Dodd-Frank. Distributed ledger technology virtually eliminates credit and liquidity risk by requiring pre-funding, in which the cash and collateral to be traded pre-exist prior to trading.[43]

Blockchain technology can disrupt the clearing and settlement process by bringing with it decentralization and disintermediation. For example, a consortium of clearing members could set up a distributed clearing house, thus eliminating the need for a CCP. Clearing then becomes closer to bilateral clearing, however as the contract stipulations through the Blockchain administered through a smart contract[44], there is reduced risk management issues.[45] The use of Blockchain technology could "increase the speed of the entire settlement cycle from days to minutes or even seconds," eventually leading to continuous settlement. Additionally, all reporting, compliance and collateral

[40] Peters, page 26.
[41] Peters, page 27.
[42] Peters, page 27.
[43] Condos, James, William H. Sorrell, and Susan L. Donegan, "Blockchain technology: opportunities and risks,"January 15, 2016, pages 15-16 (citing to McKinsey and Co.).
[44] Smart contracts are described in further detail in Section 2.1.E
[45] Peters, page 28.

management can be handled through the Blockchain, thus reducing back-office costs.[46]

A closely-related feature is placing funds in escrow and not allowing them to be released until each party is satisfied with the performance of the other as reflected in a digital signature. Additional security could be added to a transaction by requiring the signature of a third or even more parties, who play a role in authenticating performance.[47]

Not everyone is approaching Blockchain equally optimistically. Some authors indicate that "Blockchain is always going to be more expensive than a central clearer because a multiple of agents have to do the processing job rather than just one, which makes it a premium clearing service – especially if delinked from an equity coupon – not a cheaper one."[48]

2.1.2 Payment systems

Another promising application for distributed ledger technologies such as Blockchain is payments. Currently, payments are cleared and settled through trusted, central third party intermediaries. Industry experts predict that private, permissioned Blockchains will gain significant volume in the payments space by 2020. For example, in June 2016, Santander UK partnered with the Blockchain startup Ripple to become the first UK bank to introduce Blockchain technology for international payments.

More particularly, in the US, states have traditionally regulated non-depository financial services providers such as Blockchain payment companies. Existing state laws establishing licensing and compliance standards for money transmitters, such as the Uniform Money Services Act, may be expanded as Blockchain-based payment systems proliferate. Additionally, certain Blockchain-based payment providers may be subject to money services business (MSB) regulations issued by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). On the other hand, the EU has a uniform legal framework–the Electronic Money Institutions Directive–for regulating electronic money.

2.1.3 Operational risks in financial markets

In the financial regulatory world, clearing intermediaries as well as most payment systems fall within a category of regulated entities called financial market infrastructures ("FMIs"). "The Federal Reserve, consistent with standards set by the G20 and Financial Stability Board, defines FMIs as 'multilateral systems

[46] Peters, page 28.
[47] Shadab, page 14.
[48] Mainelli, Michael and Mike Smith, Z/Yen Group Limited, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka Blockchain technology)", The Journal of Financial Perspectives: FinTech, EY Global Financial Services Institute, Winter 2015, Volume 3, Issue 3, page 11 (quoting Kaminska, I., 2015, "On the potential of closed system Blockchains," FT Alphaville, 19 March).

among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions,' which 'include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories.'"[49] Therefore FMIs are regulated. The automation of trade clearing or of payment systems through the Blockchain technology could eliminate the need for a trusted intermediary which could in turn also present operational risks. These risks will have to be clearly identified, disclosed and monitored.

2.2 Smart contracts

Although the Blockchain was initially developed to facilitate cryptocurrency transactions, entrepreneurs are now developing the technology for employing smart contracts. To develop a smart contract, parts of the terms that make up a traditional contract are coded and uploaded to the Blockchain, producing a decentralized smart contract that does not rely on a third party for recordkeeping or enforcement. Contractual clauses are automatically executed when pre-programed conditions are satisfied. This eliminates ambiguity regarding the terms of the agreement and disagreement concerning the existence of external dependencies.

Smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts usually also have a user interface and often emulate the logic of contractual clauses. Proponents of smart contracts claim that many kinds of contractual clauses may thus be made partially or fully self-executing, self-enforcing, or both. Smart contracts aim to provide security superior to traditional contract law and to reduce other transaction costs associated with contracting.

One of the most important characteristics of Blockchains as it relates to smart contracts is the ability to enter into "trustless" transactions. Trustless transactions are transactions that can be validated, monitored and enforced bilaterally over a digital network without the need for a trusted, third-party intermediary. Multi-signature (or "multi-sig") functionality can be incorporated into smart contracts where the approval of two or more parties is required before some aspect of the contract can be executed (e.g., an escrow agreement between two parties and an escrow agent). Where a smart contract's conditions depend upon real world data (e.g., the price of a commodity future at a given time), agreed-upon outside systems called "oracles" can be developed to monitor and verify prices, performance, or other real world events.

Financial transactions are one potential use case for smart contracts. Smart derivatives contracts could be coded such that payment, clearing, and settlement occur automatically in a decentralized manner without the need for a third-party intermediary such as an exchange or clearing house. For example, a smart derivatives contract could be pre-

[49] Walch, Angela, "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk," Journal of Legislation and Public Policy, Vol. 18:837, page 851-852 (quoting Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. 67326, 67333 (Nov. 12, 2014)).

programed with all contractual terms (*i.e.*, quality, quantity, delivery) except for the price, which could be determined algorithmically from market data fed through an oracle.[50] Margin could be automatically transferred upon margin calls and the contract could terminate itself in the event of a counterparty default. The Blockchain would perform the recordkeeping, auditing and custodial functions traditionally performed by intermediaries, resulting in transactional cost savings for the contracting parties.

As ESMA states in its recent Discussion Paper on DLT, "Smart contracts, which would sit on top of the ledgers, may help reduce the uncertainty attached to contract terms and increase the automation of the processing of corporate actions, even if their use may be limited to certain types of instruments or contracts for complexity reasons, at least in the short term. […]. Smart contracts are self-executing codes meant to replicate the terms of a given contract. They effectively translate contractual terms (e.g., payment terms and conditions, confidentiality agreements) into computational material."[51]

2.3 OTHER INDUSTRY APPLICATIONS

While financial applications have received considerable attention, Blockchain technology has the potential to provide disruptive applications to other industries.

2.3.1 Real Estate Industry

Applications of Blockchain technology in the real estate industry can be applied to both public and private sectors. In the public sector, land registry records and public records of land ownership can be placed on the Blockchain, allowing the relevant stakeholders and agencies real time access to the ownership records. This considerably reduces ownership disputes and the need for middlemen to authentic documents and adjudicate disputes, ultimately saving cost and time for the end consumer. This application is explored by various jurisdictions around the world including the government of Honduras[52].

Within the private sector, residential rental agreements between private counter-parties can be placed on Blockchain and executed using smart contracts. This will streamline private contracts and real estate agency workflow, saving resources and time.

2.3.2 Health Care Industry

There are multiple applications of Blockchain technology to the healthcare industry, including in the distribution pipeline for various goods and services. One specific case is the drug delivery pipeline from the factory floor to the end user, whereby the drug packages are authenticated and time stamped at each

[50] Houman B. Shadab, Written Statement to the Commodity Futures Trading Commission Global Markets Advisory Committee: Regulating Bitcoin and Blockchain Derivatives (Oct. 9, 2014), *available at* http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/gmac_100914_Bitcoin.pdf.
[51] ESMA/2016/773
[52] Reuters News - http://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515

intermediate delivery point. For example, for a batch of drugs being shipped from the factory floor, the batch record is authenticated, time-stamped and placed on the Blockchain and is subsequently authenticated and time-stamped again at each intermediate delivery point. This allows for tracking of the drug as it makes its way through the delivery pipeline. This greatly simplifies and streamlines the drug distribution pipeline management which can prevent the drugs from falling into the wrong hands, authenticating the drug for the end consumer which greatly reduces the counterfeiting possibility, price manipulation and delivery of expired drugs[53].

2.3.3 Smart Government

Government agencies can benefit considerably from the near instantaneous and simultaneous access to a distributed database that stores public records. An important example is identity management, e.g. "are you who you say you are". Although solutions for identity management on the Blockchain are yet to be fully developed, there is a considerable amount work being done on this topic. For example, passports or drivers' licenses can be placed on the Blockchain, enabling multiple agencies to share, access and verify identification in real time. The Estonian government is experimenting with identity management solutions on the Blockchain[54].

Another example is in Regulatory & Taxation applications. Many banks and financial institutions are currently working towards placing institutional and personal financial transaction on the Blockchain. Regulators can directly impose restrictions on the execution of transactions on the Blockchain that can be enforced automatically. This reduces the regulatory compliance and auditing costs which contributes to considerable cost reduction. Financial transactions can also be taxed automatically since the ledger keeps track of transfer of ownership of assets, as each transaction is visible to the relevant Tax agencies[55]. This reduces the overhead in terms of filing and auditing of taxes, and reduces the need for various intermediaries in the process.

Another interesting application is in Foreign Aid. Using cross-border transfers foreign aid can be distributed in a far more targeted and efficient manner to reach its intended recipients directly in disaster zones, war zones or planned foreign aid.[56] This results in a more timely and efficient delivery of the aid and considerably reduces the need for middlemen, and eliminates multiple channels and opportunities for corruption and misuse of funds.

---

[53] Blockchain Technology Could Help Solve $75 billion Counterfeit Drug Problem http://www.ibtimes.com/blockchain-technology-could-help-solve-75-billion-counterfeit-drug-problem-2355984

[54] Forbes – The Tiny European Country that became a global leader in digital government - http://www.forbes.com/sites/dell/2016/06/14/the-tiny-european-country-that-became-a-global-leader-in-digital-government/#45fc179a4c7f

[55] Blockchain: Disrupting the Financial Services Industry – Deloitte, page 10

[56] Blockchain: Blueprint for a New Economy, Melanie Swan – page 61

Finally, another application of Blockchain technology in Smart Government is in voting systems. Using Blockchain technology, each citizen (or recognized member of a group) can submit their vote on an anonymized Blockchain, and the results of the voting can be determined by consensus between participant without the details of each person's vote or identity ever becoming public.[57] This eliminates considerable voting environment overhead, from preparation to technology to staff to counts and recounts.

2.3.4 Artificial Intelligence

A very interesting application is the integration of Blockchain technology and artificial intelligence. This will have many and far-reaching implications in the future. Currently, smart contracts have very basic "narrow intelligence"; they can be programmed to execute a number of actions based on pre-determined rules and conditions, for example the timing of transaction execution. As Blockchain technology develops, smart contracts' implementation and development will advance and become more sophisticated. With the integration of artificial intelligence, nodes on the Blockchain can "learn certain functions" and be able to function on their own in a semi-autonomous way.

Further development that could result from this collaboration of technologies are, (i) negotiations between nodes on the Blockchain on asset price discovery, (ii) discovering ownership networks of financial assets which can greatly improve the KYC process in financial applications and expose tax havens, a rather relevant topic these days in wake of the recent Panama papers revelations[58] (iii) Blockchain nodes cooperating to optimize household energy consumption within the broader Internet of Things model.

3. BLOCKCHAIN REGULATION

3.1 <u>European Regulators and Governments</u>

3.1.1 ESMA

On June 2016, the European Securities Market Authority (ESMA), published a Discussion Paper entitled "The Distributed Ledger Technology Applied to Securities Markets"[59] which addresses potential benefits and risks that DLT could have on securities markets, especially from a public policy perspective. ESMA seeks comments from the industry and, at this stage, does not express any opinion as such, related to DLT. In April 2015, ESMA had already published a call for evidence on investments using virtual currencies or DLT which showed that this investment remained marginal. However, the call for evidence also showed that DLT had a potential to be used by financial markets.

---

[57] Blockchain: Blueprint for a New Economy, Melanie Swan – page 61
[58] Financial Times – Panama Papers Leaks http://www.ft.com/panama-papers-leak
[59] ESMA/2016//773

3.1.2 UK Treasury

The UK Treasury has recently published a report entitled " Distributed Ledger Technology: beyond blockchain", in which it presents a set of right recommendations which address amongst other, technology, governance, privacy, security, disruptive potential, applications and the global perspective. More precisely, in terms of regulation, the report states that "Government needs to consider how to put in place a regulatory framework for distributed ledger technology. Regulation will need to evolve in parallel with the development of new implementations and applications of the technology".

3.2 US Regulators

While many US regulators have touted the potential benefits of Blockchain and other DLTs (as well as the virtual currencies exchanged on them), some have expressed concerns regarding their impact on financial stability and market integrity. Recently, the Financial Stability Oversight Council (FSOC), a group of US regulators that includes the Securities and Exchange Commission (SEC) and the Treasury Department, warned that Blockchain and other DLTs pose "risks and uncertainties which market participants and financial regulators will need to monitor."[60] These and other US regulators have also opined individually on the benefits and potential risks associated with the nascent technology.

3.2.1 SEC

Among US regulators, the SEC has been actively exploring potential application of Blockchain and other DLTs for financial services transactions in the public securities market. In a November 2015 speech, Commissioner Kara Stein first touted the potential of Blockchain for tracing securities lending, repo, and margin financing and monitoring systemic risk by, for example, overseeing collateral reuse.[61] However, Commissioner Stein also cautioned that as the market embraces Blockchain technology, "regulators need to be in a position to lead, harnessing its benefits and responding quickly to potential weaknesses."[62] One such potential benefit identified by the SEC is the application of Blockchain for transfer agents – persons who keep track of the individuals and entities that own publically traded securities. In its 2015 proposed rulemaking on transfer agents, the SEC queried what utility, if any, Blockchain or other DLTs would have for transfer agents.[63]

---

[60] FSOC 2016 Annual Report, Financial Stability Oversight Council, p.127, *available at* https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC%202016%20Annual%20Report.pdf.

[61] Remarks of SEC Commissioner Kara Stein, *Surfing the Wave: Technology, Innovation, and Competition*, Harvard Law School's Fidelity Guest Lecture Series (November 9, 2015), *available at* https://www.sec.gov/news/speech/stein-2015-remarks-harvard-law-school.html.

[62] *Id*.

[63] Advance notice of proposed rulemaking, *Transfer Agents Regulation*, Securities and Exchange Commission Release No. 34-76743 (December 22, 2015), *available at* https://www.sec.gov/rules/concept/2015/34-76743.pdf.

Moreover, the SEC has embraced the early adoption of Blockchain as it relates to securities offerings. In an April 2016 speech before the SEC-Rock Center's Silicon Valley Initiative, SEC Chair Mary Jo White indicated that the Commission is "closely monitoring the proliferation of this technology and already addressing it in certain contexts."[64] Most notably, the SEC has addressed Blockchain in its review of Overstock.com Inc.'s bid to issue public securities using its t0.com Blockchain platform.[65] The SEC ultimately approved Overstock's S-3 filing and the retailer intends to offer common stock on the platform in the near future, which would make it the first world's first public Blockchain security.[66]

3.2.2 CFTC

The Commodity Futures Trading Commission (CFTC) is another US regulator examining how Blockchain and DLTs could be used in the derivatives market. In March 2016, CFTC Commissioner J. Christopher Giancarlo delivered a speech before the Depository Trust & Clearing Corporation concerning the regulation of DLT.[67] In his speech, Commissioner Giancarlo discussed the emergence and potential applications of DLT, before cautioning against overburdening the budding industry with multiple regulatory frameworks. He stressed the importance of adopting a "do no harm" regulatory approach that establishes "uniform principles in an effort to encourage DLT investment and innovation."[68]

More formally, the CFTC Technology Advisory Committee (TAC) meeting held in April 2016 included a Blockchain panel. The panel included a discussion of the potential applications of DLT in the derivatives market, as well as a demonstration of swap transaction executed on Blockchain, and a primer on the structure and operation of the underlying technology.[69] The TAC noted that the lack of industry standards to date is a result of the fact that Blockchain and DLTs are still emerging and their implementation will be incremental. The TAC also discussed the possibility of a regulator such as the CFTC having access to the network as an additional node on the Blockchain.

In addition to exploring the application of Blockchain and DLTs, the CFTC has recently become active in the Bitcoin and virtual currency enforcement space. In

---

[64] Keynote Address of SEC Chair Mary Jo White at the SEC-Rock Center on Corporate Governance, Silicon Valley Initiative (March 31, 2016), *available at* https://www.sec.gov/news/speech/chair-white-silicon-valley-initiative-3-31-16.html.

[65] *See* Overstock.com, Inc. Form S-3 Registration Statement (filed November 10, 2015), *available at* https://www.sec.gov/Archives/edgar/data/1130713/000104746915008523/a2226515zs-3a.htm.

[66] *Overstock to issue stock to be traded on Blockchain platform*, Reuters (March 16, 2016), *available at* http://www.reuters.com/article/us-overstock-Bitcoin-stocks-idUSKCN0WI2YA.

[67] Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium (March 29, 2016), *available at* http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-13.

[68] *Id*.

[69] CFTC Technology Advisory Committee Meeting Agenda, Commodity Futures Trading Commission (February 23, 2016), *available at* http://www.cftc.gov/About/CFTCCommittees/TechnologyAdvisory/tac_022316agenda.

September 2015, the Agency brought and settled its first enforcement action against an unregistered Bitcoin derivatives trading platform.[70] The order reiterated previous statements by CFTC Commissioners characterizing Bitcoin and other virtual currencies as "commodities" under the CEA.

3.2.3 FinCEN

FinCEN is another US regulator issuing administrative rulings and interpretive guidance regarding virtual currencies and Blockchain. In March 2013, the regulator issued guidance clarifying the applicability of Bank Secrecy Act (BSA) regulations to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.[71] The ruling states that an administrator or exchanger (but not a user) of virtual currency is a money service business (MSB) under FinCEN's regulations, (specifically, a money transmitter) absent an exemption. In 2014, FinCEN elaborated on this guidance in two administrative rulings establishing that the BSA's definition of a money transmitter includes neither users who create or "mine" virtual currency for their own purposes, nor companies purchasing and selling convertible virtual currency as an investment exclusively for their own benefit.[72] FinCEN also issued an August 2014 ruling that an online precious metals brokerage using Blockchain was subject to the regulator's money transmission regulations.[73]

3.2.4 Internal Revenue Service

From a tax perspective, the US Internal Revenue Service (IRS) has opined on the treatment of digital currency for federal tax purposes. Under IRS Notice 2014-21, digital currency is treated as property rather than a foreign currency, and the foreign currency rules for determining gain and loss do not apply to digital currency. Additionally, under IRS Notice 2014-21, taxpayers that receive digital currency as payment for goods or services must recognize income at the time of receipt in the amount of the fair market value of the digital currency received. At the time of receipt, the taxpayer takes a basis in the digital currency equal to the fair market value, and when the taxpayer disposes of the currency, it will recognize gain or loss.

---

[70] In re: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29, *available at* http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf.

[71] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, Financial Crimes Enforcement Network (March 18, 2013), *available at* https://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[72] FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors, Financial Crimes Enforcement Network (January 30, 2014), *available at* https://www.fincen.gov/news_room/nr/pdf/20140130.pdf.

[73] Financial Crimes Enforcement Network (FinCEN), *Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals*, FIN-2015-R001 (August 14, 2015), *available at* https://www.fincen.gov/news_room/rp/rulings/html/FIN-2015-R001.html.

3.2.5 Other US agencies

Other US agencies such as the Federal Trade Commission (FTC) and the Consumer Financial Production Bureau (CFPB) have brought enforcement actions and issued warnings to consumers regarding the risks associated with Bitcoin and virtual currencies more generally. For instance, the FTC brought and settled charges against a Bitcoin company preselling computer hardware that it claimed was optimized for mining Bitcoin. Meanwhile, in response to a Government Accountability Office (GAO) calling for increased oversight of Bitcoin and other virtual currencies, the CFPB issued a 2014 warning to consumers regarding the risks posed by virtual currencies.[74]

Most recently, the Office of the Comptroller of the Currency (OCC) warned in its semiannual risk survey that virtual currencies "enable anonymity for cyber criminals, including terrorists and other groups seeking to transfer and launder money globally," which in turn creates significant challenges for BSA and anti-money laundering compliance.[75]

3.3 Potential Operational and Legal Risks

In the financial regulatory world, clearing intermediaries fall within a category of regulated entities called financial market infrastructures ("FMIs"). "The Federal Reserve, consistent with standards set by the G20 and Financial Stability Board, defines FMIs as 'multilateral systems among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions,' which 'include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories.'"[76]

FMIs, and payment systems generally, face numerous risks, including "credit risk, liquidity risk, operational risk, and legal risk." Operational risk is defined by the Federal Reserve as "'the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the [financial market infrastructure] … include[ing] physical threats, such as natural disasters and terrorist attacks, and information security threats, such as cyberattacks. Further, deficiencies in information systems or internal processes include errors or delays in processing, system outages, insufficient capacity, fraud, data loss, and leakage.'"[77] FMIs subject to the

---

[74] Consumer Advisory, *Risks to consumers posed by virtual currencies*, Consumer Financial Protection Bureau (August 2014), *available at* http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

[75] Semiannual Risk Perspective, National Risk Committee, Office of the Comptroller of the Currency, p. 8 (Spring 2016), *available at* http://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2016.pdf.

[76] Walch, Angela, "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk," Journal of Legislation and Public Policy, Vol. 18:837, page 851-852 (quoting Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. 67326, 67333 (Nov. 12, 2014)).

[77] Walch, page 853 (quoting Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. at 67334 n.8.).

Federal Reserve's regulatory oversight are only those that "'expect to settle a daily aggregate gross value of U.S. dollar-denominated transactions exceeding $5 billion on any day during the next 12 months.'"[78]

Blockchain's operational risks stem from the following: "(i) software has bugs, (ii) software is vulnerable to attack; (iii) software is ever-changing through new releases; and (iv) few people understand how software works.[79] Although all software has bugs, it could be valuable to compare the bugs in existent central clearing software against those present in Blockchain software.[80] Because software is vulnerable to attack, "the effects of such an attack could be to revise recently settled transactions on the Blockchain and to prevent current and future transactions from being completed." "Any ability to tamper with it [Blockchain] or to manipulate its creation is highly damaging to the reliability of the system, and therefore to its credibility as an [FMI]."[81] "The evolving nature of software through new releases may be a bigger problem for decentralized [Blockchain] than it is for more centralized [FMIs]. Since controversial new releases of [Blockchain] software may be unevenly adopted, there would seem to be potential for periodic forks in the network when consensus cannot be found amidst the parties in the network. In a centralized FMI, however, or even in 'permissioned Blockchains,' new releases of software can likely be implemented more easily, since adopting the new version can be mandated on participants, perhaps through the contract that allows participation in the permissioned Blockchain."[82] Finally, "the fact that only a very limited portion of the population truly understands how [Blockchain] operates gives rise to systemic operational risks. This is because it requires the population to put extreme amounts of trust in the skill and integrity of the people making decisions about the Blockchain code and network. The larger the system becomes, with more 'Blockchain' companies using the Blockchain network to accomplish their tasks, the more pressure that is put on this small group of experts to make desirable policy choices that they implement accurately and safely into the code. We should proceed with caution in building complex, opaque systems that carry out tasks of significant systemic importance."[83]

Blockchain's decentralized structure presents additional operational risks. "There is no one who is responsible for keeping the Blockchain software operational. This means that even if there is a crucial repair that is needed to prevent complete collapse of the software, no one in particular would be required to perform the repair. Since no one is 'responsible' for the code, even those core developers who have been voluntarily working to maintain [Blockchain] may decide not to help in a moment of crisis, perhaps deeming their continued involvement to be personally risky."[84] "In addition, decision-making may be slower than it needs to be to resolve an operational crisis, due to the fact that no one is in charge of [Blockchain]. As there is no defined power or accountability structure, no one has to listen to anyone else's ideas about how to resolve a crisis." Due

[78] Walch, page 854 (quoting Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. at 67335).
[79] Walch, page 856.
[80] Walch, page 859.
[81] Walch, pages 861-62.
[82] Walch, page 867.
[83] Walch, page 868.
[84] Walch, page 870.

to lack of authority, "anyone with a suggested resolution to a crisis may merely propose a solution, but it may take too long to achieve buy-in from other members of the [Blockchain] community to successfully implement the solution in an emergency situation," as well as in any other situation in which the voice of Blockchain needs to be heard.[85] "Maintaining the functionality of [FMIs] is hugely important, and having no one specifically tasked with the responsibility for achieving this for [Blockchain] is a significant risk."[86] "The operation of [FMIs] is critical to financial stability, hence their strict regulation, which includes both governance and risk management requirements."[87]

4. CONCLUSION

With financial technology start-ups continuing to develop smart contracts for financial transactions, securities and derivatives regulators will ultimately need to formulate an approach for regulating their use. Several regulators have already signaled their intention to examine the use of Blockchain technology in the financial sector and while smart contracts are potentially attractive to regulators since they increase transaction security and reduce the risk of manipulation, their implementation may raise difficult legal and regulatory challenges.

There certainly needs to be global technological and commercial Blockchain standards, to create and enhance the coherent development and prevent potential future misuses of Blockchain technology and digital currencies.

There are different infrastructures, protocols, technologies, regulations, use cases, jurisdictions, opinions and long term direction views associated with Blockchain. As a result, there is the potential of parallel but inconsistent development of the technology, use cases and possibly regulation of digital currencies and Blockchain technology, which could result in a fragmented space. Further, there is the potential negligent or malicious misuse of the technology and its applications.

Effective governance is the key to the successful implementation and proliferation of Blockchain, while enhancing the resilience of the system to systemic privacy and cybersecurity risks. Ultimately, protecting participants, investors, stakeholders, and consumers.

Blockchain technology is a nascent technology that is evolving every day. It holds huge transformative potential in a wide ranging number of fields and "could transform how our economy works"[88]. Similar to other new technologies, to realize its full potential, blockchain will be developed through numerous iterations and will inevitably go through trials, evolution, failures and ultimately widespread adoption. The challenge will be to

---

[85] Walch, page 871.
[86] Walch, page 874.
[87] Walch, page 880.
[88] The Economist – The Promise of the Blockahin, http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

strike the right balance between ensuring the governance, safety and resilience of the system while not infringing on the innovation and development of this fast evolving technology.