IP, Information & Innovation

White Paper

Beyond Bitcoin: Blockchain

The Essential Building Block in Designing the Future

区块链：超越比特币

Reed Smith 律师事务所白皮书

全书主要有 **8** 个章节

1. 比特币基础知识
2. 区块链基础知识
3. 美国各州及联邦的监管政策
4. 国际监管政策（欧洲、亚洲、美洲及非洲）
5. 比特币及区块链相关商业的保险
6. 资本市场的应用
7. 知识产权
8. 对社会的影响

ReedSmith

The business of relationships.

IP, Information & Innovation

White Paper

Beyond Bitcoin: **Blockchain**

The Essential Building Block in Designing the Future

Contents

The Mysterious Origins of Bitcoin

Introduction

Though the following chapters are mostly devoted to informing and enlightening the reader about the potential of cryptocurrency and the underlying blockchain technology, the origins of these developments are somewhat shrouded in mystery.

Halloween 2008 may have been a particularly frightening one, as the world economy was facing its most dangerous crisis since the Great Depression. Yet, it also happened to be the day that Bitcoin, the most widely used cryptocurrency to date, was introduced in a rather simple and unassuming email to several hundred members of an obscure mailing list comprising cryptography experts and enthusiasts.

The sender, known only as Satoshi Nakamoto, wrote: "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party," followed by directions to the link http://www.bitcoin.org/bitcoin.pdf, a nine-page white paper about a peer-to-peer trustless system of digital "currency" that purports to solve the problem of double-spending.

After first becoming operational in January 2009, Bitcoin and its related progeny have exploded in just a short number of years. Exactly seven years after the initial enigmatic email was sent, the October 31, 2015, cover of *The Economist* featured an article on the blockchain (the technology underlying Bitcoin), dubbing it "the trust machine." Blockchain technology, which is described below, provides a cryptographically secured ledger that can be examined by all authorized parties, but cannot be changed.

Though Nakamoto initially collaborated with developers on what has been called a revolutionizing innovation, his participation ended in mid-2010, and in April 2011, he completely disappeared with the final words, "I've moved onto other things."

Though we may never uncover the originator of Bitcoin, we are left with a rapidly developing open source technology that continues to find increasing mainstream acceptance and simply cannot be ignored.

In fact, we have seen every sign that blockchain technology will be widely adopted in various industries. For example, the Hyperledger Project provides open source blockchain software that can be adapted to various applications. Intel has joined IBM, Digital Asset Holdings, and others in providing code and support for this project. Also, Digital Asset Holdings has collaborated with the Depository Trust and Clearing Corporation (DTCC) to test and build a blockchain-type distributed ledger to track and settle financial assets. The R3 consortium is a group of FinTech companies and large banks that are developing a distributed ledger customized for financial institutions.

The blockchain has also garnered the attention of government agencies and regulators, of course. For example, the U.S. Office of Comptroller of Currency (OCC) has released a white paper posing an approach to handling how banking institutions should experiment with new technologies such as the blockchain. As discussed below, regulators in other countries and the European Union are also paying attention.

The application of the blockchain is anticipated to extend far beyond financial services to include various applications of authentication and data storage. Potential applications of the blockchain include real property records, digital content ownership verification, and business process management.

Bitcoin 101 – A Primer

Cryptocurrencies[1] have gained significant attention since the introduction of Bitcoin in 2009. They offer a new medium of exchange created by and for the Internet that could potentially democratize the very idea of money itself. The following is a short primer on bitcoin's underlying technology[2] and a breakdown of a sample bitcoin transaction. Armed with this understanding, we can more clearly see the potential impact, issues, and opportunities presented by Bitcoin, similar cryptocurrencies, and the underlying blockchain technology.

Bitcoin became the first decentralized cryptocurrency, from which hundreds more cryptocurrencies have been derived. Essential to its operation are two underlying technologies: public key cryptography and peer-to-peer networking.

- **Public key cryptography** is the use of digital signatures to secure information. These signatures consist of a public key, which is known by everyone, and a private key, known only by its owner.
- **Peer-to-peer networking** is a way to organize the flow of information among equal participants on a network, rather than relying on a central authority.

Bitcoin secures transactions between currency users with digital signatures and then requires verification over a peer-to-peer network. Thus, when spending bitcoins[3], you sign the transaction with your private key to prove you own the bitcoin you want to spend. Then, your public key and the details of the transaction are published to a public ledger so that everyone knows that your bitcoin has changed hands. This public ledger is constantly being verified by the members of Bitcoin's peer-to-peer network to ensure that each bitcoin is spent only once and is held by its verifiable owner. As such, Bitcoin replaces trust with mathematical proof and accountability among currency users themselves, thereby doing away with a central authority to monitor the currency, or trusted third parties to clear transactions.

Unlike a digital file on your computer, a bitcoin cannot be copied and pasted infinitely. It can only be transferred, and transferred only once, by signing the transaction with your private digital key and recording the transaction on a shared public ledger.

Not only did Bitcoin solve the so-called "double spending" problem, where currency risked being spent more than once without the involvement of a middleman, but just as importantly, Bitcoin, owing to this middleman elimination, cut down the time required to verify and finalize transactions from what can take several days in a traditional system, to a matter of minutes – thereby enabling significant efficiencies and the growth of tremendous opportunities.

The Blockchain

Bitcoin relies on its peer-to-peer network to do two things: maintain the authoritative ledger of transactions and issue new currency. To understand how this works, we must briefly explain the bookkeeping algorithm behind Bitcoin, known as the blockchain[4]. The blockchain is a decentralized ledger that records information about transactions occurring in real time in "blocks" that are linked together through a secure mathematical function, thereby forming a chain of records (hence the name blockchain).

To add a new block of records to the blockchain, someone must discover the mathematical key (called a "nonce") that will fit the next block of records into the chain. This is done by making millions upon millions of guesses (done by computers), the process of which is called "mining" and is done by participants on the Bitcoin network. Once discovered, the nonce must also be double-checked by other users in order to be verified.

Mining secures the ledger, because once a block of records is added to the blockchain, the transactions recorded are considered final. In order to tamper with those records, a fraudster would have to re-discover the proof that allowed the records to be added in the first place. This is very unlikely for two key reasons. First, the Bitcoin network is built to adjust the difficulty (up or down) of finding the key, based on the amount of computing power on the network, to ensure that just the right amount of work is necessitated for mining so that it is neither too hard (thereby requiring too much time), nor too easy. Second, the Bitcoin network is designed to follow only the longest chain of blocks. This means that in order to go back and tamper with the ledger, you would have to find the key for the block you want to change *and any others that were found after it* in order to replace the longest chain. The computational difficulty of that task is so high that most bitcoin transactions are considered verified after six blocks are added to the network (which takes one hour on average).

So why do miners dedicate computing power to finding mathematical keys to verify bitcoin transactions? The answer lies in how new bitcoins are issued. Rather than relying on a central bank or other authority, the Bitcoin network itself creates new bitcoins as a reward for

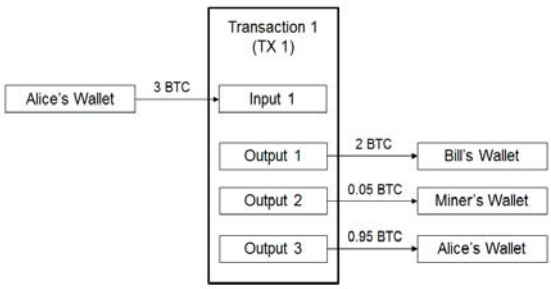
miners who successfully find the next key. The miner who successfully creates a block of records receives a set reward of new bitcoins, plus any transaction fees attached to the transactions that the block records. This incentive has led to the creation of large bitcoin mining pools and other organizations dedicating raw computing power to claim new bitcoins, while at the same time securing Bitcoin's ledger.

A Bitcoin Transaction

It would be illustrative to follow one bitcoin transaction from beginning to end to see how all the pieces fit together[5]. Say Alice, who owns three bitcoins, wants to send Bill two bitcoins. She would go to her digital "wallet," which is a program or online service that stores the keys that Alice needs to access her bitcoins. Alice puts in the address for Bill's digital wallet, which is a 27-34 character code. She knows that the Bitcoin network tends to prioritize recording transactions that include a fee, so she offers 0.05 bitcoins to the miner who records her transaction.

Alice's digital wallet creates a data packet containing Bill's wallet address, the number of bitcoins to be sent, the 0.05 transaction fee, and Alice's digital signature. This data packet is propagated through the Bitcoin network. It will flow in Bitcoin's peer-to-peer network, from one computer to another, until each member knows of the pending transaction (this will usually take less than a minute).

Within about 10 minutes, a miner finds the right nonce to record the next block of transactions. This miner prefers transactions with fees attached, so Alice and Bill's transaction is at the top of the queue to record. The new block of records contains the solution to the block, a reference to the prior block in the blockchain, and a list of all transactions, now time-stamped, that the block records, including Alice and Bill's.



Note that the transaction now has one input and three outputs. The input is Alice's original wallet address of three bitcoins. The three outputs are: (1) the two bitcoins going to Bill, (2) the 0.05 bitcoins going to the solver of this block, and (3) a new public key for 0.95 bitcoins going back to Alice as the change for the transaction. This new address is added to Alice's digital wallet, and is associated with her private key indicating Alice's ownership.

Now that the transaction is recorded in a block, it will soon be considered final. The new block of records is broadcast to the Bitcoin network. The transaction becomes final as more and more blocks are found with this transaction included. This will inevitably occur because the probability that there is a competing chain with more work performed on it falls to zero. As long as it appends to the longest confirmed blockchain, it is now considered a part of Bitcoin's ongoing ledger.

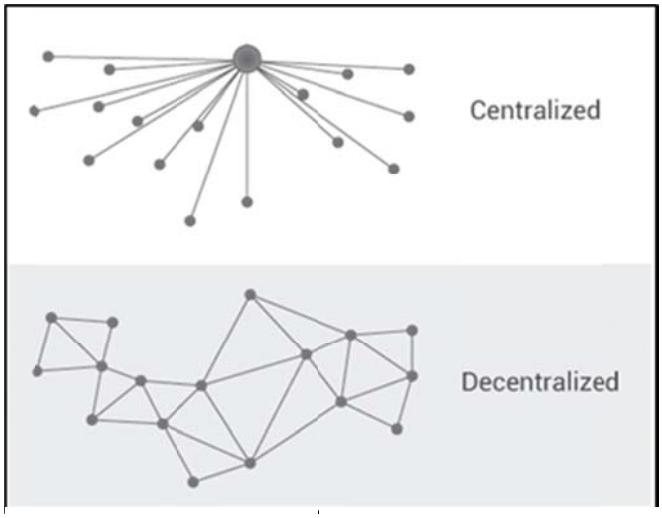
In order for Alice and Bill to be satisfied that the transaction is confirmed, they will typically wait for five more confirmations to reduce the probability that a fraudulent miner recorded or changed a block. This confirmation will normally happen within an hour. Once it does, Alice and Bill's digital wallet programs will alert them that the transaction is confirmed, and they can be confident that they can spend their new bitcoins.

Summary

Bitcoin and other decentralized cryptocurrencies eliminate the middleman that verifies transactions and controls currency. Thanks to ongoing development by a dedicated online community, this technology has spawned new types of businesses, new channels of commerce, and a renewed discussion over how the Internet impacts economies across the globe. However, bitcoin as a currency is merely the tip of the iceberg of what the blockchain has to offer.

Blockchain 101

The blockchain is a cryptographically secured database of a continuously growing list of data records that is shared by all parties participating in an established, distributed network of computers. What makes blockchain interesting is that it is a trustless system. That is, the blockchain makes it possible for participants that are not necessarily known to each other to transfer a digital asset without the requirement of any third-party validation. This chapter discusses in greater detail how the blockchain algorithm works to help you consider its greater potential.[6]



Adapted from Ioptio:
https://github.com/ioptio/design/blob/master/networks/networks.png

How It Works

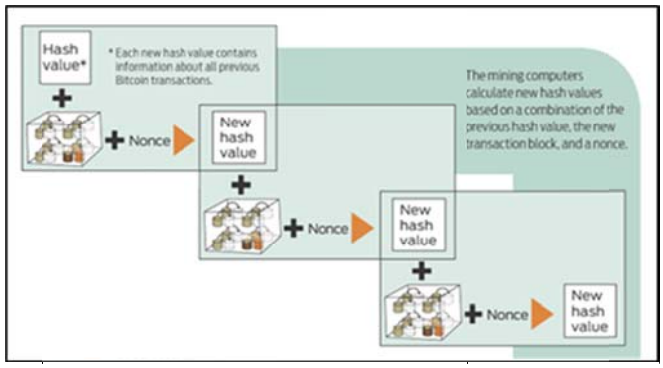
A **blockchain**[7] is nothing more than a digital record, or ledger, of transactions. Unlike a traditional ledger, however, a blockchain is stored collectively by all of the participants on its network. Each transaction is stored with others in a unit of data called a **block**, and, as the name "blockchain" suggests, those blocks securely link to one another, forming a "chain" of records going all the way back to the very beginning of the ledger.

To participate in a blockchain network, a user must operate a software client that will connect them to that blockchain. The software client allows the user to record transactions, and also lends computing power to the network to help build new blocks of records.

Participants build new blocks of records by investing computer time to solve complex mathematical problems. These new records are only added to the ledger when a majority of participants have double-checked the work of the person who wants to add it. What this means is that Blockchain does not rely on trust; instead, confirmation of transactions is done by **consensus**.

When a user wishes to transfer a digital asset to another user, the users broadcast cryptographically secured digital signatures and the details of their transaction to nearby peers on the network. The users are identified in the transaction by their public keys; this is termed "pseudonymity." When a peer participant solves the mathematical puzzle required for the next block, these pending transactions may now be recorded into a block. That new block is then double-checked by other members of the network until a majority agrees that it is correct. Once a majority consensus is achieved, the new block is added to the chain and the pending transactions are recorded in the ledger.

When a user wishes to transfer a digital asset to another user, the users broadcast cryptographically secured digital signatures and the details of their transaction to nearby peers on the network. The users are identified in the transaction by their public keys; this is termed "**pseudonymity**." When a peer participant solves the mathematical puzzle required for the next block, these pending transactions may now be recorded into a block. That new block is then double-checked by other members of the network until a majority agrees that it is correct. Once a majority consensus is achieved, the new block is added to the chain and the pending transactions are recorded in the ledger.



Adapted from the IEEE:
http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg

Though the above summary is actually a simplification of the process, this is how blockchain allows a network of strangers to collectively maintain an accurate ledger of secure online records for any type of transaction, without the need for a trusted third party to act as a middleman.

As time goes on, more and more blocks of records are added to the blockchain, each one securely referencing the next. This is important because if someone wanted to go back and change a transaction on the ledger – to cook the digital books – she would not only have to re-solve the mathematical puzzle allowing her to create a fraudulent block, but she would also have to re-solve every subsequent block in the blockchain. Even worse for the fraudster, she would have to convince a majority of network participants to accept these fake blocks before the next legitimate participant added the next real block. The sheer volume of work and speed required make it extremely difficult to alter transactions on a blockchain. This means that after a certain number of new blocks are added, the parties to a transaction can be well-assured that the transaction is considered final – not only by them, but also by the entire community of participants on the network. It is precisely this assurance that allows blockchain participants to trust the ledger itself, even though they do not necessarily trust (or know) their fellow participants on the network.

Advantages of Blockchain

Distributed ledgers like Blockchain solve important problems in Internet commerce. Chief among them is the problem of double spending, where two transactions draw upon the same underlying asset. By requiring every transaction to be at least partly public, distributed ledgers dramatically increase counterparty trust. Moreover, because Blockchain requires **proof of work** and consensus to record new transactions, it is very difficult for fraudsters to tamper with digital records to steal or re-spend assets.

Blockchain also helps achieve certainty in the concept of digital ownership itself. A consummate problem with digital information is that it is freely transferable and may be copied. This means that possession cannot be equated with ownership. Merely having a copy of a file does not include the right to exclude – a touchstone right built into the concept of property. Distributed ledgers like blockchain make proving the ownership of a digital asset more like performing a real property title search. Like the grantor-grantee index in land records, the blockchain records every transaction involving a particular digital asset. The advantage of blockchain over other forms of exclusive digital ownership, like encryption at rest,[8] is that there is always a record that reflects not only the current possession of the asset, but also the history of rightful ownership going all the way back to the digital asset's creation.

Disadvantages of Blockchain

Like all technical solutions, the blockchain algorithm reflects certain tradeoffs. Because of latency and scalability issues, many current blockchain applications put severe limits on the size of each new block of records. This limits the frequency with which a blockchain network can process transactions. For example, the Bitcoin network can only process seven payments per second, while major credit card providers can handle more than 1,400. Designers of applications that leverage blockchain should carefully consider factors such as block size, the proof of work required to verify blocks, and the expected number of participants on a blockchain, to ensure the ledger operates efficiently and effectively.

Blockchain relies heavily on public key cryptography to identify users and permit access to assets tracked through the ledger. For this reason, key security is of increased concern. If a user's private key is lost or stolen, the user has lost access to his or her assets on the blockchain forever. For example, as many as 4 percent of bitcoins have been rendered permanently ownerless because users have misplaced their digital keys. Future applications of blockchain, especially in private or semi-private contexts, should consider employing multi-factor authentication or digital certificates to safeguard the cryptographic keys used to identify rightful owners and permit access.

While smaller blockchain networks may offer more technical security options, they are not necessarily safer. Organizations that host private or semi-private blockchains should especially consider the possibility of so-called "51% attacks," where the majority of the network's mining hashrate is concentrated in a single entity, thereby allowing that single entity to manipulate the public ledger at will. In addition, the pseudonymous nature of blockchain transactions can make fraud detection and collusion between users more difficult to detect. Carefully consider the sensitivity of information stored in a distributed ledger, the type and number of network participants, and the incentives for fair play on the network.

Summary

The blockchain algorithm is an important contribution to the foundational technologies we use to store and secure information. It addresses particular problems with counterparty trust and digital asset ownership. While not a panacea, the blockchain algorithm presents exciting opportunities in how we store and share information securely online. Many commentators posit that the invention of the blockchain will be remembered in the same vein as the invention of the World Wide Web or email.[9] As a foundational technology, the blockchain could one day be a major part of how we store and transmit electronic information itself.[10] The opportunity is wide open for innovators to apply blockchain across the digital landscape. Armed with an understanding of how the blockchain works, you can be a part of that conversation.

U.S. Regulatory Landscape

In the United States, it is currently legal to transmit, mine, and develop cryptocurrencies, such as Bitcoin. It is also generally legal to use cryptocurrencies to purchase goods and services, or for investment purposes. However, with their dramatic increase in prevalence and overall use, cryptocurrencies have become the target of regulations issued by both the federal and state governments. The increase in regulatory oversight has been particularly significant during the past year.

One state, New York, has already issued regulations explicitly subjecting those engaging in virtual currency-based business activities to licensing, supervision, and other compliance requirements. In addition, various federal agencies have provided guidance that certain virtual currency-related activities may be subject to already-existing regulations, such as those governing money transmission.

Furthermore, several agencies have initiated enforcement actions against businesses and individuals related to cryptocurrency activities. The focus of these regulations tends to be on virtual currencies themselves and their transmission, as opposed to the pure development of cryptocurrency technology and software. For example, the New York BitLicense regulations explicitly provide that those who only develop virtual currency software and technology are not subject to licensure.

These recently promulgated regulatory regimes, along with the guidance provided by other agencies clarifying the application of already existing regulations to virtual currency-related activities, have major implications to companies engaged in virtual currency activities from a licensing, supervision, compliance, and cost perspective. Undoubtedly, with the sustained growth of cryptocurrency, governments will continue to adapt, and one can expect additional regulations from governmental authorities within the coming years.

State Regulation

New York: The BitLicense Regime

Led by former Superintendent of Financial Services Ben Lawsky, New York state has been at the forefront of virtual currency regulation since 2014. In July 2014, through its Department of Financial Services ("NYDFS"), New York became the first state to propose a comprehensive regulatory regime governing virtual currency business activities.[11] And on June 3, 2015, following comments from numerous interested parties, New York became the first state to implement a comprehensive virtual currency regulatory regime – popularly known as "BitLicense."[12]

As of September 2015, NYDFS has already received 25 initial BitLicense applications.[13] Recently, NYDFS issued the first license under the BitLicense regime to Circle Internet Financial, a Bitcoin wallet and creator of the app Circle Pay.[14] However, the BitLicense regulations have been divisive, and some have criticized the burdens that it places on virtual currency-related businesses. As a result, some companies have attempted to block users from New York in an attempt to avoid falling under the BitLicense regulations.[15]

Under the BitLicense regime, companies engaged in "virtual currency business activities" Under the BitLicense regime, companies engaged in "virtual currency business activities" are required to undergo a thorough application process, obtain a license, abide by numerous compliance requirements similar to banks and other financial institutions, and be subject to examinations by NYDFS.

Who Must Obtain a License?

Under BitLicense, a "virtual currency" is a digital unit that is a digital medium of exchange or form of stored value, with specific exceptions for prepaid cards, customer rewards programs, in-game currency and reward points.[16]

Companies that conduct "virtual currency business activities," as defined in the BitLicense regulations, and that operate in New York, or engage in business with New York customers, are subject to the BitLicense regime.[17]

Under BitLicense, the following five activities constitute "virtual currency business activities":

- Receiving virtual currency **for transmission or transmitting** virtual currency through a third party
- **Maintaining custody** of virtual currency or holding virtual currency on behalf of others
- **Buying or selling** virtual currency **as a customer business**
- Performing virtual currency **exchange or conversion services** (whether converting virtual currency to fiat currency or vice versa; or converting one type of virtual currency for another type of virtual currency)

- **Controlling, administering, or issuing virtual currency**[18]

BitLicense exempts several activities from licensure. For example, cryptocurrency mining on its own would not subject a party to the BitLicense regime.[19] Similarly, consumers or merchants only using virtual currency to buy or sell goods or services would not be required to obtain a license.[20] And finally, parties who engage purely in software development and dissemination do not fall under BitLicense.[21] However, there are many unanswered questions as to the particular circumstances in which various exceptions would apply. For example, BitLicense exempts from licensure the transmission of "nominal amounts" of virtual currency for "non-financial purposes."[22] Some have surmised that this would allow for transmission of nominal amounts of cryptocurrency for purposes of, for example, identity verification. However, it is less clear whether this exception would apply to the use of a nominal amount of cryptocurrency to create a "digital contract." Likewise, there are several gray areas as to whether certain businesses are engaged in one of the five "virtual currency business activities," or mere software development.

Application and Licensing Process

The BitLicense application and licensing process is extensive, and is similar to the licensing required for other types of financial institutions chartered in New York. Applicants must pay a $5,000 application fee, and submit to NYDFS extensive biographical, historical, financial, and business information about the applicant, its principal officers, and its principal stockholders.[23] Under BitLicense, NYDFS must approve or deny applications within 90 days of deeming the application complete.[24] However, in practice, the regulators can also ask for more documentation, and likely often will as is the case with other financial regulatory licensing. Further, the superintendent may also extend the 90-day window in certain cases.[25] Therefore, as with the licensing process for other financial institutions, the BitLicense application will likely be time- and cost-intensive.

NYDFS may also issue conditional licenses under BitLicense for those applicants that do not comply with all BitLicense requirements upon licensing.[26] This conditional license is valid for two years. However, the conditional license may be issued subject to reasonable conditions imposed by NYDFS, and the licensee may be subject to heightened scrutiny, review, and examination.

Licensees must also obtain NYDFS written approval to offer any materially new product, service, or activity, or to make a material change to an existing product, service, or activity.[27] Finally, NYDFS has the authority to suspend or revoke both full and conditional licenses on several grounds, including on any ground that the superintendent may refuse an initial license, for violation of any provision of BitLicense, good cause, or for failure to pay a judgment.[28]

AML, KYC, Compliance Issues, and Examinations

Perhaps the most significant BitLicense provisions are the numerous ongoing compliance provisions that the NYDFS requires of licensees. Many such compliance regulations are similar to those required of New York-chartered banks and other types of financial institutions.

Licensees under BitLicense must maintain a comprehensive anti-money laundering (AML) policy.[29] This policy is subject to both an initial risk assessment and ongoing annual risk assessments.[30] Licensees must adopt internal controls and policies to ensure AML compliance, including appointing a dedicated compliance officer and subjecting the policy to review and approval by the licensee's board of directors.[31] The policy must be subject to annual independent testing, and the audit report must be submitted to NYDFS.[32]

The AML provisions also include numerous additional know-your-customer ("KYC") requirements similar to those in existence for other financial institutions, or for money transmitters under FinCEN regulations.[33] Licensees must identify and verify customers' identities, check customers against the list of Specifically Designated Nationals maintained by the Office of Foreign Assets Control ("OFAC"), and maintain customer records.[34] Licensees are also required to submit to NYDFS suspicious activity reports ("SARs") and currency transaction reports for transactions in cryptocurrency of more than $10,000.[35]

Additional compliance regulations promulgated by the BitLicense regime include those addressing a licensee's:

- Capital requirements[36]
- Custody and protection of assets[37]
- Books and records[38]
- Consumer protection disclosures[39]
- Consumer complaint policies[40]
- Advertising[41]
- Anti-fraud policies[42]
- Cybersecurity programs[43]
- Business continuity and disaster recovery plans[44]

Under BitLicense, licensees are subject to at least one examination by NYDFS every two years.[45] Licensees

must also submit numerous financial statements and reports to NYDFS on a quarterly and annual basis.[46]

Conference of State Bank Supervisors

On September 15, 2015, the Conference of State Bank Supervisors issued a model licensing regime as a guide to states in regulating virtual currency. The Conference recommends that companies involved in the exchange and transmission of virtual currencies and "services that facilitate the third-party exchange, storage and/or transmission of virtual currency (e.g. wallets, vaults, kiosks, merchant-acquirers, and payment processors)," be supervised and licensed by state banking regulators.[47] "Virtual currency" is defined here as a digital representation of value used as a medium of exchange, unit of account, or store of value, but which does not hold legal tender status. Virtual currency would not include the software or protocols governing transfer.[48]

Other State Proposals

Following New York's lead, other states have made various proposals to implement virtual currency regulations within the past year.

Perhaps most prominently, in June 2015, the California House of Representatives passed AB-1326.[49] The bill, introduced in February 2015, would provide for a similar, but not quite as extensive, licensing regime to New York's BitLicense.[50] Like BitLicense, AB-1326 would provide that virtual currency businesses could not operate unless licensed by the California Department of Business Oversight. The proposal also calls for capital requirements and an extensive application process. However, the California proposal would be more relaxed than BitLicense in certain areas: for example, it would not require submission of state-level SARs and would contain less stringent AML requirements. As of September 2015, AB-1326 stalled in the California Senate and is no longer listed as an active bill; however, it could be revived on a future date.[51]

At least three states have issued guidance as to how state law, particularly concerning money transmission, applies to virtual currency transactions. Washington state has concluded that virtual currency is included in the definition of "money transmission" in its Uniform Money Services Act.[52] However, both Kansas and Texas have concluded that virtual currency does not constitute money under its money transmission laws, and therefore, the two states' respective money transmission laws generally do not apply to virtual currency transactions; the one exception may be where the acts may apply is transactions in which virtual currency is exchanged for sovereign fiat currency through a third-party exchange site.[53]

New Jersey, Connecticut, Pennsylvania, North Carolina, Utah, and New Hampshire have also made various virtual currency regulation proposals; however, none has been adopted as of this writing.[54]

Federal Regulation

Unlike New York state, federal agencies have not yet issued specific sets of regulations specifically addressing virtual currency. However, in recent years, agencies have clarified that certain laws and regulations already in existence may apply equally to activities and transactions involving virtual currency as to those involving traditional fiat currency. Two of the agencies whose regulations may most impact virtual currency businesses include the Commodity Futures Trading Commission ("CFTC") and Financial Crimes Enforcement Network ("FinCEN").

Commodity Futures Trading Commission ("CFTC")

On September 17, 2015, the CFTC confirmed that it would treat bitcoin and other virtual currencies as "commodities" for regulatory purposes under the Commodity Exchange Act ("CEA") and other CFTC regulations.[55] Under the CEA and its regulations, the CFTC may assert jurisdiction over the trading of futures, options, and swaps on "commodities."[56] The term "commodity" is defined broadly to include "goods and articles…and all services, rights and interests…"[57] The CFTC's determination came in the form of a settlement order against Coinflip, Inc., which is discussed in more detail below. The decision to treat virtual currencies as "commodities" under the CEA and CFTC regulations confirms prior informal guidance provided by CFTC Chairman Timothy Massad and other CFTC officials, who had commented in testimony and speeches that the CFTC would be able to assert jurisdiction over virtual currencies.[58] The order also appears to confirm that the CFTC would only treat virtual currency as a "commodity," and that it would *not* treat virtual currency as "currency"; and therefore virtual currencies would not be subject to certain regulations governing foreign exchange derivatives.[59]

The treatment of virtual currency as a "commodity" carries significant implications for businesses that engage in the trading of virtual currency-based derivatives. Such firms that come under the CFTC's jurisdiction may have to register with the CFTC, and could be subject to regulation by the CFTC and/or the National Futures Association. This supervision will undoubtedly subject the firms to numerous regulatory obligations. As a result of the CFTC's September 2015 settlement with Coinflip, almost any business whose business activities involve virtual currency-based derivatives will need to assess whether it is required to register with the CFTC and may be subject to CFTC regulation. Two such businesses might include firms running trading platforms

involving virtual currency-based derivatives, or firms providing advisory services concerning virtual currency-based derivatives.

Financial Crimes Enforcement Network ("FinCEN")

Like the CFTC, FinCEN has not issued any regulations directly addressing virtual currency. However, businesses engaged in virtual currency activities may come under the purview of FinCEN's regulations concerning money services businesses ("MSBs"). Under FinCEN regulations, MSBs include "money transmitters."[60] In 2011, FinCEN opened the door to regulation of virtual currency businesses as money transmitters – and therefore MSBs – when it revised the definition of "money transmission services" to include "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[61] Therefore, any party that engages in the transmission of virtual currency must abide by FinCEN's MSB regulations, just as if the business transmitted traditional currency.

The implications for being deemed a money transmitter and MSB are significant. MSBs must comply with numerous AML requirements, including implementation, adoption, and maintenance of an AML program; independent review of such AML program; filing of SARs and currency transaction reports; and maintenance of records.[62] Further, MSBs must register with FinCEN. It is a federal crime to knowingly conduct an MSB while failing to register with FinCEN (or state licensing money transmission licensing agencies).[63]

Starting in 2013, FinCEN has issued guidance clarifying what types of virtual currency activities could trigger treatment as an MSB by FinCEN. In March 2013, FinCEN provided three types of parties that may engage in virtual currency activities:

- **Users** (those who use virtual currency to purchase goods or services)
- **Exchangers** (those providing for the exchange of virtual currency for real currency, funds or other virtual currency)
- **Administrators** (those issuing virtual currency, or with the authority to redeem virtual currency)[64]

FinCEN concluded that, broadly speaking, users of virtual currency would not be considered MSBs, but that exchangers and administrators **would** fall under the MSB regulations.[65]

Since then, FinCEN has provided additional guidance as to what types of activities may trigger regulation. FinCEN has issued various guidance providing that it would not view the following activities as subjecting a party to MSB regulations:

- Mining virtual currency[66]
- Use of virtual currency to purchase goods and services[67]
- Conversion of virtual currency to fiat currency for one's own use[68]
- Investing in virtual currency for one's own account[69]
- Renting out of computer systems and software that mine virtual currency to third parties (where any virtual currency mined by the third party using the software would remain the property of that third party)[70]

Many of the above were deemed not to constitute the activities of an MSB because they were performed for one's own account; however, as soon as such activities were performed by or on behalf of a third party, the analysis could change.

On the other hand, FinCEN has confirmed that the following activities would constitute engaging in business as an MSB:

- Maintaining a trading system to match offers to buy and sell virtual currency for fiat currency[71]
- Maintaining a set of book accounts where customers may deposit virtual currency[72]
- Developing and maintaining a system to provide virtual currency payments to merchants in the United States and Latin America wishing to receive payment for goods/services sold in a currency other than that of legal tender[73]
- Conducting Internet-based brokerage services between buyers and sellers of precious metals, in which buyers pay sellers directly by check, wire, or bitcoin; and the entity uses the bitcoin blockchain to transfer previous metal ownership by issuing a digital certificate. The customer could then later exchange its holdings using the bitcoin blockchain ledger.[74]

Other Federal Agencies

Numerous other federal agencies have also issued guidance on virtual currency or issued consumer advisories, although not as significant as the CFTC's or FinCEN's interpretations. For example, the Securities and Exchange Commission ("SEC") has issued guidance stating that, even if it does not consider virtual currencies to be "securities," it may still invoke its enforcement authority to prosecute virtual currency-based Ponzi schemes and other fraud – which it has already done.[75]

The Internal Revenue Service has concluded that cryptocurrency should be considered "property" under the Internal Revenue Code, and thus transfers involving virtual currencies would be taxable events.[76]

Other agencies issuing guidance and consumer advisories include the Consumer Financial Protection Bureau, Board of Directors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Federal Trade Commission, and FINRA.

Enforcement

Over the past several years, various federal agencies have stepped up their enforcement of virtual currency-related activities. Although no federal agencies have yet issued virtual currency-specific regulatory regimes, such as New York's BitLicense, the agencies have prosecuted numerous individuals applying existing laws to virtual currency-based activities. In some cases, these enforcement actions have been precedent-creating, such as the settlement agreement between Coinflip and the CFTC, in which the CFTC confirmed its interpretation that virtual currencies constituted "commodities" under the CEA.

Some examples of key enforcement actions include the following:

CFTC

On September 17, 2015, the CFTC settled an enforcement action against Coinflip, Inc. and its chief executive officer. Coinflip operated an online facility called Derivabit that matched buyers and sellers of bitcoin option contracts. The CFTC found that Coinflip was operating a facility for trading commodity options in violation of the CEA and CFTC regulations, including by operating the facility without having registered with the CFTC. Although the Order did not carry any monetary penalties, this enforcement action was especially significant because, through the Order, the CFTC established that it considered virtual currencies to be "commodities" under the CEA, and thus could exercise jurisdiction over various virtual currency-related derivatives.[77]

FinCEN

On May 15, 2015, FinCEN issued a $700,000 civil monetary penalty against Ripple Labs, Inc. for willful violations of the Bank Secrecy Act regulations. Specifically, FinCEN accused Ripple of acting as a money services business by selling virtual currency. However, Ripple did not register with FinCEN, failed to implement appropriate AML programs, and failed to report suspicious activities, among other violations.[78]

SEC

In September 2014, the United States District Court for the Eastern District of Texas entered a final judgment against Bitcoin Savings & Trust and Trenton Shavers following an SEC enforcement action. The SEC alleged, and the court found, that Bitcoin Savings & Trust and Shavers conducted a Ponzi scheme soliciting investments in bitcoin-related investment opportunities.[79]

In December 2014, the SEC sanctioned Ethan Burnside for operating two digital currency exchanges without registering them as either broker-dealers or stock exchanges.[80]

In June 2014, Erik Vorhees was sanctioned by the SEC for violating sections 5(a) and 5(c) of the Securities Act of 1933 for publicly offering unregistered securities in two Bitcoin-related ventures, SatoshiDICE and FeedzeBirds.[81]

FBI/DOJ

Following an investigation by numerous agencies, Ross Ulbricht was sentenced to life in prison in May 2015 in connection with his role in Silk Road. Mr. Ulbricht founded Silk Road, an online black marketplace used to facilitate criminal activity; the site was later shut down by government task forces. Mr. Ulbricht was found guilty in February 2015 of conspiracy to distribute controlled substances, computer hacking, and money laundering.[82]

Blake Benthall, who operated Silk Road 2.0, a follow-on site to Silk Road, was arrested in November 2014 on similar charges.[83]

Charlie Shrem, a former vice chairman of the Bitcoin Foundation, and Robert Faiella, were arrested for unlawfully converting dollars into bitcoin for users of Silk Road. Each pleaded guilty in September 2014, and were sentenced to two years and four years in prison, respectively. Shrem and Faiella were charged with operating an unlicensed Money Transmitting Business (failure to register with FinCEN), money laundering, and willful failure to file SARs with FinCEN.[84]

Conclusion

The explosion of cryptocurrencies over the past several years has not escaped the attention of regulators in the United States. For at least the past two years, agencies have applied already existing laws and regulations to adapt to the virtual currency landscape, notably FinCEN and the CFTC. In addition, New York's BitLicense regime became the first comprehensive regulatory regime aimed squarely at regulating virtual currency. The continued growth and prevalence of cryptocurrency will undoubtedly continue to solicit attention from regulators and additional regulations and enforcement actions at the federal and state level.

International Regulatory Landscape

Internationally, the regulation of cryptocurrency varies substantially by jurisdiction. Some countries have minimal regulations on the subject. Several countries have proceeded with cryptocurrency regulation in ways similar to the United States—that is, they are currently studying the potential regulation of virtual currencies, and are working to adapt and/or update their already-existing anti-money laundering ("AML") and money transmission laws and regulations to cover virtual currencies. These countries include, among others, Canada, France, Italy, Singapore, and Japan.

Within Europe, the European Court of Justice just ruled that bitcoin should be treated as a currency. This ruling will undoubtedly have a major impact on virtual currency regulation in the international sphere, and stands in contrast to the U.S. CFTC's decision that virtual currencies should be treated as commodities. This and future rulings, along with a 2014 Opinion issued by the European Banking Authority urging an EU-wide virtual currency regulatory regime, could have the effect of unifying European regulation on the subject, which had varied more substantially from country to country.

However, other countries have imposed much more stringent regulations, and in some cases have banned or criminalized the use of virtual currencies. These more stringent laws may make it effectively impossible to deal in virtual currency in various countries. For example, Russia has recently proposed legislation to make the use of virtual currency a criminal misdemeanor. Virtual currency has been banned outright in Ecuador and Bolivia (although the Ecuadorian government has created its own state-backed digital currency). In Bangladesh, virtual currency is not considered legal tender, and its use may lead to jail time. Iceland has indicated that virtual currency is not protected currency, and its purchase may violate the country's Foreign Exchange Act. And the Chinese government has instructed its commercial banks to halt all dealings with virtual currency exchanges, and has prohibited these banks from clearing virtual currency transactions – particularly notable since more than 80 percent of bitcoin transactions take place in Chinese yuan.

As noted above, international regulation of virtual currency is fast-evolving and varies substantially across jurisdictions. This chapter is just a sampling of notable regulations in certain countries, and is not meant to serve as a thorough analysis of all virtual currency regulations across the globe.

Europe

October 2015 European Court of Justice Ruling

In one of the first major virtual currency court cases impacting the European Union as a whole, on October 22, 2015, the European Court of Justice ("ECJ") held that bitcoin should be treated as a currency and means of payment for tax purposes.[85] This holding stands in contrast to regulation in the United States, in which the U.S. Commodity Futures Trading Commission ("CFTC") has recently determined that virtual currencies should not be treated as currencies, but instead as commodities.[86]

The ECJ's ruling has major implications for all players in the cryptocurrency space, especially from a tax standpoint. Under the EU's Directive concerning value added taxes ("VAT"), member states may not use their value added taxes to tax "transactions, including negotiation, concerning currency, bank notes and coins used as legal tender."[87] Because the ECJ held that virtual currencies constitute currency and a means of payment for purposes of the EU's VAT Directive, the EU member states may not use their VAT to tax cryptocurrency transactions. Therefore, bitcoin and virtual currency exchanges that convert traditional currency to virtual currency are exempt from VAT, and consumers making a bitcoin exchange would not face a VAT charge as a result of the transfer. A holding by the ECJ that virtual currencies should be treated more like commodities (in line with the CFTC) would have made transfers of fiat currency to virtual currency potentially taxable under various EU members' VATs, similar to the general tax treatment of other commodities.

The ECJ's ruling was also significant because it resolved a conflict among the member states' taxing authorities on how exactly to treat virtual currency from a tax perspective—whether as a currency or a commodity. For example, while the UK tax authority had taken the position—like the ECJ—that virtual currency should be treated as a currency, the tax authorities from Sweden and Germany argued that virtual currency should be treated as a commodity, and thus subject to the VAT.[88]

The ECJ's ruling should provide a boost to bitcoin and other cryptocurrency trading in Europe, adding certainty that exchanges involving cryptocurrencies may be made free of VAT. The ruling had an immediate impact on bitcoin, as its price rose 3 percent immediately following news of the ruling.[89] It may also pave the way for additional harmonizing of virtual currency regulations across the EU member states.

It should be noted that this ruling applies primarily to the application of the VAT to the exchange of fiat currency for virtual currency, or vice versa, or the exchange of virtual currency for another type of virtual currency. Sales of goods and services subject to VAT but paid for with virtual currency would likely still be subject to VAT. And any capital gains on virtual currency appreciation could still potentially be taxed by member states in conjunction with their income tax laws.

European Banking Authority Opinion

In July 2014, the European Banking Authority ("EBA") issued an opinion regarding virtual currency, providing recommendations to the EU Council, European Commission, and European Parliament regarding an EU-wide regulatory regime of virtual currencies.[90] The opinion also provides recommendations to national banking authorities regarding intermediate regulatory steps that can be taken to address the risks of virtual currency before a full European regulatory regime is implemented.

Overall, the EBA's Opinion concluded that, although virtual currencies have the potential to create certain benefits –particularly in the areas of reduced transaction costs and increased transaction speeds – these benefits would have less impact in the EU, because of EU directives aimed squarely at those same goals.[91] The Opinion also found that the numerous risks of virtual currency (more than 70 were identified in the Opinion) would likely outweigh the potential benefits.[92]

In order to address the numerous risks of virtual currency, the EBA's Opinion advocated that "a substantial body of regulation" be implemented.[93] Such a comprehensive regulatory regime would need to include, at a minimum, measures addressing governance requirements of market participants, segregation of client accounts, capital requirements, and the creation of "scheme governing authorities."[94] In order to mitigate the risks of virtual currencies prior to the implementation of such a regulatory regime, the EBA recommended that national banking authorities should immediately "discourage credit institutions, payment institutions and e-money institutions from buying, holding or selling virtual currencies.[95] Finally, the EBA urged EU legislators to declare market participants in virtual currencies as "obligated entities" under the EU's Anti Money Laundering Directive, and therefore subject to AML and counter-terrorist financing requirements.[96]

Regulatory Status of Cryptocurrencies in Individual European Countries

Although the ECJ's recent ruling has provided clarity on the tax status of virtual currency in EU member states, the regulations of virtual currency across Europe still vary substantially. Generally speaking, the mining, exchanging, and buying and/or selling of goods or services with cryptocurrency is generally legal and permitted across Europe. However, much like the United States, many European countries are currently seeking to apply existing laws to virtual currency, virtual currency transactions, and players in the virtual currency space. For example, Germany, France, Italy, and the Czech Republic, among others, have explored adapting existing laws concerning money transmission, AML, taxation, and registration/licensure of financial institutions to apply to virtual currency.[97] Of course, any prior differences on tax treatment of virtual currency vis-à-vis the VAT may now be eliminated following the ECJ ruling.

Notable European nations that many view as having less stringent virtual currency regulation include the United Kingdom and Switzerland. Many believe the United Kingdom has a relatively more favorable view of blockchain and digital ledger technology. Numerous technology incubators focusing on blockchain technology and cryptocurrencies, such as those backed by Barclays and others, are headquartered in the United Kingdom. Further, in September 2014, the Bank of England released papers praising the potential benefits of blockchain technology and its potentially wide impact on the financial system as a whole. The Bank of England's papers note that distributed ledger technology is "the key innovation of digital currencies," and is "a genuine technological innovation which demonstrates that digital records can be held securely without any central authority." The Bank of England has also concluded that virtual currencies as a whole "do not currently pose a material risk to monetary or financial stability in the United Kingdom."[98]

In June 2014, the Swiss government affirmatively decided not to propose any new statutory provisions regarding virtual currency for the immediate future. Although a report by the Swiss Federal Council urged caution when conducting cryptocurrency transactions, the report concluded that no new legislation was necessary, in part, because "the economic importance of virtual currencies like Bitcoin as a means of payment is fairly insignificant at the moment and the Federal Council believes that this will not change in the foreseeable future."[99]

On the other end of the spectrum, Russia and Iceland have each passed laws that are particularly hostile to virtual currency. Legislation has been introduced in Russia that would prohibit the distribution, creation and use of "money substitutes," which includes virtual currencies; violators of the law would face criminal penalties.[100] Various sources have suggested that the legislation will be enacted by the end of 2015.[101] Even though the legislation has not passed, as early as

February 2014, Russian authorities warned that the ruble was the sole currency of Russia, and using virtual currency as a money substitute was illegal.[102] The Central Bank of Iceland has also declared that neither bitcoin nor Auroracoin is a recognized currency or legal tender under Icelandic law, and that the purchase of virtual currency is restricted under Iceland's Foreign Exchange Act.[103]

Asia

Generally speaking, Asian countries have more stringent regulations governing virtual currency compared with the rest of the world. For example, the use of Bitcoin and other virtual currencies is completely barred in Bangladesh, and officials from the Bangladesh Bank have stated that anyone caught using virtual currencies may be sentenced to up to 12 years in jail under the country's strict AML laws.[104] In China, while the use of Bitcoin and virtual currencies by individuals technically remains legal, its use is difficult if not impossible. This is because the People's Bank of China has warned financial institutions, payment institutions, and third-party payment providers that they may not accept, use, or sell virtual currencies; may not generally be involved in virtual currency transactions; and may not work with virtual currency-related businesses.[105] The regulatory status of virtual currency in Thailand is far from clear: in 2013, the Bank of Thailand informed a virtual currency-based business that virtual currency activities were illegal in Thailand; however, one year later, the same bank reportedly concluded that Thai law does not regulate virtual currency, but that exchanges still could not operate if they could not prevent virtual currencies from being exchanged with currencies other than the Thai Baht.[106]

On the other end of the spectrum, Japan stated in June 2014 that, despite the fall of Japanese-based bitcoin exchange Mt. Gox, the country would not move to regulate virtual currencies in the immediate future.[107] Finally, several other Asian countries, such as India and Singapore, are pursuing a more cautious approach similar to Europe and the United States, where they are seeking to adapt already existing laws to cover virtual currencies.[108]

The Americas

Outside of the United States, two countries in the Americas hold "first" status in digital currency regulation: Canada became the first country in the world to enact a national law specifically regulating virtual currencies, while Ecuador became the first country to issue its own state-backed digital currency.

In June 2014, Canada amended its Proceeds of Crime (Money Laundering) and Terrorist Financing Act to include provisions specifically governing virtual currencies from an AML perspective.[109] Pursuant to the amended statute, dealers in virtual currencies would be subjected to the same regulations as money services businesses.[110] The implications of this classification are that those dealing in virtual currencies would be required to register with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC," similar to FinCEN in the United States), and abide by various regulatory obligations surrounding recordkeeping, suspicious transaction reporting, and verification procedures, among others.[111] Under the revised statutes, banks are also prohibited from opening or maintaining banking relationships with unregistered businesses that are now classified as money services businesses on account of dealing in virtual currency.[112]

Second, in 2015, Ecuador became the first nation to issue its own, state-sponsored digital currency—the dinero electrónico—that is officially legal tender in the country alongside the U.S. dollar.[113] However, although the Ecuadorian government's own digital currency is legal tender, Ecuador has explicitly banned Bitcoin, Ripple, and other types of virtual currency.[114] Bolivia has a similar ban on virtual currency, but has not issued its own digital currency as a substitute.[115] Perhaps because of these bans issued by its South American neighbors, authorities in Argentina and Brazil have issued warnings about the risks of using virtual currencies not recognized as legal; however, these countries have not banned virtual currency themselves.[116]

Africa

There is limited data on the regulation of virtual currency throughout Africa.[117] In South Africa, a joint statement issued by the National Treasury, the South African Reserve Bank, the Financial Services Board, the South African Revenue Service and the Financial Intelligence Centre confirmed that "[c]urrently in South Africa there are no specific laws or regulations that address the use of virtual currencies."[118] Therefore, the use of the virtual currency in the country is generally permissible. However, the same authorities warned against the risks of virtual currency, and also clarified that because of this unregulated status, "no legal protection or recourse is afforded to users of virtual currencies," and "virtual currencies cannot be classified as legal tender as any merchant may refuse them as a payment instrument."[119]

Insuring Bitcoin and Bitcoin Business

Companies that service the Bitcoin industry and its holders face risks unique to the bitcoin[120] market, as well as to the financial services market generally. Thus, key questions for potential policyholders include how, if at all, insuring bitcoin is different from insuring other currencies? What insurance products currently exist that may cover bitcoin holders, servicers, and third-party vendors, and is the industry developing new types of coverage specific to bitcoin? And, to date, how has the insurance industry responded to claims made under those insurance policies? This chapter examines these questions and identifies practical concerns and tips for policyholders.

Does Bitcoin Raise Unique Insurance and Underwriting Issues?

Bitcoin is both an asset akin to currency and a protocol for digitally recording transactions. Viewed from this (simplified) perspective, insuring bitcoin holders, storage providers, exchanges, or related companies should be no different in terms of risk than any other business that safeguards or transfers an anonymous commodity, like cash, or that must protect its trade secrets or sensitive digital information. A variety of "traditional" insurance coverages exist, for example, to insure financial institutions and technology companies and their management, including network security and privacy liability (cyberliability) insurance, financial institution bonds and commercial crime insurance, directors' and officers' liability (D&O) insurance, and professional liability (E&O) insurance. At least one court even has characterized bitcoin as equivalent to traditional assets like "money" or "securities,"[121] suggesting that traditional insurance ought to respond to risks faced by the Bitcoin industry, just as insurance responds to similar risks in more established financial and technology industry sectors.

But novel issues abound, as Bitcoin (and its derivatives) feature several unique characteristics. Unlike most "traditional" currencies, bitcoin requires no financial institutions to issue new currency and no banks to store it, and transactions may be anonymous and are non-reversible. Also, because Bitcoin is decentralized, and its software is open-source, there is limited control over the currency or technology beyond a core group of developers and dedicated individuals. Thus, Bitcoin raises potentially unique issues with regulation, information security, price volatility, and reputation.

Regulation

As discussed in Chapters 3 and 4, governments have taken divergent approaches to regulating Bitcoin, with some outright banning cryptocurrencies altogether.[122] The possibility remains that governments will impose substantial regulatory burdens or penalties on companies operating within the industry, including the risk of fines, application of anti-money laundering laws, and rigorous oversight by government agencies that range in focus from consumer protection to commodities regulation.

Information Security

The cryptocurrency industry is seeking consensus on how best to secure Bitcoin and other cryptocurrencies, and the companies that service cryptocurrency holders, including storage companies, trading platforms, and exchanges. Ownership of cryptocurrency is synonymous with knowing a private "key" associated with an address on the public chain of title (the "blockchain"). To conduct transactions, owners may use the services of a company acting as an intermediary to secure their private keys and run the software needed to spend bitcoin. These companies take varied approaches to securing private keys in their possession. Some put private keys in "cold storage," meaning keys are saved in computers not connected to the public Internet. Other companies utilize (among other methods) "multi-sig" technology that requires knowledge of multiple keys before a transfer of bitcoin is possible, with the company holding one key, the owner another, and a third retained offline as a backup. Thus, neither the industry serving bitcoin users nor the users of the currency have yet identified preferred standards of asset protection.

Price Volatility

Bitcoin has risen and fallen in price dramatically since its introduction. Price volatility raises issues with respect to the financial strength of insured companies, the severity of the risks they face, and how to predict or quantify losses.

Reputation Concerns

Bitcoin's infancy has been plagued by an association with criminal activity. Media reports often discuss Bitcoin in connection with cybercrime, including schemes to defraud, phishing attacks, and theft. Bitcoin has also reportedly been used by criminals as an anonymous means of payment for drugs, extortion schemes, and other illegal activities.

Given these issues and concerns, what can companies operating within the bitcoin economy expect? In short, a rigorous insurance underwriting process, and potentially a rigorous claims process when losses ultimately occur. Insurers may assess a company's current practices and protocols concerning data, network and privacy security, physical protections for data held in cold storage, and breach or loss response. In the event of a loss, insurance policies may require rapid identification of the breach or loss, collection and preservation of information, mitigation of any damages or losses, and prompt notification to the insurance carrier. Due to the sensitivity of the information a policyholder may be required to share with insurers, both during the underwriting process and in the event of a loss, companies should insist on signing strong confidentiality agreements with insurers and brokers. Coverage counsel can help policyholders navigate these and other related issues both during placement of coverage and after a loss occurs.

Potential Insurance Coverage Under Traditional Policies

Although Bitcoin raises a number of novel issues, insurance companies may seek (and have sought) to insure the risks arising from this technology with well-established forms of coverage. Some insurers also have begun developing hybrid forms of insurance coverage to address both the more traditional risks associated with the industry and the unique aspects of bitcoin and bitcoin technology.

Cyberliability

Cyberliability insurance is designed to address first-party losses and third-party liability as a result of data security breaches and the disclosure of or failure to protect private information. It commonly insures against (or helps defray) the cost of misappropriated data, investigating a breach, responding to regulators, defending against lawsuits, notifying affected persons, restoring or recreating any lost data, and paying damages and settlements, among other expenses. Cyberliability policies often are negotiable and may be tailored to a particular company or industry.

Ideally, a cyberliability policy intended to cover Bitcoin or Bitcoin-related operations should be drafted broadly enough to cover issues unique to the currency and technology. The policy thus might insure against liability related to the company's storage or exchange of bitcoin, corruption or breach of its associated technology, or losses due to a compromised vendor. The definition of a liability event should be broad enough to include disclosure of or damage to the types of confidential information unique to Bitcoin, including users' private keys. Security concerns or vulnerabilities particular to bitcoin and bitcoin technology also should be addressed where possible, including the generation of flawed keys, transaction malleability attacks, 51 percent attacks intended to manipulate the blockchain, sybil attacks, and distributed denial of service attacks.[123]

Financial Institution Bonds and Commercial Crime Policies

These policies insure against first-party losses caused by certain types of criminal, fraudulent or dishonest activity, including employee dishonesty, fraud, forgery, and extortion. Many bonds and commercial crime policies contain coverage for computer crimes and frauds that directly result from the use of a computer and result in the transfer of money, property, or securities from within the company to parties outside of the company.

Businesses that use, keep, or perform services related to bitcoin should ensure that "bitcoin" is included in the definition of "money," "currency," "property" or any related terms or definitions that identify covered types of loss.[124] Bitcoin transactions may be conducted "peer-to-peer," meaning the buyer and seller do not need to use a central exchange. Companies should examine their potential exposure to losses arising from peer-to-peer transactions, because at least one insurer has publicly stated that peer-to-peer transactions are not covered under its commercial crime policy form.[125]

Social engineering and "phishing" attacks also are a threat to a Bitcoin business. A bad actor could seek to convince an employee that they are conducting a genuine transaction or sharing private information with a trustworthy recipient, when the employee is in fact an unwitting intermediary in a scheme to defraud. Social engineering attacks can implicate the "direct" causation and intent standards in many bonds and commercial crime policies. Traditional financial institution bonds cover only losses "directly caused" by a covered activity. The "direct loss" standard is not uniformly interpreted by the courts and is a frequent source of insurance disputes. Some courts hold that the "direct loss" standard is equivalent to proximate causation under traditional tort law, but others hold that "direct loss" means that there can be no intervening cause between an action intended to cause harm and the harm itself. If the latter interpretation applies, it may be difficult to obtain insurance proceeds for losses caused by a social engineering or phishing attack on a bitcoin company.

A recent lawsuit filed by bitcoin payment processor Bitpay, Inc. against its commercial crime insurer illustrates this issue.[126] After a phishing attack compromised the email account of a Bitpay executive, the hacker used information collected from the executive's email to induce the company to transfer funds to an ostensible customer wallet that was, in fact,

controlled by the hacker. Bitpay's commercial crime insurer denied coverage, asserting that because the Bitpay executive acted as an unwilling intermediary in the scheme, the loss was not "directly caused" by the activity of the hacker. (Bitpay's lawsuit remains pending as of this writing.)

In addition, many policies require "manifest intent" by an employee before a loss caused by employee dishonesty is insured, a phrase sometimes interpreted by courts to mean that an employee must not only intend to personally gain from his or her dishonesty, but also to intend to harm the company. Thus, an insurer may assert a defense to coverage if a defalcating employee's intent was directed at the bitcoin holder, not the company.

D&O Insurance

D&O insurance is designed to protect a company's directors and officers, and often to a more limited extent, the company, against third-party liability. D&O policies commonly insure individual directors and officers when they cannot be indemnified by their companies ("Side A" coverage), the company when it pays indemnification to its directors and officers ("Side B" coverage), and the company in connection with lawsuits alleging violations of the securities laws ("Side C" coverage). Monetary damages may be covered, but property damage generally is not. D&O insurance often can be negotiated.

Although a variety of D&O policy provisions should be tailored to Bitcoin-related risks, three are of particular note. First, any Bitcoin-related company should ensure its policy will cover securities lawsuits triggered by a loss of bitcoin or damage to the company's bitcoin operations. Second, given the prevalence of criminal activity related to the currency and technology, as well as the uncertain regulatory environment, the insurance policy should clearly insure the costs of cooperating with government investigations, inquiries, and any administrative proceedings related to Bitcoin. Finally, companies should pay attention to any exclusion for loss arising from professional services provided by the company.

E&O Insurance

E&O insurance is designed to protect individuals and companies from liability for mistakes, omissions, and other errors made in the performance of a professional service. E&O polices can be tailored to specific risks and are frequently negotiable. Every company that provides services related to bitcoin in return for a fee – whether they host or maintain customer "wallets," operate exchanges, facilitate transactions, or provide any of the myriad services relevant to the industry – can potentially benefit from having E&O insurance. A lawsuit accusing a company of an error, even if frivolous or baseless, could result in substantial legal expenses and reputational damage.

Would a traditional E&O policy cover a financial institution utilizing new bitcoin technology, such as a financial institution implementing blockchain technology, to record and maintain the ledger of private stock transactions? Although many E&O policies broadly define what constitutes a covered "professional services," E&O policies are not entirely uniform among different insurers and different industries and may be tailored to specific risks, and thus the definition of "professional services" may or may not automatically include such services. For instance, many E&O policies issued to financial institutions define "professional services" simply as those services provided by the insureds to a customer or client for a fee or other form of compensation or services. In some cases this language may be read to capture all such services provided by the policyholder (i.e., any service performed for a customer for a fee), but for other policyholders, this generalized description of "professional services" may be tied, either explicitly or implicitly, to particular representations made in the company's application for the insurance, or in the company's public filings with the SEC or other regulators. Further, the definition of "professional services" in some E&O policies may incorporate or list specific types of services performed by the particular policyholder. Accordingly, companies performing Bitcoin-related services should carefully review the way in which their E&O insurer defines covered professional services to decrease the possibility of a coverage dispute in the event of a loss.

Kidnap and Ransom ("K&R") Insurance

K&R coverage insures an individual or company from loss in the event the insured, an employee, or some other identified person is kidnapped, detained, or ransomed. K&R coverage is an indemnity product, meaning that the ransom money must first be paid before the insurer will provide reimbursement. According to recent media reports, bitcoin has emerged as a preferred currency for kidnappers and extortionists. As such, companies should ensure, where possible, that its K&R coverage allows for ransoms and extortion payments to be paid in bitcoin. For example, any definition of "money" or "currency" in the policy should expressly include "bitcoin."

Bitcoin-Specific Insurance

Several major insurers reportedly have developed specialized insurance products for the bitcoin market. Although the details, terms and conditions of these policies are not widely known, it has been reported that at least one major carrier has created an E&O policy with the privacy and data protection elements of cyberliability

coverage, commercial crime protection, and deposit protection;[127] and another has developed a "new" type of commercial crime coverage specific to bitcoin. [128] Other companies have created captive insurance funds to protect their customers instead of turning to insurance companies. [129] As this nascent industry and its technology continues to develop, it remains to be seen how these initial insurance products will respond to the unique risks posed by bitcoin and the industry that serves the currency and its users.

The Bottom Line

Bitcoin has created a small but growing industry focused on, among other things, securing users' private keys, facilitating transactions, running bitcoin exchanges, and trading bitcoin futures or swaps. In order to increase customer and investor confidence, and to free capital to grow their businesses, companies providing Bitcoin-related services may, like the financial services industry supporting "traditional" currencies, look to transfer their risk of liability and loss through the purchase of insurance. Until insurance policies and products specifically tailored to the industry are widely available to companies providing Bitcoin-related services, companies should review their current insurance coverage to assess how and to what degree insurance will respond in the event of common claim scenarios. Companies purchasing either traditional policies or Bitcoin-specific coverage for the first time should carefully review the terms and conditions of any proposed coverage, and consult with a reputable broker and policyholder coverage counsel when comparing different policy forms and negotiating important changes and enhancements where possible.

Applications in Capital Markets

Although it was developed in the context of creating cryptocurrency, the blockchain has the potential to have a major impact on both financial institutions and financial transactions involving fiat currency. In fact, few Bitcoin-related developments generated by financial institutions have to do with trading bitcoins or conducting transactions involving other cryptocurrencies. Instead, these institutions are applying the technology behind bitcoin—the blockchain—to numerous types of other financial innovations that do not involve any type of cryptocurrency.

Already, banks and financial institutions have met to discuss how to respond to and/or utilize this technology, and several financial institutions are performing in-house experiments and projects seeking to take advantage of the blockchain's benefits.[130] Several tech startups, such as Digital Asset Holdings, led by Blythe Masters, and R3, which is supported by JPMorgan, Barclays, Credit Suisse, and Goldman Sachs, among others, are also exploring the blockchain space, and seek to find ways to implement blockchain technology into everyday banking and financial transactions.[131]

Some analysts are hailing blockchain technology as transformative, with Accenture describing it as possibly the "critical backbone" of the future capital markets infrastructure,[132] and the *New York Times* describing it as a "fundamentally new way" of transacting and maintaining records.[133] Financial industry consultancy firm Greenwich Associates interviewed 102 institutional financial professionals in mid-2015; of those surveyed, 94 percent responded that they believed that blockchain technology could be applied in institutional markets, and almost half reported already being in the midst of reviewing the technology within their firms.[134]

Spending by capital markets firms on research and development in the technology will more than double from $30 million in 2014 to $75 million in 2015, according to consultancy firm Aite Group.[135]

While there are those who are more skeptical, industry professionals, including major financial players, have demonstrated a keen interest in applications of blockchain to their industry.

Greater Efficiencies

Transactions involving the blockchain have the potential to be significantly more efficient. This increased efficiency will come in the form of quicker settlement, improved accuracy, lower error rates, automated settlement, and significantly less reliance on third parties for post-trade settlement. This may lead to lower costs for all parties involved.

One of the most exciting potential applications of the blockchain in capital markets is the possibility of using it to eliminate the cost and time of clearing and settling financial assets. Because the blockchain is decentralized and is not maintained by any one party, two parties can exchange an asset or information directly with each other without the use of a third party validating the information in a near instantaneous settlement. In the blockchain, the assets can be tied to individuals, with no need for institutional custodians.

This development could save Wall Street banks and investors billions of dollars by radically reducing a transaction's lifespan, as it would free up capital that is otherwise pledged to back trades until they are settled. Typical securities trades take two to three days to settle,[136] and the potential savings for other transactions is even greater: for example, the average bank loan took nearly 23 days to settle in 2013.[137]

Initially, the blockchain is most likely to impact asset transactions where there is no central clearing or trading authority, such as transactions involving FICC derivatives, syndicated loans, and private investments. NASDAQ has already announced that it is looking to implement the blockchain in connection with the trading of private companies, and to replace paper trading for these types of transactions.[138]

Furthermore, the security provided by the blockchain may have an even greater impact on markets with high transaction volume, but less trading infrastructure in place, such as loans and private over-the-counter derivatives that cannot be backed by clearinghouses.

More Security and Transparency

Many analysts believe that the blockchain can make financial transactions more secure. Because the blockchain is not controlled by a central party, but instead involves decentralized control, the blockchain is less vulnerable to (if not immune from) cyberattack. The blockchain cannot be lost or corrupted by participants, and thus counterparty risk in transactions is significantly reduced.

Because of the public nature of the blockchain, and the completeness of the information contained in its ledger, the blockchain also has the future potential to more easily facilitate data-sharing for KYC and AML purposes, trade surveillance, regulatory reporting, collateral

management, and perhaps even real-time auditing of transactions.

However, despite the blockchain being publicly available and easily shared among parties, various identifying information about parties making transactions may be hidden and made private in certain circumstances. There is thus a means to limit privacy risks in conjunction with the improved transparency.

Imagine also reconfiguring on the blockchain various protocols widely used in the capital markets, such as SWIFT (a communications platform designed by the Society for Worldwide Interbank Financial Telecommunications to facilitate the transmission of information about financial transactions), or FIX (a trading platform for communicating trade information based on the Financial Information eXchange Protocol). With the blockchain's ability to record the complete history of all transmissions, disputes or errors typically lost in communications will be minimized, if not eliminated.

"Smart Contracts"

Finally, the blockchain may offer improved contractual performance. Innovators are currently working to develop "smart contracts," where the terms of contracts may become automated and agreed upon using computer protocols within the blockchain.

Potential Risks

Although the blockchain has the potential to provide tremendous benefits to financial institutions and transacting parties more generally, widespread use of this technology does not come without risks and potential issues.

First, as with the implementation and adoption of any new technology across a space as complex and massive as the capital markets infrastructure, there are likely to be hiccups and growing pains along the way. It is difficult to predict the immediate impact that any glitches in blockchain adoption might have on individual transactions, or the future impact of those glitches on future adoption of the technology.

Second, some question whether the blockchain in its current technological state would be able to handle transactions in data classes with particularly high volume and speed requirements. Some analysts are skeptical as to whether the blockchain can be updated sufficiently frequently to be useful in such transactions.

Third, as discussed elsewhere in this paper, there are numerous unanswered questions as to how regulators across the globe will react to the blockchain and virtual currencies more generally. Regulators have still not yet caught up to the current technology, and when they do, these regulations could have a significant impact on the ability of financial institutions and other parties to implement blockchain technology into everyday financial transactions.

Finally, whether blockchain technology will impact capital markets will depend on the use of the technology by major financial institutions, and the extent to which these institutions develop the technology. Ironically, although cryptocurrencies were developed in the hope of reducing dependency on banks and other major financial institutions, whether these same institutions cooperate in instituting the technology will play a role in determining the impact that the blockchain has on capital markets.

Conclusion

Despite the potential downsides, the key attraction to blockchain technology for industry professionals is risk reduction. The blockchain offers the potential to improve the current infrastructure of financial transactions in significant ways: by making transactions more efficient and more secure, providing more transparency and regulatory control, and improving contractual performance. In addition to highly capitalized start-ups in this rapidly developing field, numerous major financial institutions have been spending significant resources on understanding and developing relevant applications.

Bitcoin, Privacy, and Reidentification

As one paper noted, "anonymous digital cash is another state-of-the-art technology for Internet privacy. As many observers have stressed, electronic commerce will be a driving force for the future of the Internet. Therefore, the emergence of digital commerce solutions with privacy and anonymity protection is very valuable..."[139] Since the paper in question, Privacy-enhancing technologies for the Internet was published in 1997, the authors thought not of Bitcoin but of a predecessor, DigiCash's ecash. However, the paper identified risks to privacy in using anonymous digital cash that have only grown:

> Of course, the DigiCash protocols only prevent your identity from being revealed by the protocols themselves: if you send the merchant a delivery address for physical merchandise, he will clearly be able to identify you. Similarly, if you pay using ecash over a non-anonymized IP connection, the merchant will be able to deduce your IP address. This demonstrates the need for a general-purpose infrastructure for anonymous IP traffic...In any case, security is only as strong as the weakest link in the chain.[140]

Bitcoin has been described as "anonymous but not private: identities are nowhere recorded in the Bitcoin protocol itself, but every transaction performed with bitcoin is visible on the distributed electronic public ledger known as the block chain."[141] In addition, an individual Bitcoin user may use one (or very many) public keys (sometimes referred to as a "bitcoin address") to engage in transactions. These public keys do not identify individual users, and without additional data or analysis, one cannot determine whether two (or more) public keys are linked to the same user. Therefore, the Bitcoin protocol theoretically provides for anonymity (but not privacy) in transactions because the blockchain does not involve recording any identifying information to individual public keys.

However, in practice, it may be difficult to maintain one's anonymity when using Bitcoin. Some chinks in the armor of privacy when using Bitcoin are akin to those described 22 years earlier as to DigiCash. Some Bitcoin users voluntarily disclose their public keys; in so doing, they may either intentionally or unintentionally allow others to link identifying data with these public keys. Those who are able to link public keys with this outside identifying information may have the ability to then analyze the blockchain and potentially determine the identity of the user. This identifying data does not necessarily have to be as specific as a person's name, address, or phone number. It could be something as seemingly innocuous as the knowledge that a particular user made a purchase with a particular business around a certain time.

For example, at the onset, many users purchase bitcoin through an online wallet or exchange service. That wallet or exchange service has the personal information of the purchaser.

> Bitcoin for these users is effectively no more anonymous than a bank account, although this loss of anonymity takes place at the point of entry into the currency and is not a feature of the bitcoin protocol itself.

Further, some users voluntarily reveal or disclose their public keys, whether publicly (as may be the case for businesses accepting bitcoin as payment), or through blockchain.info, or more privately in forums, signature lines in internet posts, or in forums. In this respect, one may think of a bitcoin public key in a way similar to an email address: some email addresses may be relatively anonymous in nature (for example, an email that does not reveal one's name or initials), but one may of course still choose to reveal that email address to acquaintances.

In addition, "[e]ven supposing one manages to acquire bitcoins without giving up personal information, one's real-world identity can still be discovered in the course of transacting bitcoin within the network."[142] As discussed above, when outside information becomes linked with a particular public key, there is a risk that reidentification may occur through various types of behavior-based clustering analysis of the blockchain, and in some cases, analysis of the IP addresses of nodes adding blocks to the blockchain.

In the case of Bitcoin, there is not only the risk that a delivery order to a physical address will lead to reidentification. There is also, in the distributed ledger itself, a large amount of public data with respect to transactions made with the bitcoin currency, leading one author to note:

> A complementary source of potentially deanonymizing information is available to every computer that participates in the decentralized transaction network by hosting a bitcoin node. This information is the set of IP addresses of the computers that announce new bitcoin transactions...

> An example of this kind of IP address deanonymization made public is blockchain.info, which discloses the IP address of the first node to report a transaction to its servers. The information is only as reliable as the web site's node connectivity: with a declared 800–900 connected nodes at the time of writing, it is probably not enough to reliably pinpoint the originating IP in all cases.[143]

Some of the concerns surrounding the privacy and pseudonymity of Bitcoin are similar to the concerns of pseudonymity raised in other industries and other contexts. For example, the National Institute for Standards and Technology (NIST) has issued standards regarding pseudonymity and deidentification. The NIST standards concern a different type of pseudonymity issue than is present in Bitcoin. Specifically, the NIST standards concern data sets that have been stripped from personally identifiable information, and the risk of re-identification from those data sets. These standards are aimed at companies managing individuals' sensitive information so as to not inadvertently reveal their identities. In contrast, the "rules of the game" concerning Bitcoin pseudonymity are more well known and "spelled out." Further, Bitcoin users have more control over whether they made be re-identified, and can take various actions to greater maintain privacy (however, this increased privacy may lead to higher transaction costs).

NIST defines pseudonymization as a "specific kind of de-identification in which the direct identifiers [like names or account numbers] are replaced with pseudonyms." [144] NIST defines "re-identification risk" as "the measure of the risk that the identities and other information about individuals in the data set will be learned from the de-identified data."[145] The factors that determine reidentification risk include: "the technical skill of the data intruder, the intruder's available resources, and the availability of additional data that can be linked with the de-identified data."[146]

The report includes a number of highly public instances in which pseudonymized identities were re-identified based on ancillary information, from movie choices to medical outcomes to location data.[147]

However, as NIST warns, "In many cases the risk of re-identification will increase over time as techniques improve and more background information become available."[148] In the case of distributed ledger technology, the permanence of transaction history ensures that the transaction history available to analyze continues to expand even as the techniques to do so improve over time.

NIST's concern regarding reidentification risk is mirrored internationally. For example, under European privacy law, a pseudonym is personal data under specific standards set forth by the Article 29 Working Group. [149] "Pseudonymity is likely to allow for identifiability, and therefore stays inside the scope of the legal regime of data protection."[150] The Article 29 Working Group lists as a "common mistake":

> Believing that a pseudonymized dataset is anonymized....Many examples have shown that this is not the case; simply altering the ID does not prevent someone from identifying a data subject if quasi-identifiers remain in the dataset, or if the values of other attributes are still capable of identifying an individual.[151]

The paper identifies as weaknesses of the pseudonymous approach, "the user using the same key in different databases," as well as storing the key to re-identify in the same place as less secure data. "If the secret key is stored alongside the pseudonymized data, and the data are compromised, then the attacker may be able to trivially link the pseudonymized data to their original attribute."[152]

Of course, every form of extensive activity is potentially subject to re-identification. This theoretically includes Bitcoin activity, in which re-identification is theoretically possible using information from the blockchain. Nevertheless, those using bitcoins and distributed ledger technology should be aware of the already-identified risks of reidentification inherent in the current model, and take steps to reduce such risks by protecting pseudonyms used and linkable public information

Intellectual Property

While Bitcoin made the blockchain famous, the benefits of a secure distributed ledger are being implemented across many fields. Ancillary technologies are being invented to improve and expand cryptocurrency services, improve block mining, and implement the blockchain in new ways. New software is being developed to advance the technology in even more directions. As with many technologies, the intellectual property rights surrounding blockchain technologies are quickly evolving and maturing—and becoming less open.

Satoshi Nakamoto published his idea for the blockchain underlying Bitcoin, placing the idea into the public domain for anyone to implement. And Bitcoin software is distributed under an open source license that allows others to freely use, modify, and share the software. The Hyperledger Project proposes a similar model. But what does that really mean for companies involved in the Bitcoin industry? What are the specific terms of the open source licenses? Are there any intellectual property (IP) rights, such as patent rights, that fall outside of an open source license? And what IP rights come into play for companies developing or using applications of the blockchain separate from Bitcoin or Hyperledger? This chapter examines these questions and identifies emerging trends in blockchain IP. The IP landscape developing around Bitcoin and blockchain technologies can be a minefield. Stakeholders and market entrants need to know how to navigate the risks and protect their contributions.

Bitcoin's Open Source License

The Bitcoin Project is released under the MIT License. The MIT License grants the rights to any person with a copy of the licensed software the rights to copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the software. The only condition the MIT License places on copies and derivative works is that its copyright notice and terms must be included in all copies or substantial portions of the software. Companies involved in the Bitcoin industry can thus freely copy and use Bitcoin software.

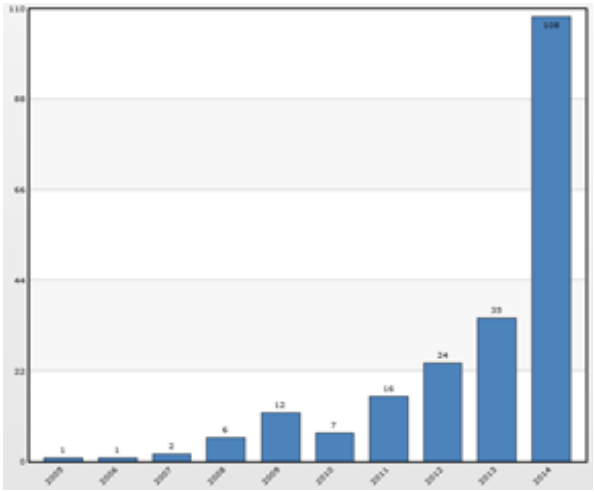
Bitcoin has sparked development of third-party software, other cryptocurrencies, and other applications of blockchain technology. The Bitcoin Project encourages innovation, and the MIT License permits development of software and new technologies incorporating Bitcoin code. The license even allows for proprietary software to use Bitcoin software. Some Bitcoin-based software therefore may not be freely modified or copied. Companies utilizing Bitcoin software or other open source blockchain software therefore need to be aware of the terms of the license to the specific software they are using to understand their rights and potential liabilities.

Other Blockchain Application Licenses

Many promising new technologies are developing based on the blockchain idea and its permissive license. The Hyperledger Project, for example, is a cross-industry, open source collaborative effort created to advance blockchain technology. Its stated mission is to create an enterprise grade, open source distributed ledger framework and code base, upon which users can build and run robust, industry-specific applications, platforms and hardware systems to support business transactions. While the Hyperledger Project is open source, like the Bitcoin Project, its open source license is more restrictive than the MIT License under which the Bitcoin software is distributed. Inbound code contributions to the Hyperledger Project and outbound code will be made available under the Apache License, Version 2.0. The Apache License V2.0 grants broad rights, but includes additional notice requirements and restrictions on derivative works not included in the MIT License. The Apache License V2.0 also grants a patent license from each contributor with various restrictions. Companies using or developing blockchain technologies that are unaware of the specific terms of relevant licenses risk infringement.

The Rise of Blockchain Patents

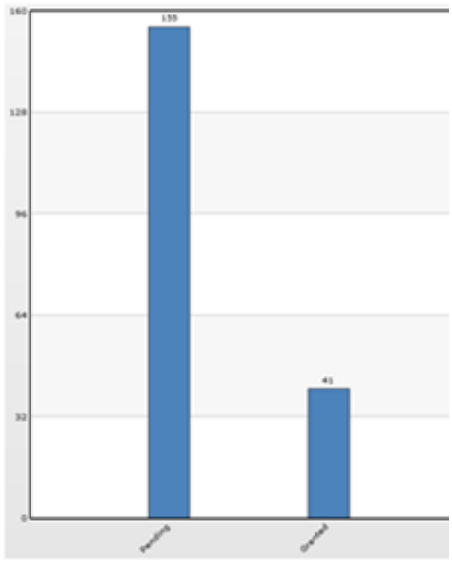
The growth of Bitcoin has sparked innovations in supporting and complementary technologies. More innovation is expected as the applications of blockchain technology beyond cryptocurrencies are explored. A sharp increase in patent applications in recent years evidences both the rate at which the technology is developing and the desire of stakeholders to maintain their competitive advantage by protecting their inventions.



The above chart shows the number of new patent applications directed specifically to blockchain-related technologies filed per year from 2005 through 2014 on the horizontal axis. As shown, new patent filings more than tripled from 2013 through the portion of 2014 with available public data. Patent applications take 18 months to publish, so the data for 2014 remains incomplete. As applications publish, we expect to find an even sharper rise in 2015.

Bitcoin and the underlying distributed ledger technology are inherently technologies that reach across borders. Patent application filings provide an indication of anticipated markets for developing technology. The map below shows individual patent filings in each country, with darker blue indicating a greater number of filings. While the greatest density of patent filings has been in North America, applications are being filed across Europe, Asia, South America, and Australia. An international patent minefield is developing, and market participants with an international reach need to know their international exposure. And because of the international reach of most blockchain-rooted technologies, innovators should consider international protection for their inventions.

Empirical analysis of global published applications shows that the largest numbers of patent applications cluster around payment methods and systems using cryptocurrencies or the block chain. Other areas of intense patent activity surround encryption technologies and blockchain mining technologies. As the technology implementing the underlying blockchain in other ways matures, we expect the areas of activity, and thus the areas of exposure to stakeholders, to expand.



The chart above shows that while only 41 patents directed specifically to blockchain-related technologies have issued, more than 155 published applications are pending. Patent filings are on the rise and patent examination in most countries typically takes at least two years, so the global landscape for issued patents relating to Bitcoin and blockchain inventions is just now forming. It will be imperative for stakeholders and market entrants to protect their valuable IP and understand the risks presented by the IP of others in this emerging IP landscape.

Social Impact

Despite being an emerging technology, Bitcoin has been the focus of several charity and social impact projects since its inception. While the use of bitcoins to fund charity projects and for remittances has garnered recent attention, there has been less focus on how the blockchain algorithm itself might be used in applications with a social impact. This chapter describes some successful applications of the blockchain algorithm to problems in the social responsibility space, and describes the wide opportunity in this area.

Lowered Transaction Fees Mean More Money for Causes

The immediate appeal of cryptocurrencies in the context of international aid is the potential to lower transaction and currency exchange fees, especially for smaller donation amounts. Donors can send small donations of fiat currency, which are converted to bitcoin at an approximately 1 percent transaction fee, which are in turn sent to an aid organization's digital wallet for conversion into a local currency of choice. By reducing these fees, organizations can make more out of smaller donations.

ChangeTip, a micropayment service, partnered with Direct Relief to enable donors to purchase $5 prenatal vitamin supplements for mothers in the developing world.[153] ChangeTip channeled these small donations through bitcoin, cutting down on fees that would have made such small donations impracticable.

Greater Transparency

The Bitgive Foundation, partnering with Factom, recently launched the Donation Transparency Project, which aims to track donations and expenditures in aid projects using the blockchain algorithm.[154] The platform aims to add transparency and traceability to international aid organizations, so that donors can see the impact of their giving and make informed decisions about effective aid organizations. Similar applications could improve the ability of governments and international charities alike to track international development spending, reduce corruption, and analyze trends across projects.

Access to Financial Services

Applications of the blockchain algorithm have much to offer the 2 billion adults in the world who lack a bank account. Much of the attention has focused on using cryptocurrencies to send remittances, which have typically been subject to high fees. However, while much has been said about the potential for Bitcoin to reduce fees for remittances,[155] building an end-to-end money transfer system using cryptocurrency has remained difficult.

The most successful applications pick a single country or region and focus on the so-called "last mile," where the incoming money transfer is converted to cash for its recipient.[156] For example, BitPesa focuses on converting bitcoins to Kenyan or Tanzanian shillings and depositing that local currency to a mobile money number.[157] By relying on the pre-existing mobile money wallet system in use by many Kenyans and Tanzanians, BitPesa is able to sidestep the complicated international money transfer system that has made a general-purpose bitcoin-based remittance system so elusive. The Philippines, which is the world's third-largest recipient of remittances, has also seen significant innovation in using bitcoin to send money into the country. Several startups focus on converting bitcoins to Philippine pesos and making cash available to remittance recipients in partnership with the ATM networks, convenience stores, and pawnshops that customers already use.

Much like with international aid, the blockchain algorithm has more to offer than simply reducing fees for money transfers. Coins.ph, one of the remittance startups in the Philippines highlighted above, has introduced a new service called Teller.[158] Teller, in startup nomenclature, is "Uber for ATMs," in that the Teller application connects customers to pre-screened tellers who can take or distribute cash in exchange for bitcoins. Tellers and customers are kept accountable through a two-way reviewing system, and its inaugural tellers are the same convenience stores and pawnshops that customers currently use for remittances. Because the financial transaction itself is secured by the blockchain, Teller can focus on the security and availability of only one step of the process: the exchange of an electronic balance for cash. Using the blockchain, in other words, makes it possible to serve the unbanked where they already are.

Financial Empowerment

One of the defining features of blockchain and cryptocurrencies is democratization. For those who do not have control over their financial destinies under traditional financial systems, the blockchain opens up significant opportunities. For example, two projects started by Afghan entrepreneur Fereshteh Forough use bitcoin to pay Afghani women for work they complete as they learn skills for the digital economy. The Digital Citizens Fund[159] builds women-only computer centers to teach young women word processing, presentation, financial and Internet-based tasks, while Code to

Inspire[160] similarly teaches young women computer programming. Both organizations use bitcoin to pay their students, not only because of the number of unbanked people in Afghanistan, but also because of the cultural, legal, and safety issues associated with giving women cash in that country.[161] With bitcoin, these young Afghani women can exercise a measure of control over their financial futures.

Improving Governance and Minimizing Corruption

As *The Economist* phrased it, blockchain's central innovation is that it is a "machine for creating trust."[162] An important application area for blockchain, and perhaps one of the largest opportunities, is modernizing the way we store and secure information relating to large groups. For governments, blockchain offers the opportunity for an open, transparent ledger of public information with an unchangeable audit trail for every record. One country, Honduras, is already experimenting with using the blockchain to store land title records.[163] The current land title system is not only incomplete, but it is also subject to near constant corruption and manipulation. The government of Honduras, working with U.S.-based startup Factom, hopes to leapfrog current land records techniques to create an auditable and incorruptible title database. Future applications of the blockchain algorithm could offer similarly secure records of procurement activities, votes, budgeting information, or other government information.

Summary

The initial successes and challenges of using cryptocurrencies for social impact projects have inspired a new wave of innovation focused on blockchain. We have only scratched the surface of the tremendous opportunity in this area, as entrepreneurs and institutions around the world find ways to use the blockchain algorithm to empower the developing world, reach those in need, and build a better future for all.

Closing Note

We trust that by now you have become comfortable, and hopefully even enthusiastic, about the potential transformative power of the blockchain. Many have compared the development of bitcoin and its underlying blockchain with the development and adoption of the Internet. At that time, many remained skeptical of the Internet's application to financial transactions and the financial world more generally. Today, we cannot imagine an economy and financial system without the capabilities that the Internet offers. In five to 10 years, we may be sharing the same view of the blockchain.

Of course, the development of online transactions and e-commerce has generated numerous unique regulatory and legal issues for financial institutions and other participants in the financial world. To the extent that the blockchain will impact the financial system as much as some predict, the technology will similarly generate unique regulatory and legal issues that our clients must address. At Reed Smith, our focus on client services means staying ahead of the curve, and advising clients on the potential legal issues surrounding new technology as that technology develops. As your business or organization begins to devise strategies regarding cryptocurrencies and the blockchain, the Reed Smith Blockchain Technology Team and its members across our global offices are always available to advise you on the legal issues surrounding this exciting new technological development.

There is no doubt in our minds that the blockchain has the potential to effect significant changes in the financial world, and other industries, by providing the ability to have a transparent, immutable record of a transaction, without the need for trusted third-parties. As has been discussed throughout this white paper, some of the most exciting potential applications of the blockchain's distributed ledger technology arise outside of the cryptocurrency context. We hope that this white paper has provided you the tools to begin strategizing how the blockchain may impact, or even transform, your business and operations.

Sincerely,

The Reed Smith Blockchain Technology Team

Glossary of Terms

51% Attack (also Majority Attack)

The ability of someone controlling a majority of network hash rate or mining power to revise transaction history and prevent new transactions from confirming.

Bit

Bit is a common unit used to designate a sub-unit of a bitcoin - 1,000,000 bits is equal to 1 bitcoin (BTC or ฿). This unit is usually more convenient for pricing tips, goods and services.

Bitcoin

Bitcoin - with capitalization, is used when describing the concept of Bitcoin, the Bitcoin protocol, or the entire network itself, e.g., "I was learning about the Bitcoin protocol today."

bitcoin - without capitalization, is used to describe bitcoins as a unit of account, e.g., "I sent 10 bitcoins today." It is also often abbreviated BTC or XBT.

Bitcoin Exchange

A marketplace that allows people to buy or sell bitcoins using different currencies. Because of the blockchain algorithm, exchanges can be made securely upon transfer.

Bitcoin Foundation

An American nonprofit corporation founded in September 2012 and headquartered in Washington, D.C., with the stated mission to "standardize, protect and promote the use of Bitcoin cryptographic money for the benefit of users worldwide." See bitcoinfoundation.org.

BitLicense

A popular name for the business license (and its associated regulations) issued by the New York Department of Financial Services ("NYDFS") under regulations that came into effect August 8, 2015, designed for companies engaged in virtual currency business activities.

Block

A unit of data containing information regarding transactions that have occurred during a period of time. A block contains the hash code of the previous block in the blockchain, a set of transactions that are recorded in that block, and (if it exists), a reference to the following block in the blockchain.

Blockchain

A blockchain is a public ledger of all bitcoin transactions that have ever been executed. The term may also be used to more generally describe the distributed ledger technology utilized by the Bitcoin blockchain, even if applied outside of the Bitcoin context.

Block Height

A measure of the age of a digital ledger - the more blocks that are solved and added to the ledger, the higher the block height. When choosing between two distributed ledgers, the one with the higher block height will often be more secure, and therefore more likely to be accurate.

Byzantine Generals Problem

An abstraction of a computer system problem concerning the handling of malfunctioning components that give conflicting information to different parts of the system:

> A group of generals of the Byzantine army camped with their troops around an enemy city, and communicate only by messengers. The generals must agree upon a common battle plan; however, one or more of the generals may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors.

Bitcoin has frequently been extolled for solving the Byzantine Generals Problem with its applications of proof of work and consensus.

Cold Storage

The storage of a reserve of bitcoins or private keys offline, i.e., disconnected from the Internet, in a physical storage device such as a hard drive or USB storage device.

Consensus

A requirement for updating a distributed ledger requiring a sufficient number of participants to agree (usually more than half) before accepting the update as accurate.

Distributed Consensus

Refers to consensus from the various different computers making up the network coming to an agreement without the need for a central control unit making that determination, and then broadcasting it to the rest of the network This is at the crux of how Bitcoin operates.

Federated Consensus

Consensus achieved under what is known as a federated Byzantine agreement system, whereby consensus can be achieved from a "quorum slice," a subset of trustworthy nodes that have earned trust organically on the system over time.

Cryptocurrency

A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Cryptography

The use of mathematics to secure information and to convert data into a secret code for transmission over a public network. Today, most cryptography is digital, and the original text ("plaintext") is turned into a coded equivalent called "ciphertext" via an encryption algorithm.

Cryptographic Hash Function

A cryptographic hash function is a hash function that takes an input (or "message") and returns a fixed-size alphanumeric string, which is called the hash value (sometimes called a message digest, a digital fingerprint, a digest or a checksum).

The ideal hash function has three main properties:

- It is extremely easy to calculate a hash for any given data.
- It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.
- It is extremely unlikely that two slightly different messages will have the same hash.

Cypherpunk

An activist advocating widespread use of strong cryptography as a route to social and political change. Cypherpunks have been engaged in an active movement since the late 1980s.

Digital Currency (also e-Currency, e-Money, Electronic Cash, Electronic Currency, Digital Cash, Cyber Currency)

An electronic medium of exchange in which a person can securely pay for goods or services electronically without necessarily involving a bank to mediate the transaction.

Digital Signature

The combination of a public key, which identifies you to others, and a private key, which allows you to access secret information. Blockchain uses public keys to identify participants in the ledger, and requires private keys to allow participants to access assets recorded on the ledger.

Distributed Consensus

See ***Consensus***

Distributed Ledger

A record of transactions that is shared over a network with others without a central server or entity that others must connect to.

Double Spending

Double spending is the result of successfully spending the same unit of currency (e.g., the same bitcoin) more than once. Bitcoin protects against double spending by verifying each transaction added to the blockchain to ensure that the inputs for the transaction had not previously been spent.

Federated Consensus

See ***Consensus***

Fork

When miners produce simultaneous blocks at the end of the blockchain, each node individually chooses which block to accept. Absent other conditions that suggest a more stable block, nodes usually use the first block they see, and the problem is resolved once one chain has more proof of work than the other.

Hard Fork

A permanent divergence in the blockchain. A hard fork may occur when upgraded nodes

follow newer consensus rules previously considered invalid, and therefore newer nodes would recognize blocks as valid that older nodes would reject. This will cause non-upgraded nodes to not recognize and validate blocks created by upgraded nodes that follow newer consensus rules, creating a divergence.

Soft Fork

A temporary fork in the blockchain. A soft fork may occur when miners using non-upgraded nodes violate a new, stricter consensus rule of updated nodes. This would lead to non-upgraded nodes accepting certain blocks, while updated nodes would reject these same blocks. Provided that a majority of nodes become updated, a permanent fork in the blockchain may be avoided.

Hash

A kind of algorithm that converts a string of data (of any size) into another, usually smaller, fixed-size output in a reasonable amount of time. Generally, hashes are "one-way," which means that if you have the hash, you don't know the original value. Hashes are used in cryptography to compare and verify data without having to see the original.

Hot Storage

Refers to keeping a reserve of bitcoins on a web-based storage device or wallet.

Merkle Tree (or Hash Tree)

A cryptography term that refers to a data structure made up of linked nodes, called a tree. A Merkle tree is a tree in which every non-leaf node (a node with children) is labeled with the hash of the labels of its children nodes. Hash trees are useful because they allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

Mining / Miner

Mining is the process of making computer hardware do mathematical calculations to solve new blocks to add to the blockchain. In the case of Bitcoin, miners are rewarded with newly minted bitcoins. But in other applications of blockchain, miners may be rewarded in a different way, or not at all.

Mining Pool

Groups of people who mine together as a single unit in order to successfully mine faster by pooling computing resources.

Mt. Gox

Mt. Gox was a bitcoin exchange based in Tokyo, launched in July 2010, which by 2013 was handling 70 percent of all bitcoin transactions. In February 2014, the company suspended trading, subsequently closed its website and exchange service, and later filed for a form of bankruptcy protection from creditors. In April 2014, the company began liquidation proceedings and announced that approximately 850,000 bitcoins (valued at more than $450 million at the time) belonging to its customers and the company were missing and likely stolen. Although 200,000 bitcoins have since been "found,", the reason(s) for the disappearance—theft, fraud, mismanagement, or a combination of these—have remained unclear.

Multi-signature Address

A multi-signature address is associated with more than one private key.

Node

A node is a point of intersection/connection within a network. Any computer that connects to the Bitcoin network is called a node. Nodes share a copy of the blockchain and relay transactions to other nodes.

Nonce

The name for the string of digits that is added to a new block by miners when attempting to add this new block to the blockchain. The goal is to find the nonce that, when linked with the previous hash and the list of transactions comprising the new block, will produce a hash output falling below a certain target value. Once the correct nonce is found, the new block is added to the Blockchain. Because it is impossible to predict what nonce will result in the correct target value, such a calculation involves computing and re-computing a hash output for numerous nonce values by "brute force." Presentation of the new block with the correct nonce value constitutes proof of work.

Peer-to-Peer

Describes a type of network where each participant is considered equal. Peer-to-peer networks share information without a central server, controller, or authority. Participants are often connected to a few neighbors that will pass information to the rest of the network, and vice versa.

Proof of Stake

Proof of stake is a method by which a cryptocurrency blockchain network aims to achieve distributed consensus. While the proof-of-work method asks users to repeatedly run hashing algorithms to validate electronic transactions, proof of stake asks users to prove ownership of a certain amount of currency (their "stake" in the currency). Peercoin was the first cryptocurrency to launch using proof of stake.

Proof of Work

Data that is difficult to produce, but easy to verify. Blockchain uses proof of work to ensure new blocks of records added to the ledger are legitimate, because the miner invested work in producing the new block.

Private Key

The unpublished key in a public key cryptographic system, which uses a two-part key: one private and one public. The private key is kept secret and never transmitted over a network. Contrast with "public key," which can be published on a website or sent in an ordinary email message.

Public Key

An encryption key that can be made public or sent by ordinary means, such as by an email message. See also ***private key*** and ***public key cryptography.***

Public Key Cryptography

A cryptographic system in which a two-part key is used: one public key and one private key.

Satoshi

The smallest usable denominations of bitcoin value. One bitcoin equals 100,000,000 satoshis.

Satoshi Nakamoto

The pseudonym of a person or group of people who created the Bitcoin protocol and reference software, Bitcoin Core (formerly known as Bitcoin-Qt).

Silk Road

Silk Road was an online black market and the first modern darknet (a network overlay that is only accessible by using non-standard communications protocols and ports) market, best known as a platform for selling illegal drugs. All products sold on the site could be purchased anonymously with bitcoin.

Smart Contract

Contracts allowing for contract performance to be verified and technically enforced, without requiring a judicial system or other centralized third party. While implementation of these new solutions are still fairly theoretical, a number of companies are actively building software solutions for smart contracts.

Sybil Attack

An attack to the Bitcoin network where an attacker attempts to fill the network with nodes disguised to appear as unique network participants, but which in reality are nodes controlled by the attacker.

Virtual Currency

"Virtual currency" is defined by the European Central Bank as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community," and by the European Banking Authority as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically." The Financial Crimes Enforcement Network ("FinCEN"), a bureau of the U.S. Treasury Department, has also defined virtual currency in its guidance published in 2013.

Wallet

The digital equivalent of a physical wallet containing private key(s). Each wallet can show the total balance of all bitcoins it controls and lets users pay a specific amount to a specific person

Key Contacts

Angela Angelovska-Wilson
Partner
Washington, D.C.
+1 202 414 9294
aawilson@reedsmith.com

Marc Kaufman
Partner
Washington, D.C.
+1 202 414 9249
mkaufman@reedsmith.com

Ranajoy Basu
Partner
London
+44 (0)20 3116 2827
rbasu@reedsmith.com

Paul Bond
Partner
Princeton
+1 609 520 6393
pbond@reedsmith.com

Ed Estrada
Partner
New York
+1 212 549 0247
eestrada@reedsmith.com

Anthony Ford
Associate
New York
+1 212 549 0376
aford@reedsmith.com

Jacqui Hatfield
Partner
London
+44 (0)20 3116 2971
jhatfield@reedsmith.com

Tyree Jones, Jr.
Partner
Washington, D.C.
+1 202 414 9296
tpjones@reedsmith.com

Mark Melodia
Partner
New York
+1 212 205 6078
mmelodia@reedsmith.com

Andrew Moss
Partner
Chicago
+1 312 207 3869
amoss@reedsmith.com

Cynthia O'Donoghue
Partner
London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

Carolyn Rosenberg
Partner
Chicago
+1 312 207 6472
crosenberg@reedsmith.com

Evan Thorn
Associate
Washington, D.C.
+1 202 414 9204
ethorn@reedsmith.com

Stephen Winter
Associate
Chicago
+1 312 207 2439
swinter@reedsmith.com

Endnotes

Chapter 1

[1] The terms "cryptocurrency," "virtual currency," and "digital currency" are sometimes incorrectly used interchangeably. "Digital currency" is the broadest term, and means an Internet-based medium of exchange with characteristics similar to physical currencies. "Virtual currency" is a subset of digital currency, and is defined by the European Banking Authority as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically." Finally, "cryptocurrency" is a subset of "virtual currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds.

[2] https://bitcoin.org/bitcoin.pdf.

[3] "Bitcoin" with a capital B refers to the protocol or software, whereas "bitcoin" (lower case b) refers to the unit of currency.

[4] Please see Chapter 2 – "Blockchain 101" – for a more detailed discussion of the blockchain.

[5] http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg.

Chapter 2

[6] http://radar.oreilly.com/2015/01/understanding-the-blockchain.html

[7] https://bitcoin.org/bitcoin.pdf

[8] "Encryption at rest" refers to the practice of storing data in an encrypted form so that only the owner of a digital key or password can access it.

[9] http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin

[10] Melanie Swan, Blockchain: Blueprint for a New Economy, 2015, O'Reilly Media, Sebastopol, Calif.

Chapter 3

[11] Sydney Ember, New York Proposes First State Regulations for Bitcoin, New York Times DealBook (July 17, 2014), http://dealbook.nytimes.com/2014/07/17/lawsky-proposes-first-state-regulations-for-bitcoin/?_r=0.

[12] 23 N.Y.C.R.R. Part 200 (Virtual Currencies), available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (hereinafter, "BitLicense").

[13] New York Department of Financial Services, Press Release: NYDFS Announces Approval of First BitLicense Application from a Virtual Currency Firm (Sept. 22, 2015), http://www.dfs.ny.gov/about/press/pr1509221.htm.

[14] *Id.*

[15] *See, e.g.,* Daniel Roberts, Bitcoin company ditches New York, blaming new regulations, Fortune (June 11, 2015), http://fortune.com/2015/06/11/bitcoin-shapeshift-new-york-bitlicense/.

[16] BitLicense § 200.2(p).

[17] *Id.* § 200.3(a).

[18] *Id.* § 200.2(q).

[19] Nermin Hajdarbegovic, Lawsky: Bitcoin Developers and Miners Exempt from BitLicense, CoinDesk (Oct. 15, 2014), http://www.coindesk.com/lawsky-bitcoin-developers-miners-exempt-bitlicense/.

[20] *Id*

[21] BitLicense § 200.2(q).

[22] *Id.* § 200.2(q)(1).

[23] *Id.* §§ 200.3(a), 200.4, 200.5, 200.21.

[24] *Id.* § 200.6.

[25] *Id.*

[26] *Id.* § 200.4(c).

[27] *Id.* § 200.10.

[28] *Id.* § 200.6.

[29] *Id.* §§ 200.12(a), 200.15.

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id. § 200.8.*

[37] *Id.* § 200.9.

[38] *Id.* § 200.12.

[39] *Id.* § 200.19.

[40] *Id.* § 200.20.

[41] *Id.* § 200.18.

[42] *Id.* § 200.19(g).

[43] *Id.* § 200.16.

[44] *Id.* § 200.17.

[45] *Id.* § 200.13.

[46] *Id.* § 200.14.

[47] Conference on State Bank Supervisors, State Regulatory Requirements for Virtual Currency Activities, CSBS Model Regulatory Framework (Sept. 15, 2015), *available at* https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf.

[48] *Id.*

[49] A.B. 1326, Cal. Leg. 2015-2016 Reg. Sess. (Cal. 2015), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1326.

[50] *Id.*

[51] Yessi Bello Perez, California's Bitcoin Bill Shelved by State Senator, CoinDesk (Sept. 16, 2015), http://www.coindesk.com/californias-bitcoin-bill-shelved-by-state-senator/.

[52] Washington State Department of Financial Institutions, Bitcoin and Virtual Currency Regulation, http://www.dfi.wa.gov/bitcoin.

[53] Kansas Office of the State Bank Commissioner, Regulatory Treatment of Virtual Currencies under the Kansas Money Transmitter Act, Guidance Document MT 2014-01 (June 6, 2014), available at http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf; Texas Department of Banking, Regulatory Treatment of Virtual Currencies under the Texas Money Services Act, Supervisory Memorandum – 1037 (April 3, 2014), available at http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf.

[54] Merkle Tree, US State-level Digital Currency Law & Regulation, http://merkletree.io/blog/2015/07/us-state-level-digital-currency-law-regulation/.

[55] U.S. Commodity Futures Trading Commission, CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering, Release: PR7231-15 (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 (hereinafter, "Coinflip Settlement").

[56] See generally Commodity Exchange Act, 49 Stat. 1491, 7 U.S.C. §§ 1, et seq.

[57] 7 U.S.C. § 1a(9).

[58] *See, e.g.,* U.S. Commodity Futures Trading Commission, Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry (Dec. 10, 2014), available at http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6.

[59] Coinflip Settlement.

[60] 31 C.F.R. § 1010.100(ff).

[61] 31 C.F.R. § 1010.100(ff)(5)(i)(A) (emphasis added).

[62] U.S. Department of the Treasury, FinCEN, BSA Requirements for MSBs, https://www.fincen.gov/financial_institutions/msb/msbrequirements.html.

[63] 18 U.S.C. § 1960.

[64] U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013), available at https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[65] *Id.*

[66] U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (Jan. 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R001.html.

[67] U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013), *available at* https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[68] U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (Jan. 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R001.html.

[69] U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002 (Jan. 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R002.html.

[70] U.S. Department of the Treasury, FinCEN, Application of Money Services Business regulations to the rental of computer systems for mining virtual currency, FIN-2014-R007 (Apr. 29, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R007.html.

[71] U.S. Department of the Treasury, FinCEN, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform , FIN-2014-R011 (Oct. 27, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R011.html.

[72] Id.

[73] U.S. Department of the Treasury, FinCEN, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R012.html.

[74] U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals, FIN-2015-R001 (Aug. 14, 2015), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2015-R001.html.

[75] Letter from Mary Jo White, Chair, U.S. Securities and Exchange Commission to Sen. Thomas R. Carper (Aug. 30, 2013), available at http://online.wsj.com/public/resources/documents/VCurrenty111813.pdf.

[76] Internal Revenue Service, IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply, IR-2014-36 (Mar. 25, 2014), https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

[77] Coinflip Settlement.

[78] U.S. Department of the Treasury, FinCEN, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), https://www.fincen.gov/news_room/nr/html/20150505.html.

[79] U.S. Securities and Exchange Commission, Final Judgment Entered Against Trendon T. Shavers, A/K/A/ "Pirateat40" - Operator of Bitcoin

Ponzi Scheme Ordered to Pay More Than $40 Million in Disgorgement and Penalties, Litigation Release No. 23090 (Sept. 22, 2014), https://www.sec.gov/litigation/litreleases/2014/lr23090.htm.

[80] U.S. Securities and Exchange Commission, SEC Sanctions Operator of Bitcoin-Related Stock Exchange for Registration Violations, Press Release 2014-273 (Dec. 8, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543655716.

[81] U.S. Securities and Exchange Commission, SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities, Press Release 2014-111 (June 3, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520.

[82] U.S. Attorney's Office for the Southern District of New York, Press Release: Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), https://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison.

[83] U.S. Attorney's Office for the Southern District of New York, Press Release: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court (Nov. 6, 2014), https://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.

[84] U.S. Attorney's Office for the Southern District of New York, Press Release: Bitcoin Exchanger Sentenced In Manhattan Federal Court To Four Years In Prison For Selling Nearly $1 Million In Bitcoins For Drug Buys On Silk Road (Jan. 20, 2015), http://www.justice.gov/usao-sdny/pr/bitcoin-exchanger-sentenced-manhattan-federal-court-four-years-prison-selling-nearly-1.

Chapter 4

[85] Case C-264/14, *Skatteverket v. David Hedqvist* (Oct. 22, 2015), available at http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dd8ccd881260ee4096a4a6a9b3d479002e.e34KaxiLc3qMb40Rch0SaxuRbxn0?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=170305&occ=first&dir=&cid=854516 ("ECJ Ruling").

[86] *See infra*, III.B.1

[87] ECJ Ruling.

[88] Digits: Tech News & Analysis from the WSJ, EU Rules Bitcoin Is a Currency, Not a Commodity—Virtually (Oct. 22, 2015), http://blogs.wsj.com/digits/2015/10/22/eu-rules-bitcoin-is-a-currency-not-a-commodity-virtually/.

[89] CNBC Tech Transformers, Bitcoin now tax-free in Europe after court ruling (Oct. 22, 2015), http://www.cnbc.com/2015/10/22/bitcoin-now-tax-free-in-europe-after-court-ruling.html.

[90] European Banking Authority, EBA Opinion on 'virtual currencies,' EBA/Op/2014/08 (July 4, 2014), available at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

[91] *Id.* at 5.

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.* at 6.

[96] *Id.*

[97] Sarah Jane Hughes and Stephen T. Middlebrook, *Advancing a Framework for Regulating Virtual Currency Payments Intermediaries*, 32 Yale J. Reg. 496 (2015); Merkle Tree, http://merkletree.io.

[98] Robleh Ali, John Barrdear, Roger Clews and James Southgate, Bank of England Quarterly Bulletin 2014 Q3, Innovations in payment technologies and the emergence of digital currencies, http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf.

[99] State Secretariat for International Financial Matters SIF, Federal Council publishes report on virtual currencies such as bitcoin (June 25, 2014), https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilungen.msg-id-53513.html.

[100] State Secretariat for International Financial Matters SIF, Federal Council publishes report on virtual currencies such as bitcoin (June 25, 2014), https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilungen.msg-id-53513.html.

[101] Merkle Tree.

[102] Reuters, Russian authorities say Bitcoin illegal (Feb. 9, 2014), http://www.reuters.com/article/2014/02/09/us-russia-bitcoin-idUSBREA1806620140209,

[103] Central Bank of Iceland, Significant risk attached to use of virtual currency (Mar. 19, 2014), http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency/.

[104] Why Bangladesh will jail Bitcoin traders, The Telegraph (Sep. 15, 2014), http://www.telegraph.co.uk/finance/currency/11097208/Why-Bangladesh-will-jail-Bitcoin-traders.html.

[105] China Central Bank Warns Banks on Bitcoin, *Wall Street Journal* (May 7, 2014), http://www.wsj.com/articles/SB10001424052702304655304579547251552490962; Alex Hern, Bitcoin price tumbles after warning from Chinese central bank, *The Guardian* (Dec. 5, 2013), http://www.theguardian.com/technology/2013/dec/05/bitcoin-price-tumbles-chinese-central-bank-warning.

[106] Pathom Sangwongwanich, Bitcoins back in the Thai marketplace, *Bangkok Post* (Feb. 20, 2014), http://www.bangkokpost.com/business/marketing/395952/bitcoins-back-in-the-thai-marketplace.

[107] Japan's ruling party says won't regulate bitcoin for now, Reuters (June 19, 2014), http://www.reuters.com/article/2014/06/19/japan-bitcoin-idUSL4N0P01LS20140619.

[108] Virtual Currencies: International Actions and Regulations, Perkins Coie (last updated Oct. 2015), https://www.perkinscoie.com/en/news-insights/virtual-currencies-international-actions-and-regulations.html#Japan.

[109] Christine Duhaime, Canada implements world's first national digital currency law; regulates new financial technology transactions, Duhaime Law Notes (June 22, 2014, updated July 30, 2014),

http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] Stan Higgins, Ecuador Bans Bitcoin, Plans Own Digital Money, CoinDesk (July 25, 2014), http://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote/; Jim Wyss, Ecuador's new virtual currency is a source of pride, worry, *Miami Herald* (Aug. 12, 2015), http://www.miamiherald.com/news/nation-world/world/americas/article30968391.html.

[114] *Id.*

[115] Pete Rizzo, Bolivia's Central Bank Bans Bitcoin, CoinDesk (June 19, 2014), http://www.coindesk.com/bolivias-central-bank-bans-bitcoin-digital-currencies/.

[116] Hughes and Middlebrook; Merkle Tree.

[117] *See* Merkle Tree.

[118] Farhaanah Mahomed, S.African Financial Authorities Warn Against Virtual Currencies, CNBC Africa (Feb. 12, 2015), http://www.cnbcafrica.com/news/southern-africa/2014/09/18/virtual-currencies-warning/.

[119] *Id.*

Chapter 5

[120] In this chapter references to "bitcoin" generally also refer to similar derivative cryptocurrencies.

[121] *SEC v. Shavers*, No. 4:13CV416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013).

[122] China has taken steps to restrict the use of bitcoin. *See Bitcoin in China: A dream dispelled, Chinese regulators make life hard for crypto-currencies*, *The Economist*, Apr. 12, 2014, *available at* http://www.economist.com/news/finance-and-economics/21600736-chinese-regulators-make-life-hard-crypto-currencies-dream-dispelled.

[123] See Chapters 5 & 7 of this White Paper, discussing security concerns particular to bitcoin; *see also Lloyd's Bitcoin Report.*

[124] Hannover Group has modified its commercial crime policy by endorsement to include "Bitcoins" in its definition of "Money." *See Bitpay, Inc. v. Massachusetts Bay Ins. Co.,* No. 1:15-cv-03238 (N.D. Ga.) (Ex. A to Bitpay's compl., at Doc. 1-1, Manuscript End. 1).

[125] See Press Release, "Great American Insurance Group First to Offer Bitcoin Coverage to Commercial and Governmental Entities," available at http://www.businesswire.com/news/home/20140602006331/en/Great-American-Insurance-Group-Offer-Bitcoin-Coverage (last visited Oct. 16, 2015).

[126] *Bitpay, Inc. v. Massachusetts Bay Ins. Co.,* No. 1:15-cv-03238 (N.D. Ga.).

[127] *See* https://www.bitgo.com/insurance (last visited Oct. 16, 2015).

[128] *See supra*, Note 8.

[129] *See* https://support.xapo.com/insurance (last visited Oct. 7, 2015).

Chapter 6

[130] *See*, e.g., Nathaniel Popper, Bitcoin Technology Piques Interest on Wall St., New York Times DealBook (Aug. 28, 2015), http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0.

[131] Edward Robinson and Matthew Leising, Blythe Masters Tells Banks the Blockchain Changes Everything, BloombergBusiness (Aug. 31, 2015), http://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything; Jemima Kelly, Nine of world's biggest banks join to form blockchain partnership, Reuters (Sept. 15, 2015), http://www.reuters.com/article/2015/09/15/us-banks-blockchain-idUSKCN0RF24M20150915#vbbT0RlRCTT8TkRP.97.

[132] Accenture, Blockchain in the Investment Bank (2015), available at https://www.accenture.com/t20150811T015521__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_13/Accenture-Blockchain-Investment-Bank.pdf#zoom=50.

[133] Nathaniel Popper, Bitcoin Technology Piques Interest on Wall St., New York Times DealBook (Aug. 28, 2015), http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0.

[134] https://www.greenwich.com/greenwich-research/research-documents/greenwich-reports/2015/jul/is-digital-ledger-tech-2015-gr

[135] http://www.efinancialnews.com/story/2015-09-10/capital-markets-blockchain-spend-to-reach-400-million-by-2019

[136] *See*, *e.g.,* Joanna Payne, Stock Settlement: Why You Need to Understand the T+3 Timeline, Charles Schwab (May 21, 2014), http://www.schwab.com/public/schwab/nn/articles/Stock-Settlement-Why-You-Need-to-Understand-the-T-3-Timeline.

[137] *See, e.g.*, Kristen Haunss, With Loan Market Still Using Faxes, Settlement Times Trail Goal, BloombergBusiness (Apr. 2, 2015), http://www.bloomberg.com/news/articles/2015-04-02/with-loan-market-still-using-faxes-settlement-times-trail-goal.

[138] Nasdaq, Press Release: Nasdaq Announces Inaugural Clients for Initial Blockchain-Enabled Platform "'Nasdaq Linq" (Oct. 27, 2015), http://www.nasdaq.com/press-release/nasdaq-announces-inaugural-clients-for-initial-blockchainenabled-platform-nasdaq-linq-20151027-00986#ixzz3qXDjeI7z.

Chapter 7

[139] *Privacy-enhancing technologies for the Internet*, Ian Goldberg, David Wagner, Eric Brewer, University of California, Berkeley (1997), available at https://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html.

[140] *Id.*

[141] *How Anonymous is Bitcoin? A Backgrounder for Policymakers*, Adam Ludwin (January 25, 2015), available at http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/.

[142] *Id.*

[143] *How Anonymous is Bitcoin? A Backgrounder for Policymakers*, Adam Ludwin (January 25, 2015), available at

http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/.

[144] DRAFT NISTIR 8053 1, *De-Identification of Personally Identifiable Information*, Simon L. Garfinkel, National Institute of Standards and Technology, U.S. Department of Commerce (April 2015) ("Deidentification Standards"), p. 5.

[145] Deidentification Standards, p. 6.

[146] *Id.*

[147] *Id.* at 17.

[148] Deidentification Standards, p. 17.

[149] *Opinion 05/2014 on Anonymisation Techniques*, Article 29 Working Group (Adopted 10 April 2014), p. 5.

[150] *Id.* at 17.

[151] *Id.* at 22.

[152] *Id.*

Chapter 8

[153] http://www.forbes.com/sites/laurashin/2015/08/19/change-tip-and-direct-relief-launch-charitable-campaign-using-bitcoin/

[154] http://bitgivefoundation.org/bitcoin-charity-2-0-initiative/

[155] https://www.foreignaffairs.com/articles/2015-02-26/bitcoin-unbanked

[156] http://techcrunch.com/2015/01/30/the-bootstrappers-guide-to-bitcoin-remittances/

[157] https://www.bitpesa.co/guide

[158] https://coins.ph/teller

[159] http://www.digitalcitizenfund.org/

[160] http://codetoinspire.org/

[161] http://nytlive.nytimes.com/womenintheworld/2015/09/07/ceos-afghan-citadel-teaches-women-in-afghanistan-how-to-code/

[162] http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

[163] http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0O01V720150515