McGUIREWOODS

Bitcoin Basics for Corporate Counsel

STEVE GOLD, PARTNER
312.321.7664 | sgold@mcguirewoods.com
77 West Wacker Drive
Suite 4100
Chicago, IL 60601

May 2015
www.mcguirewoods.com

Bitcoin, the online "cryptocurrency," is not just for anti-government doomsday fanatics and drug dealers. Seen everywhere from SEC filings, to state legislature hearings, to an episode of *The Good Wife*, it is both an influential new Internet technology and a new financial medium that will have a growing impact on corporate enterprises across the economy.

Corporate counsel who support technology transactions are likely to face a variety of legal issues of first impression as corporate planners, strategists, investors and consumers find new applications and run into old problems with this technology. This article will catalog eight of the most salient aspects of Bitcoin that corporate counsel should understand.

What is Bitcoin?

Touted as a new currency and as a disruptive technology, Bitcoin is both. At its most basic Bitcoin is little more than a shared online ledger, called the "blockchain," that lists every bitcoin transaction that has ever occurred. Users interact with the blockchain through software referred to as a bitcoin "wallet." It is the complex cryptography that secures the blockchain and the clever incentive structure for volunteers to maintain the blockchain and earn new bitcoins that makes Bitcoin sophisticated, practical and disruptive.

Bitcoin was created in 2009, based on a paper posted to the Internet in late 2008 under the (most likely pseudonymous) name Satoshi Nakamoto. Nakamoto's paper outlined the underlying technical details: Ownership of an entry in the blockchain is demonstrated by possession of a cryptographic private key (in a Bitcoin wallet) that is mathematically tied to the numerical designator (a Bitcoin address) of that entry. The blockchain is also protected against tampering by a process called "mining," which rewards new bitcoins to the first computer on the Bitcoin[1] network that successfully solves a mathematical calculation associated with validating additional blockchain entries. The costs and incentives of mining are designed to make it unfeasibly difficult to introduce nonexistent transactions into the blockchain (i.e., to "double spend" a bitcoin).

It is the complex cryptography that secures the blockchain and the clever incentive structure for volunteers to maintain the blockchain and earn new bitcoins that makes Bitcoin sophisticated, practical and disruptive.

Online reports indicate that as of spring 2015 there may be as many as 5 million Bitcoin wallets holding the more than 14 million bitcoins now in existence. The value of a bitcoin has fluctuated from about $14 at the beginning of 2013, to a high of $979 late that year. In May 2015, the price fluctuated between approximately $225 and approximately $250.

[1] By convention, "Bitcoin" – capitalized – refers to the software, protocol and entire network, while "bitcoin" – not capitalized – refers to the unit of account.

Eight Things Corporate Counsel Should Know

1. Bitcoin is a Decentralized System

Bitcoin does not rely on a government as the issuer of currency or on a software company that controls its existence – anyone can join the network and the core software is open source. It is, however, dependent on the volunteer software developers that maintain and modify the core network and mining software and on the many "miners" who maintain the blockchain. If, for example, too few miners were validating transactions, the entire system would be open to manipulation.

2. Bitcoin is Not Anonymous

Bitcoin has been called anonymous, but that is not entirely accurate. It is anonymous in the limited sense that no personally identifying information is required to be stored as part of the blockchain. Every transaction, however, is publicly traceable. If it becomes known who controls a particular Bitcoin address it is an easy matter to see the Bitcoin addresses that sent or received those bitcoins. Although a lot of Bitcoin's publicity has associated it with online anonymous drug markets, its public traceability has proven to be an Achilles' heel, or at least a significant burden, for law evaders, so Bitcoin has far more utility for law-abiding transactions.

3. Bitcoin is Currently in Use

Bitcoin is becoming more widely used, with approximately 100,000 transactions per day being added to the blockchain. Many well-known businesses have begun to accept bitcoin as payment, and bitcoin can be spent many more places through third-party relationships with bitcoin payment processors and gift cards. Bitcoin also has two very attractive features for its use for funds transfer: essentially no transfer fee and quick processing. Although a future change to this structure is built into the Bitcoin protocol, at present all transfer fees are essentially paid out of the Bitcoin network as a whole through mining rewards, so any amount of bitcoin can be transferred (anywhere) without the payment of a transaction fee. The protocol also is designed so the time to make a transfer is short: Assuming that sufficient miners are working on updating the blockchain, new transactions will be added approximately every 30 minutes, though additional cycles of mining are required in order to assure security. The handling of transaction fees, and the fact that payments are accounted for to eight decimal places, also makes Bitcoin attractive for micro payment applications.

4. Thefts Have Resulted from Failures Outside the Bitcoin Protocol Itself

There have been many press reports about collapsed bitcoin exchanges and millions of dollars of lost or stolen bitcoins. Those losses, so far as has been reported, do not arise out of insecurities in Bitcoin's software, the cryptography on which it is based, or the Bitcoin network. Indeed, the nature of a Bitcoin transaction is theoretically more secure than a credit card transaction because a buyer paying with bitcoin need not give any sensitive information about his bitcoins to the seller, while a buyer paying with a credit card generally has to give the seller her credit card number. From the seller's perspective, a Bitcoin transaction may be more secure than a credit card payment because there is no intermediary that might reverse or charge back the transaction. Once bitcoins are transferred and recorded on the blockchain, they are fully controlled by the recipient.

The publicly reported losses have resulted from thefts or failures outside the blockchain itself. There are many reasons for this, but one of the most significant is that current Bitcoin wallet software is at an

early stage of usability development and remains complex for many users. So, rather than operate the software themselves, users have their bitcoins held online by third parties. In quite a few cases, those third parties have not proven trustworthy.

5. Bitcoin Isn't the Only Game in Town

Bitcoin is only the most well-known and most widely adopted of many similar crypto-currencies that have emerged over the last few years. At least 25 different crypto-currencies each had total market capitalizations over $1 million in May 2015, according to online sources. Bitcoin, however, is the most significant one, with a total value over $3.5 trillion, nearly 15 times the total value of Ripple, the next largest entry.

6. Blockchain Technology is the Real Breakthrough

According to many observers, the importance of Bitcoin goes well beyond bitcoin itself as a currency. The Bitcoin blockchain is said to represent both an important advance in computer science and a disruptive innovation that has a wide variety of applications. Some well-known blockchain advocates claim that the technology, though at an early stage today, will be as important as, for example, the development of the TCP/IP protocol that was the foundation of the Internet, the worldwide web and all of the online world built around those.

In this view, blockchain technology is a way to keep a reliable electronic record of things and transactions, not just bitcoins, without the need for a central authority. Possible applications, some of which are already under development, include using something like the blockchain to manage other technological assets (such as data storage locations); records of ownership of other financial assets, such as securities; or even physical assets.

Blockchain transactions themselves are also programmable, which opens even more possible applications. It is theoretically possible, for example, for a blockchain-based financial instrument to automatically make payments over time, or for a blockchain-based escrow to respond to external inputs in order to settle a transaction.

Recently Nasdaq announced plans to leverage blockchain technology as part of an enterprise-wide initiative to expand and enhance the equity management capabilities offered by its Nasdaq Private Market platform.

7. People (and Governmental Agencies) are Taking Notice

Because of these many possible future applications, as well as the current financial uses of Bitcoin (and the other similar systems), Bitcoin has received a considerable amount of attention. Highlights include the following:

- The IRS has, in early 2014, issued guidance on the treatment of bitcoins for United States federal income tax purposes. The IRS notice and "frequently asked questions" took the position that bitcoins should be treated as property for tax purposes, that transactions in bitcoins (including mining) are subject to tax, tax withholding and tax reporting to the same extent as transactions involving other forms of property.

- The New York State Department of Financial Services is preparing to implement financial regulation over certain economic participants in the Bitcoin financial systems, with other states likely to follow suit. The regulation is going to impose money laundering and capital requirements on businesses that exchange bitcoin into other currencies for consumers. Without the state-level regulations in place, federal officials are already taking notice of Bitcoin and, in fact, fined Ripple (one of the largest currencies other than Bitcoin) for violating anti-money laundering requirements.
- At least two state legislatures have initiated studies into whether facilities could be established for taxpayers in their states to pay taxes in bitcoin.
- In March 2015, the UK Treasury issued a report in which it acknowledged the potential of innovation of digital currencies and undertook further investigation and regulation. Several other countries with strict currency controls have taken steps to ban or restrict bitcoin.
- One of the leading Silicon Valley venture capital firms is actively promoting the significance of Bitcoin and investing in several startup ventures that are seeking to capitalize on Bitcoin.
- Finally, as an indication of the penetration of Bitcoin into popular culture, the mystery surrounding Bitcoin's creation (recently renewed in the business section of The New York Times) has appeared in a highly rated network TV show. Popular CBS drama The Good Wife devoted an episode to a fictionalized Satoshi Nakamoto-like character seeking legal advice related to an investigation by the secret service.

8. Legal Issues Will Abound

Bitcoin and blockchain technology will raise a wide variety of legal issues that may cross corporate counsel's desk. Some of these could arise right now, as businesses seek to take advantage of the existing capabilities of Bitcoin, while others will be relevant to strategy and planning for the wide variety of possible future applications.

- **Licensing and regulatory compliance.** For any entity already in, or seeking to enter, a business that directly involves providing exchange or other financial services around Bitcoin, advice on licensing and regulatory compliance is a "must," along with constant monitoring and adjustment as regulation expands and matures. Those issues will be heavily influenced by geography, with many countries around the world taking very different approaches to bitcoin regulation.
- **Data security.** Similarly, any business lawyer in a business that receives funds from consumers also should be monitoring developments with a particular focus on the contractual and data security aspects of receiving and handling consumer funds, whether in bitcoin or other media. The payments industry as a whole is under disruption – Bitcoin, Square, smartphone-based payments and other new competitors in that area are likely to be expanding dramatically over the coming months and years. Because of the decentralized, irrevocable nature of bitcoin transfers, any payment application for bitcoin will require close attention to legal developments affecting data security and encryption.
- **Third-party contractual arrangements.** For businesses that outsource the handling of bitcoin transactions, close attention will be required regarding the contractual arrangements with third-party processors. In Bitcoin, the usual centralized infrastructure of the banks and payment card industry does not exist. Indeed, eliminating fees to those entities is part of the attraction of Bitcoin. But without those intermediaries and without standards yet in existence, every relationship will be unique and require attention to such things as chargebacks, transaction documentation, equipment, security, effect of errors, and all the other aspects of a payment system's rules.

- **Liability.** As Bitcoin and blockchain technology are applied outside of the payments environment, lawyers will have wide latitude (and few fixed direct precedents) to establish the basic parameters of accountability and trust. Contractual, industry or legislative steps will be needed to establish appropriate allocation of liability for transactions that go wrong, particularly if circumstances arise in which the distributed blockchain itself is at fault (or is alleged to be at fault) for a party's losses. Beyond that, difficult questions of attribution can arise if automated transaction steps (repetitive withdrawals of consideration over time, for example) were carried out without human intervention and without even a single human-owned computer being responsible, but rather distributed responsibility occurring over the blockchain.
- **Jurisdiction.** As with any online legal issue, there will be the question of which jurisdiction's laws will apply and which courts will decide the issues. These questions have long been an academic concern for Internet-mediated transactions, even if they turned out to be of very little practical concern. Blockchain transactions will raise these issues to a much greater degree. An Internet transaction can be problematic because it might not be clear which of many physical locations' laws apply; in a blockchain transaction, by contrast, it is almost a certainty that a great many geographically scattered physical locations will be implicated simultaneously.

McGuireWoods' technology and outsourcing practice team supports a wide range of business transactions driven by technology. In addition to counseling companies on the legal issues arising out of the applications of the latest technologies such as Bitcoin, the team assists in all phases of documenting, negotiating and handling disputes in connection with IT procurements, outsourcings, ERP implementation and data security. Our clients include Fortune 1000 corporations and emerging business enterprises spanning the industry spectrum. The practice team is chaired by Steve Gold in McGuireWoods' Chicago office.