SHOP TALK

Blockchain & Cryptocurrency—Two Roads Converge

By JUSTIN E. HOBSON

JUSTIN E. HOBSON is an attorney with the law firm of Lane Powell PC in Portland, Oregon.

Blockchain and cryptocurrency are two well-known buzzwords these days. Most people are familiar with Bitcoin, the cryptocurrency that relies on blockchain technology. But what is blockchain? Or cryptocurrency? And what impacts will they have on state taxation?

Background

Bitcoin is a cryptocurrency that originated with a so-called white paper from 2008 written by someone claiming to be Satoshi Nakamoto. However, the identity of Satoshi Nakamoto is unknown. Nakamoto’s white paper detailed a “peer-to-peer electronic cash system.” The intent of the system was to enable peer-to-peer currency transfers without the aid of financial institutions. The timing of Bitcoin’s launch is notable—about the same time in 2008 the “Great Recession” hit and multiple financial institutions failed. As a result of these events, the public lacked trust in financial institutions and the appetite for an alternative to them grew.

Bitcoin operates on a blockchain. A blockchain is nothing more than a transactional ledger. The blockchain relies on timestamps and cryptographic signatures. Timestamps ensure that a Bitcoin holder does not attempt to spend the same currency more than once (akin to over-drafting your checking account and writing multiple bad checks). Cryptographic signatures deter fraudulent transactions.

Each time a transfer is initiated, a Bitcoin holder combines his wallet address with a private key to digitally sign the transaction and creates a transaction hash. Then the holder broadcasts the transaction to the Bitcoin network. Sophisticated computers verify the transaction through a process called proof of work.
mining. The network aggregates multiple transactions into a block. The blocks are sequentially numbered and form a chain—hence the term blockchain.

Following the launch of Bitcoin, multiple competitors emerged. The second largest cryptocurrency by market cap is Ether and runs on the Ethereum network. Ethereum adds incremental improvements over the Bitcoin network through several features. Most notably, Ethereum utilizes “smart contracts.”

Smart contracts are not legal contracts in any sense of the word. They represent computer programmed logic based transactions. For example, you can initiate a transaction that will self-execute when predefined conditions are met. Smart contracts open limitless potential use cases beyond the simple peer-to-peer transactions first envisioned by Bitcoin.

Simple smart contracts could mirror the traditional contracts we see today. For instance, the financing company for a new vehicle could require a smart contract that automatically makes payments every month. Smart contracts could also revolutionize trust and estate practices. A smart contract could automatically self-execute one or more transfers upon death. Beyond these examples probably lie a number of smart contract possibilities just waiting to be dreamt up by the next generation of startup companies.

Real world application?

With all of this potential, you might be asking yourself (with good reason), if blockchain has all of these great uses, why are its most well-known uses illicit? There are a couple reasons illicit markets adopted cryptocurrency. First, the lack of a financial institution in the middle is attractive to illicit markets due to the “know-your-customer” and anti-money laundering rules. Without the man in the middle, cryptocurrency changes hands freely without the fear of financial institutions notifying authorities. Second, most cryptocurrencies are pseudonymous.

Both of these reasons make for a more attractive option for illicit activities than relying on financial institutions to move cash or engaging in face-to-face transactions. However, pseudonymous does not mean anonymous. Federal authorities have successfully associated Bitcoin transactions with real persons involved in illicit activities.
Regulators, mount up!

On July 14, 2014, the New York State Department of Financial Services released details on a proposed "BitLicense." Regulations were finalized and effective on August 5, 2015. Generally, most persons and companies in New York that use cryptocurrencies are required to obtain a BitLicense. The few exceptions are for merchants and consumers that utilize cryptocurrency for the purchase or sale of goods and for the development and dissemination of cryptocurrency software. Everyone else needs a BitLicense.

In 2017, there was a significant rise in initial coin offerings (ICOs). ICOs generally involve a startup project where the developers issue new coins in exchange for existing cryptocurrency—usually Bitcoin or Ether. The U.S. Securities and Exchange Commission (SEC) took note. The SEC has issued guidance regarding potential securities violations for ICOs and unregulated cryptocurrency trading platforms. Federal, state, and local regulations are inevitable.

The death of cryptocurrency speculation and hard currencies

A common criticism of Bitcoin is that it's not used for anything other than illicit purchases. Others will cite an early use involving a pizza purchase for thousands of Bitcoins—worth millions of dollars today. While merchants have not widely adopted cryptocurrency payments for a variety of reasons, some notable online merchants do accept cryptocurrency as payment: technology retailer Newegg accepts Bitcoin payments, as does retailer Overstock.com.

As adoption of cryptocurrency gains traction, the U.S. may eventually rid itself of hard currency. In late 2015, the president of the U.S. Money Reserve advocated eliminating the penny because it costs more to produce the coin that it is worth. It also costs more to produce a nickel than it is worth.

While Bitcoin's reputation for illicit activities is unlikely to go away anytime soon, bad actors commonly use hard currencies for illicit activities, too. The illicit use of hard currency provides the government with some incentive to shift from hard currency to a cryptocurrency system. The government could closely monitor, regulate, and control the use of cryptocurrency. All activities would be permanently recorded on the blockchain.
The death of pseudonymity

Governments will be reluctant to maintain the status quo of pseudonymity with any cryptocurrency they adopt. Instead, the government will probably force its citizens to register wallet addresses. This simple step eliminates the need for the government to obtain financial data from financial institutions or track suspects' hard currency spending habits. The cypherpunks that initially dreamt up the idea of cryptocurrencies valued privacy and security. However, government regulated cryptocurrency is unlikely to follow these ideals.

The death of *Quill* and rise of *Wayfair*?

As of the time of this writing, the U.S. Supreme Court is yet to decide *South Dakota v. Wayfair*. Some tax and legal experts expect the Court to overturn the 1992 holding in *Quill*. If *Quill* is overturned by the Court (or Congress ultimately acts to do so), the result would increase the tax collecting and reporting obligations of online sellers. Failing to overturn *Quill*, conversely, could provide incentives for states to welcome cryptocurrencies.

Traditionally, the data stored on the blockchain is limited to the quantity of currency, the sender, and the recipient. Future blockchains might record additional transactional data for online sales. A blockchain could store customer data like a shipping address or tracking information. It could also store invoice data including the amount of any sales tax paid. Rather than focusing on out-of-state sellers, states could use blockchain data to obtain unpaid use taxes.

Smart contracts make things even more interesting. It is entirely possible that future uses of smart contracts would include the direct and automatic payment of sales and use taxes to the taxing authorities. Traditionally, retailers collect and remit these taxes for consumers. Smart contracts make it possible to bypass this function. Sales tax audits also might become outdated. In the future, state and local governments might simply rely on a well-written smart contract for compliance. Rather than a specific audit of sales and use taxes, blockchains would likely encounter instant audits. Earlier this year, accounting firm PricewaterhouseCoopers LLP announced its instant access to blockchain data from Northern Trust. 
Will we travel both?

Blockchain technologies face an interesting dilemma. On the one hand, their origin stems from a general distrust of government and financial institutions. One specific objective noted in the Bitcoin originating whitepaper was the lack of a “trusted central authority.” Tension with this objective occurs as the technology evolves and it faces regulation and control from a variety of stakeholders.

Regulated and controlled blockchains will likely coexist with unregulated *laissez faire* blockchains for some time. If the public is willing to give up the level of privacy required for regulated blockchains to operate, it would be difficult or impossible to exchange regulated cryptocurrencies for unregulated ones. It is unclear if this pressure on unregulated blockchains would be sufficient to eliminate them, or if they could somehow continue to coexist with regulated ones.

1 Note that critics attack proof of work mining because it is vulnerable to a so-called 51% attack. A single miner or a group of miners colluding could mine false transactions if they control more than half of the proof of work mining power. As a result, some blockchains rely on a different mining technique—proof of stake. In a proof of stake system, miners stake cryptocurrency in order to verify transactions. This creates a disincentive to falsify transactions because the miner could lose his staked currency if he attempts to poison the mining process. However, this system, too, is susceptible to 51% attacks.


© 2018 Thomson Reuters/Tax & Accounting. All Rights Reserved.