

Blockchain and the future of banking

By Michael A. Holmes, Esq., *Godwin Bowman PC*

OCTOBER 29, 2018

"That'll be \$40.69."

"OK. Do you take American Express?"

"No ma'am, but we do take bitcoin, Litecoin, Zcash, Ethereum and Ripple."

"Excuse me? What?"

By now, everyone has heard of bitcoin, blockchain's infamous spawn. However, bitcoin and its innumerable cryptocurrency clones are just one application of blockchain technology.

While blockchain is gaining recognition and acceptance in many industries, its future in the banking world is still very uncertain, especially in light of the Securities and Exchange Commission's repeated rejection of cryptocurrency exchange-traded fund proposals.

For example, in August the SEC rejected ProShares' proposal to track bitcoin futures contracts. The Winklevoss twins of Facebook fame also had their "Winklevoss ETF" rejected after the SEC cited concerns of fraud and manipulation in the cryptocurrency world.

Explanations of bitcoin — and associated get rich quick schemes — already litter the internet and won't be addressed here. Rather, this commentary will explain blockchain technology in general and then discuss how that technology is being gradually applied to the banking world.

Finally, we'll explore some of the additional, experimental uses of blockchain, its potential benefits and detriments and how businesses and their counsel can prepare for the new blockchain era.

WHAT IS BLOCKCHAIN?

Blockchain is a computer algorithm that organizes data in a way that is self-validating, decentralized and therefore secure. Traditional data organization on a hard drive puts only one copy of the data together in a linear string of ones and zeros. While this method is simple and convenient, the data is prone to theft if the hard drive is compromised.

In contrast, blockchain uses a peer-to-peer, also known as P2P, network (people connected using a specific sharing software via the internet) to store a copy of the blockchain data with multiple peers on their storage drives.

From a macro perspective, this ensures that the data is decentralized because there is never just one copy to be lost/corrupted/stolen. Having multiple, identical copies of the data across multiple storage drives also allows the blockchain to be self-validating, meaning each copy can verify itself against other copies on the P2P network to ensure the blocks in the chain have not been changed.

If someone tampers with a block in the chain, and that block is checked against the system and found to be changed, the system rejects the offending block and replaces it with a correct copy from another peer in the P2P network.

Each block contains thousands of bits of user data, such as transactions for bitcoin or internet traffic. In addition to the user data in the blocks, the chain contains two bits of important information: the location of that block within the larger chain (known as the "hash") and the hash of the previous block in the chain.

The use of cryptography, which allows security from a micro perspective, enables the data to be both self-validating and secure. The hash for each block is a completely unique string of numbers and letters (for example, f03jr5bh6iyu8fbnm10) with no two identical hashes, producing a cryptocurrency fingerprint.

If any data inside a block changes — for instance, if the data is somehow tampered with — the hash changes to reflect that the block has been changed.

Including the previous hash in each subsequent block ensures that the chain's order and integrity is maintained because each block can self-validate by checking its current hash with the previous block's record of its hash. If a hash changes and doesn't validate with the chain, the block is rejected as invalid.

This ensures that the data in the block stays the same or, at the very least, a user is made aware of any changes to the data. Any data change can be verified by looking to the previous block's hash, because if a block is rejected it is replaced with a correct copy from another peer.

This also keeps the chain order from being modified, as each block in that chain has a record of what block should follow it.

If you've watched or read any news in the past five years, you have heard about the prevalence of data breaches. What is the

potential for blockchain hacking? While nothing is ever 100 percent secure, blockchain is much more secure than any other commercially available system currently on the market.

The argument has been made that you could (theoretically) force all the hashes in a chain to change simultaneously, making the hash-verification system in blockchain fail. To avoid this potential problem, the blockchain algorithm also requires a proof of work. This means a block cannot be instantly created or modified.

Instead, there is a waiting period of about 10 minutes before a new block can be created within a chain. In that time, the block is verified and authenticated extensively (think back to showing your math work in grade school).

So, the blockchain algorithm itself, through the required proof of work mechanism, does not allow you to force-change all the blocks and steal entire chains.

Simply put, blockchain is a superior algorithm for data organization in our current technological landscape because it allows data to be decentralized and much less vulnerable to attack, loss or corruption.

Any attack that tampers with the data in the block or the chain will be discovered and fixed because the system has built-in checks and balances to ensure its validity and integrity. And any loss or corruption can be easily replaced with numerous other copies of the blockchain on other peer storage drives.

HOW BLOCKCHAIN IS BEING USED IN BANKING

Blockchain and the banking world are a match made in heaven — a technology that is decentralized, self-validating and secure sounds like something the banking industry should have created itself!

While no one knows who authored the final blockchain algorithm, and the banking world is a bit late to the party, the industry is doing its best to catch up, just as it did with the rise of the internet.

IBM has predicted that in four years, about 70 percent of the banking industry will be utilizing blockchain for various transactions. An estimated 200 international banks are already utilizing blockchain mobile payments, and a handful of domestic banks may be doing so by the end of the year.

Banks also rely on blockchain to manage customer investment portfolios in a more secure and reliable manner that, in addition to providing the benefits previously discussed, makes in-house or third-party investment portfolio software unnecessary.

Indeed, cost-cutting and operational efficiencies are some of the biggest reasons banks are already implementing blockchain into their business models, as it can reliably replace costly systems including those for verification, security, backup, big data, fraud and even secure customer

communications. Banks will likely create in-house blockchain systems that can handle everything an institution offers within one secure, decentralized system.

Blockchain also provides a much easier way to identify and verify banking clients. When your client has a verifiable hash that has been duplicated across the entire P2P network, identify theft becomes a thing of the past.

Customers can be identified and verified, no matter where they are in the world, so long as they possess their hash in some secure form. Secure cards that contain encrypted keys are already being utilized.

Further, if your identity is compromised somehow (you clicked on that link you shouldn't have, didn't you?) the problem can be easily rectified by having your blockchain identity verified and repaired on the P2P network.

Additionally, many banks are looking at blockchain for what are known as smart contracts. In the simplest terms, this means utilizing blockchain to write a set of criteria, such as the terms of the contract. When the criteria are met, the transaction is completed automatically. If the criteria are not met, the transaction is automatically rejected without further input from the user.

For example, suppose you have found a buyer for your 1,000 widgets. However, the price of the widgets is too high for the buyer to pay cash, and you and the buyer have yet to agree on terms such as delivery and refunds.

Through blockchain, the bank can provide a system for you and the buyer to establish a smart contract. The smart contract will have your acceptable terms and the buyer's acceptable and unacceptable terms, along with potential payment.

If the smart contract determines that the range of terms between you and the buyer matches up, then the contract self-executes (no concern about signatures/dates/authority when blockchain can self-validate), payment self-executes (via a secure blockchain transaction) and the order is sent (via blockchain secure communications).

Because the bank's work is done once it puts the smart contract in place, it should be apparent how much time, money, liability and overhead the banking world can save with this technology.

THE FUTURE OF BLOCKCHAIN, BANKING AND YOU

One of the biggest advantages of applying blockchain to the banking industry is that it eliminates the middleman while increasing the transparency of transactions. Blockchain enables banks to provide secure and transparent transactions to their own customers — and indeed the entire world of customers — all with less direct involvement. Which begs the question: If blockchain eliminates the middleman, will big banks still be needed? The answer is yes, but probably not in the role they play now.

Banks have historically been the bastions of transactions — including day-to-day deposits and withdrawals, storage of money and loans of all sizes. But picture the scenario of a strictly online company, instead of a bank, offering instant, secure and untraceable blockchain transactions between you and anyone else in the world from a smartphone.

That same company could issue you a digital wallet that could hold all your currency in a secure blockchain form on your smartphone, so you no longer need a savings account. And if your smartphone is stolen, your account wouldn't be compromised because your wallet is continually verified with the other copies of your wallet on the P2P network.

For loans, combine the smart contract technology we discussed earlier with secure currency transfers like bitcoin. Now online services can offer loans that are self-executing and self-verifying when the terms are met, issue the loan proceeds securely and directly into your smartphone wallet, securely withdraw your monthly interest payments and terminate the loan if certain conditions aren't met or maintained.

The benefits of future applications of blockchain to the banking world are obvious: massive cost and time savings.

But what about the detriments? Well, as a cynic of human nature might foresee, untraceable purchases using cryptocurrency transactions, without human oversight, could result (as we have already seen) in unscrupulous buying and selling.

How is a bank or online institution supposed to ensure the ethics and integrity of the purchases and sales ultimately made by the transactions it facilitates? One of cryptocurrency's inherent strengths and weaknesses is that it arguably cannot. Blockchain will magnify the massive struggle between privacy and security and transparency.

Further, as many lenders and mortgage professionals will tell you, a significant part of their due diligence comes from meeting with the potential borrowers face to face. Will creditworthiness decrease, and the potential for default increase, when people can take out loans or mortgages via an automatic blockchain transaction system on their smartphone without ever stepping inside a bank and experiencing the fear of God that comes from a mountain of paperwork?

And from the customer's perspective, how will they know if a particular online institution is reputable and will honor the terms of the loan?

From knowing that person can likely be found again to seeing how they present themselves, there is something to be said for face-to-face meetings between a customer and banker. Then again, maybe blockchain loan and mortgage transactions will help erase some of the inherent, systemic or

unconscious biases and prejudices otherwise resident in the current financial system, thus providing more equal access to investment money.

What can businesses and their counsel do to prepare for the impending shift to blockchain? First, think through the processes and procedures for your business, or your client's business, and ask where blockchain might provide some operational efficiencies or the potential for increased security and transparency.

Write out the pros and cons of investing in blockchain now versus waiting until the early-adopter stage has passed. Evaluate your customer base to see if blockchain would be a benefit or detriment to your clients' use of your product or service. If you find potential efficiencies that would make you more attractive to your client base, speak with blockchain experts about the practicalities of implementing it into your business model.

Most importantly, meet with an attorney who understands blockchain and your business, and can provide insight into any potential risks, liabilities or other relevant business issues.

Above all, a decision to harness blockchain's power should involve input from all aspects of the company, both for its current implementation, as well as long-term viability and scalability. But if a business can wade into the blockchain world now, it will establish itself as a forerunner for the next big technological shift.

This article first appeared in the October 29, 2018, edition of Westlaw Journal Bank & Lender Liability.

ABOUT THE AUTHOR



Michael A. Holmes is a senior business and technology attorney at **Godwin Bowman PC** in Dallas, where he represents scrappy startups and mature Fortune 500 players across the United States in corporate transactions and complex dispute resolution matters. His practice focuses on emerging and disrupting technology, enabling him to position his clients' businesses to minimize risk and maximize potential success. He can be reached at MHolmes@GodwinBowman.com.

He can be reached at MHolmes@GodwinBowman.com.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.