BLOCKCHAIN *for Lawyers*

By J. Mason Bump

At the outset, blockchain technology may seem confusing or downright unnerving to lawyers, even those who are masters at learning and applying new information to their practices, but I'm here to explain that this technology won't fundamentally change many of the concepts we're used to in the legal profession. This technology will only apply them in more effective ways and will also result in more efficient outcomes for all participants.

When we refer to "blockchain," "crypto," or any other application of this technology, what we are actually referring to is a basket of technology combined in a secure system with verifiable, reliable outcomes for all participants. These systems have been deemed "trustless" because they can operate without a middleman that verifies the negotiating position or credit of each party, and because they provide instant verification of network integrity. The way this is accomplished is a basket of tech concepts that includes a digital "public ledger" allowing the public to verify the integrity of the system as a whole and "triple-entry accounting" that requires all participants to rectify their own ledgers with the public ledger. If that all sounds like a mouthful, you're not alone, but I will do my best in the following paragraphs to explain it in plain English.

THE BASKET OF TECH

The first piece that makes this work is the "public ledger" that shows the "state" of the network at any given time, including what the network looked like in the past through records of transactions called "blocks." In the blockchain world, think of the network "state" as the status of all accounts (or "wallets") and the network itself, and think of "blocks" as new pages in a public checkbook of transactions between participants that can be accessed and viewed at any time. Each new block is basically a memorial of the state of the network at a certain point in time, and is "append-only," which means that new data can only be added in sequential order.

By making this information public, the integrity of participation, transactions and the network itself is assured because anyone can verify the information of any transaction between accounts at will. However, in the case of networks like Bitcoin, this information merely shows the movement of digital assets between digital addresses, so in most cases those digital "wallets" can be created without any identifying information, with users effectively acting under pseudonyms.[1]

The data of participants can only be updated by consensus of the participants, which will be explained in the example below. The decentralized method by which participants interact, combined with the extreme difficulty in adding new information to the network and the "cryptographically secure" manner that makes it resistant to tampering, results in a reliable network system that does not require trust between any of the participants to function as intended.

PAPER BLOCKCHAIN EXAMPLE

Interestingly, a blockchain system can be built with pen and paper as long as all participants are known and have equal voting power. Let's say that you and your friends are stuck on a desert island, and you need to figure out a way to exchange value for resources without going to the highly inefficient barter system (in fact, "money" was the original "app" created to solve the inefficiencies of this system). You and your friends each get 100 "I-Coins" for agreeing to be part of the island's monetary system. Each day, the ledger gets updated with I-Coin transactions, and the participants agree to their new account balances by signing at the bottom to reach consensus. Let me be clear, I-Coins are not the same as "membership units," because each person has the same power to vote on a new batch of transactions regardless of how many I-Coins they have.

For example, let's say John wants to send you 10 I-Coins in exchange for a bag of tomatoes. Before agreeing, you can check the ledger and verify that John has 10 I-Coins and that John isn't trying to send both you and Tom the same 10 I-Coins for two different transactions. This is what's known as the "double-spend problem," and is what Bitcoin solved with its distributed public ledger system.

You may be wondering now, what's stopping John from fudging the numbers in the checkbook to make it seem like he has more money in his account? When dealing in the I-Coin example, it is relatively easy to verify John's account because all participants are known to each other and transactions are verified by them equally at regular intervals.

In the context of a digital network of participants who don't know each other, this concept gets a bit more complicated. Think of the digital checkbook example as having automatically-updated, cross-referenced page numbers, and each page has a unique identifier that has been verified by the account holders, and that these records are nearly impossible to change once entered. These pages of the checkbook are the blocks of transactions and are secured by cross-referencing the identification data from previous blocks, all of which have been verified by "signatures" and adopted in the participants' own ledgers. In this way, if one wanted to change data in any given block, they would not only have to alter the information and security data in that block, but also in all subsequent blocks that refer to it.

This is essentially the concept of "triple-entry accounting," which solves what is known as the "trust problem" in double-entry accounting, in which one party needed a third-party to guarantee or ensure the representations of the other party in case they were lying. Under a decentralized blockchain system, parties are required to coordinate their own ledgers with the public ledger in order to participate and engage with other parties on the network. Since the public ledger is constantly updated and verified by a decentralized network of independent third parties, if any part of the network is hacked or fails for any reason, the rest of the network will continue to operate in a decentralized manner, as intended.

THE BYZANTINE GENERALS PROBLEM

This technology solves what NASA called "The Byzantine Generals Problem," which asks how decentralized groups can come to a consensus about the best way to carry out a plan, given the presence of bad actors or communication failures. The analogy is essentially as follows:

> *Several divisions of the Byzantine army are stationed just outside of an enemy city and are preparing for battle. Various generals can only communicate with each other via a messenger. They must agree upon a common course of action. However, we must assume that some generals are traitors who wish to prevent loyal generals from agreeing upon a common course of action. An algorithm is needed to ensure that a small group of traitors can't disrupt communications. To solve the Byzantine Generals problem, loyal generals need a secure way to come to agreement on a plan (known as consensus) and carry out their chosen plan (known as coordination).*[2]

Although there are quite a few proposed solutions to this problem, the Bitcoin whitepaper published by Satoshi Nakamoto is the most successful. This concept resulted in the first successful decentralized blockchain network, with a limited supply cap of 21 million coins incorporated directly into its source code.[3] The Bitcoin network achieves what is known as "Effective Byzantine Fault Tolerance" by enabling asynchronous communication between nodes to replicate the state of the network, assymetric encryption, peer-to-peer networking and Proof of

Work (PoW) block validation. Each one of these technologies is incredibly detailed in its own right, and since this article is about legal implications resulting from the application of these networks, they will not be discussed here, but these concepts all contribute to what makes Bitcoin and many other blockchain systems so secure, reliable and successful.

SMART CONTRACTS

While Bitcoin uses these combined technologies to let participants send and receive digital currency, networks like Ethereum use these technologies to let participants write and execute coded agreements known as smart contracts, or even "mint" specialized tokens that allow participants to interact in unique ways. In some cases, new tokens have been minted as a way to increase transactional efficiency for commodities via specialized smart contracts, such as coffee trading in Brazil.[4] Although the nuts and bolts can be complicated, generally this can be seen as an upgrade to existing processes in the same way email was an upgrade to physical memoranda. Blockchain-backed smart contracts enable parties to rely on the fulfillment of terms in a way that is more efficient, accurate, transparent and virtually instantaneous, and allow participants to interact from anywhere in the world without the usual inefficient international barriers.

As a result, smart contracts are powering many new developments in the business world, including Decentralized Finance (DeFi), Decentralized Insurance and Decentralized Autonomous Organizations (DAOs), which utilize digital governance structures that allow participants to vote and act on enterprise initiatives using digital tokens. These DAOs represent a common organization, enterprise or interest and as a result they fundamentally operate based on contract principles. The key difference is that the contracts are now written in a more secure and open way, which allows for more efficient recordkeeping and transparent participation by all parties.

Interestingly, the concept of escrow is incorporated into nearly every smart contract, with the contract being initially funded with a cryptocurrency (usually Ethereum) by one party, and then released to the other party upon fulfillment of the contract terms. If that party doesn't deliver on the terms of the contract, the money is either released at a discount or released back to the funding party. Fulfillment of contract terms can be verified in many ways, but the most promising and institutionally-adopted method is through oracle services like Chainlink.[5]

Although regulatory guidance is still scant within our borders, the UK Jurisdiction Taskforce has recently published arbitration rules for resolution of disputes concerning digital assets and smart contracts.[6] A notable example of regulatory clarity within the United States is Wyoming's approach, which clarified the status of smart contracts in commercial law, allows the issue of bank charters for banks that deal mostly in digital assets and even granted legal status to DAOs that recognizes them in a similar way as LLCs.[7]

NON-FUNGIBLE TOKENS (NFTS)

A variant of these tokens that is gaining traction and notoriety are Non-Fungible Tokens (NFTs). These tokens are based on technology similar to cryptocurrency, but represent individual, non-replicable items rather than fungible assets like cash, which are all basically identical in nature. It is best used to digitize an identifying characteristic of a unique item, and recent use cases include artwork, intellectual property and real estate. For a real-world metaphor, think of an NFT as a VIN tag for anything unique that can be owned, and think of a blockchain network as the place where that VIN is registered. The application potential of this technology is massive and may change everything from vehicle titles to supply chains through a transparent, verified chain of ownership memorialized on blockchain networks.

CONCLUSION

As lawyers, we already take on a lot of commitment to learning specialized vocabulary in our own field, and now that our clients are using terms like "blockchain," "crypto" and "NFT" in conversation and business planning, it can seem daunting to take on even more, especially in the field of cutting-edge technology. My hope is that you can now rest comfortably knowing that this technology won't substantially alter many of the legal principles we're already used to – it simply applies them in more efficient ways.

[1] Alison Frankel, *SEC's failed bid for Ripple exec's bank records shows government's crypto suspicions*, April 12, 2021, REUTERS, https://www.reuters.com/article/legal-us-otc-ripple/secs-failed-bid-for-ripple-execs-bank-records-shows-governments-crypto-suspicions-idUSKBN2BZ2ID.

[2] Delton Rhodes, *The Byzantine Generals Problem, Explained*, KOMODO, https://blog.komodoplatform.com/en/byzantine-generals-problem/.

[3] Paul Browder, *Why the supply of Bitcoin is limited to 21 million*, April 22, 2021, CRYPTOINVOKE, https://www.cryptoinvoke.com/2021/04/22/why-the-supply-of-bitcoin-is-limited-to-21-million/.

[4] Christina Comben, *Why Brazilian farmers are using crypto coffee coins*, July 17, 2019, YAHOO FINANCE, https://finance.yahoo.com/news/why-brazilian-farmers-using-crypto-080049435.html.

[5] *Connect your smart contract to the outside world*, CHAINLINK, https://chain.link/.

[6] JD Alois, *UK Jurisdiction Taskforce of LawtechUK publishes rules for dispute resolution for crypto, blockchain*. April 26, 2021, CROWDFUND INSIDER, https://www.crowdfundinsider.com/2021/04/174623-uk-jurisdiction-taskforce-of-lawtechuk-publishes-rules-for-dispute-resolution-for-crypto-blockchain/.

[7] Chris Matthews, *How Wyoming became the promised land for bitcoin investors*, April 23, 2021, MARKETWATCH, https://www.marketwatch.com/story/how-wyoming-became-the-promised-land-for-bitcoin-investors-11619201182.

J. Mason Bump is an associate at Sullivan & Ward, P.C., where he mainly practices in the areas of business structuring, contractual agreements and litigation. He has been a dedicated blockchain research writer since law school, and continues to pursue emerging applications of this technology that maximize value for users.