



The Blockchain Moment

BY ERIC KINTNER

Blockchain, the distributed ledger technology at the heart of cryptocurrencies like Bitcoin, is one of the most talked about new forms of technology today. Proponents claim that blockchain technology is one of the most innovative technologies of the 21st century and has the potential to bring the biggest change to modern life since the introduction of the Internet. This article describes blockchain technology and how government regulators have started to address the challenges presented by blockchain-related activities and cryptocurrencies. It also discusses

potential implications for lawyers and the legal profession at the dawn of this blockchain era.

What is Blockchain?

Blockchain is a type of database technology in which data is stored on a network of distributed ledgers in a chain of blocks or “blockchain” that is protected with cryptography. The first use case for blockchain technology was Bitcoin, the peer-to-peer digital cryptocurrency. Bitcoin allows an individual to transfer digital currency to another person without an intermediary, such as a bank, having to process the transaction.

Today, there are over 1,600 cryptocurrencies with a total market cap of approximately \$350 billion.¹

Traditional, centralized ledgers are used by banks, Internet companies, and other intermediaries to track transactions over time. The problem with centralized ledgers is they require trust that the holder of the centralized ledger will not be hacked or lose the data, or, even worse, steal the data or extort network participants for access to or maintenance of their data. Blockchain ledgers, in contrast, are distributed across the network so that each network participant—or “node”—maintains an identical copy of the ledger. As a result, no single node can control data in the network.

To add a new transaction to the blockchain ledger, the transaction is broadcast to the network and then linked with other transactions into a single block. Each block of data includes a small piece of data that connects it to the previous block. This block is then encrypted so that the entire set of data in the block is represented by a fixed set of random numbers and letters called a hash. If a malicious actor were to try to modify just one bit of data in a given block, the hash for the entire block would change, which would then be spotted and rejected by the other network participants. This feature helps ensure that the data stored in the blockchain is immutable and secure.

To determine which block to add next to the ledger, blockchain networks feature different mechanisms for reaching consensus. It is the consensus mechanism that enables the gate-keeping function to be entrusted to a network of participants rather than a centralized authority. In “permissionless” or “public” blockchain networks, like Bitcoin, consensus is reached through the competition of nodes running energy-intensive computations, with the “winning” node being rewarded with newly created or “mined” Bitcoins. Incentivizing network participation by mining new Bitcoin ensures a more robust network and a more censorship-resistant blockchain database. In “permissioned” or “private” blockchain networks, like Hyperledger, consensus is reached by a set of trusted nodes that vote on the order by which new blocks are added.

Because private blockchains do not require the same energy-intensive computations to reach consensus, private blockchains often have better transaction latency and speed and, as a result, better scalability for enterprise-level solutions.

Smart Contracts

A “smart contract” is software code that is capable of facilitating, executing, and enforcing the performance of an agreement automatically upon the satisfaction of conditions set out in the code. Smart contracts have the potential to drive massive operational efficiencies by automating processes that are currently handled manually by intermediaries.

Smart contracts are currently used to help provide transparency to the supply chain, to reduce the timeframe for healthcare claims reimbursement, and to simplify real estate title transfers. For example, consider a vehicle lease connected to a smart contract in a blockchain-based financing program. If the lessee were to default on her lease payment, the smart contract could transmit wirelessly to the vehicle’s onboard software to disable the ignition, lock the doors, and transmit the GPS location of the vehicle for repossession.

Smart contracts are, however, not without their challenges. Too much rigid automation could lead to draconian and even fatal outcomes. Consider the single mother whose leased vehicle’s doors lock after missing her

As cryptocurrencies have grown in popularity and market cap, federal and state agencies have begun to take interest in, and in some cases regulate, their use and operation.

lease payment while her children are still inside the vehicle. Smart contracts can also have “bugs in the code” that can be exploited. In July 2017, an unknown attacker exploited a critical flaw in “The DAO” smart contract code used for multi-signature wallets on the Ethereum network, draining over \$50 million worth of Ether cryptocurrency in a matter of minutes.² Smart contracts also need to rely on real world “oracles” to connect the smart contract code to real world events. What happens if the oracle dies or goes out of business?

Government Regulation Is Evolving

Government regulation regarding blockchain-related activities remains undeveloped and likely to rapidly evolve. Blockchain-based tokens are powering new forms of crowdfunding, often referred to as initial coin offerings, which have raised over \$6 billion in funds in 2018 alone.³ As cryptocurrencies have grown in popularity and market cap, federal and state agencies have begun to take interest in, and in some cases regulate, their use and operation. For example, the U.S. Department of the Treasury, the Securities Exchange Commission, and the Commodity Futures Trading Commission have all published guidance on the treatment of cryptocurrencies.⁴ The IRS released guidance treating cryptocurrency as property and not currency for U.S. federal income tax purposes.

Some state regulators, like the New York Department of Financial Services, have created a new regulatory framework for issuing, storing, trading, or selling cryptocurrency. In Colorado, several blockchain-related bills were introduced during the 2018 legislation session. On May 16, Governor Hickenlooper signed into law Colorado Senate Bill 86, which requires the Governor’s Office of Information Technology, the Department of State, and the Department of Regulatory Agencies to consider using blockchain technology to protect confidential state records from criminal, unauthorized, or inadvertent manipulation or theft. Colorado



DECIPHER FORENSICS IS NOW EIDE BAILLY

Decipher Forensics, a leading digital forensics and eDiscovery firm specializing in mobile device forensics, is now part of Eide Bailly. We are excited to add their talent and commitment to client service to our already strong computer forensic investigative skills and cost-effective data processing protocol. Work with professionals who can truly revolutionize your eDiscovery Management process.



303.586.8504 | eidebailly.com/digitalforensics

House Bill 1426, which sought to exempt certain “open blockchain tokens” from the Colorado securities laws, easily passed the Colorado House but narrowly failed to pass the Colorado Senate on the last day of the session.

Blockchain’s Impact on the Legal Industry

Blockchain technology also has the potential to transform the legal world and the practice of law. Lawyers (and the billable hour) could be viewed as another intermediary ripe for disintermediation by blockchain technology. Projects like OpenLaw seek to automate contract drafting with embedded smart contracts, which may reduce demand for routine or commodity legal services.

On the other hand, blockchain also represents a potential source of new growth in legal services. New legal sub-specialties are

being developed around initial coin offerings and cryptoeconomics, and the regulation of exchanges for trading cryptocurrency and their derivatives. Lawyers are now assisting governments to craft new regulations for this nascent technology and roll out their own statewide blockchain initiatives.

Dawn of the Blockchain Era

The dawn of the blockchain era represents a unique opportunity for private industry, the public sector, and the legal profession. Blockchains are now underpinning new services that could have a huge impact on a range of industries, including financial services, healthcare, and real estate. Blockchain-based token sales are posed to transform capital markets and monetize new forms of digital assets without the need for traditional market participants. Smart contracts are increasingly being

explored to control and connect the operations of Internet-connected devices. Governments, such as in Colorado, are actively exploring the potential to leverage the tamper-resistant quality of blockchain technology to ensure the integrity of government information as well as provide traditional government services, including transfers of property rights, e-citizen digital identities, and voting.

One cautionary note: Blockchain innovation could be hindered if blockchain technology supporters, including those in the legal profession, ignore the need to engage government officials in the regulation of blockchain technology. It will be critical for future blockchain innovation that regulatory regimes balance the need to protect cryptocurrency purchasers with the countervailing need to allow for the full exploration of potentially useful applications of blockchain technology. Given the early stage of blockchain development, it still seems possible to capture the benefits of blockchain technology, while limiting its downsides. 



**law office
accounting
specialist**

- & COLTAF accounting & reconstruction
- & Full-service billing, bookkeeping & payroll for law firms
- & Training & consulting for QuickBooks® Timeslips® TABSIII®
- & Forensic accounting
- & Fraud investigations (occupational fraud expert)

daphne a salone cfe, cfc
certified fraud examiner & certified forensic consultant

970.527.3075
dsalone@lawandequityltd.com

**law & equity
ltd**
*servicing lawyers and
small businesses since 1993*



Eric Kintner is a partner at Snell & Wilmer. He focuses his practice on blockchain and digital currency—(303) 634-2071, ekintner@swlaw.com.

Coordinating Editor: Joel Jacobson, joel@rubiconlaw.com

NOTES

1. See CoinMarketCap, <https://coinmarketcap.com/all/views/all>.
2. Finley, “A \$50 Million Hack Just Showed That the DAO was all too Human,” *Wired* (June 18, 2016), www.wired.com/2016/06/50-million-hack-just-showed-dao-human.
3. Floyd, “\$6.3 Billion: 2018 ICO Funding has Passed 2017’s Total,” *CoinDesk*, www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017.
4. For more information on this guidance, see Popielarski, “Blockchain Research Bitcoins, Cryptocurrency, and Distributed Ledgers,” 47 *Colorado Lawyer* 10, 11-12 (June 2018), www.cobar.org/-em-Colorado-Lawyer-em/Full-Issue/IssueID/30.