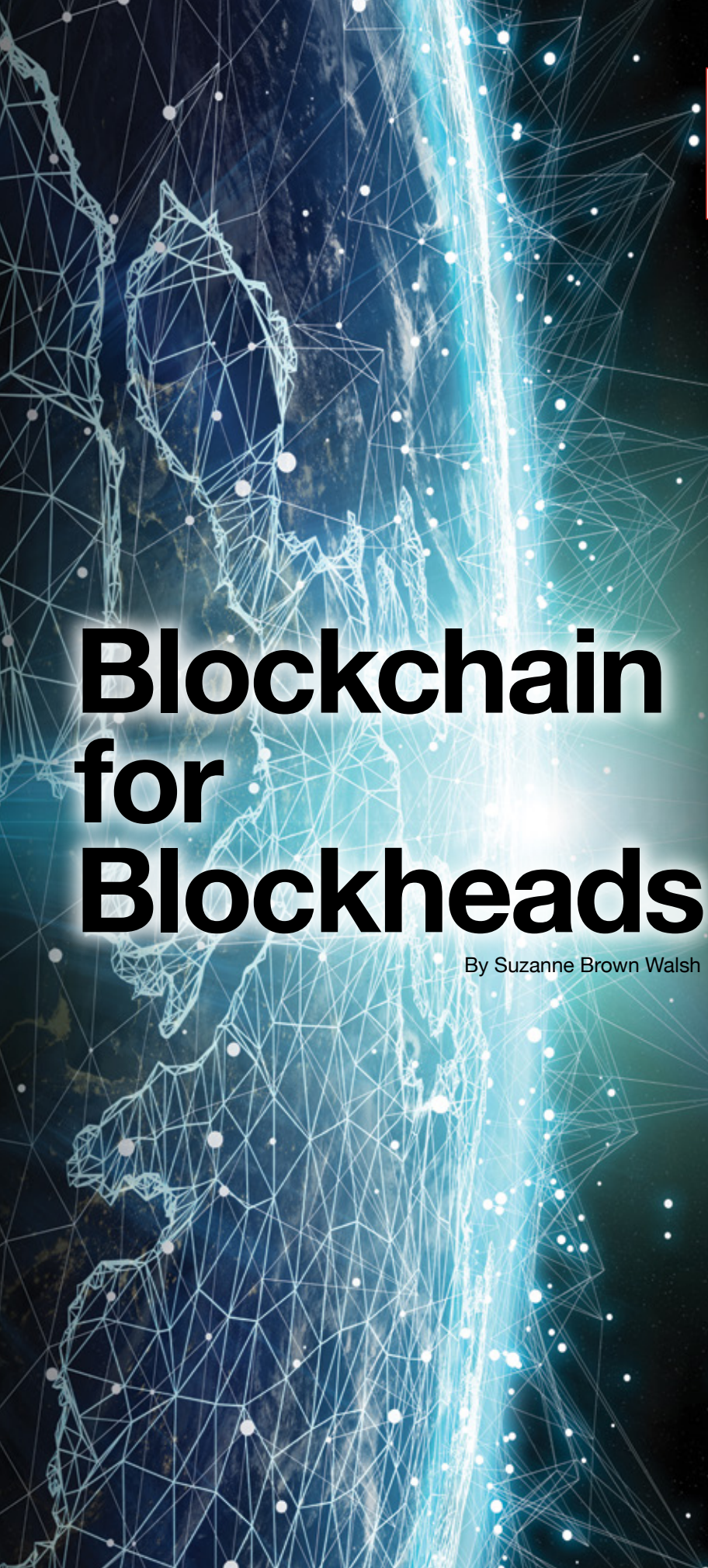


Blockchain for Blockheads

By Suzanne Brown Walsh

To learn how blockchains work and are structured, it is helpful to start with the first blockchain, Bitcoin. The Bitcoin blockchain is the protocol, or software, underlying the cryptocurrency Bitcoin. Other distributed ledger or blockchain technologies have been created that differ from Bitcoin, and are designed to perform different functions than Bitcoin. Bitcoin is simply the first use case or application that runs on blockchain. Blockchain is now, a mere nine years after its creation, just one of many different operating systems ("protocols")—another is Ethereum. Think of a blockchain as a computer operating system, and of Bitcoin as the "use case" or "application" it enables. Just as there are many programs or applications you can run on your computer, likewise, there are numerous applications that can run on blockchain.

To understand how this works, let's get back to Bitcoin, which was first described in a whitepaper[1] published during the depth of the worldwide financial crisis in 2008. One problem that the Bitcoin protocol solved, is how to create a viable digital currency that does not rely on a central bank, government, or other trusted authority. This accounts for Bitcoin's popularity in countries with collapsing economies or weak financial systems. The other problem that the Bitcoin protocol solves is "double spending." Traditional money, or fiat currency, relies on a central authority that ensures it is not counterfeit, and when transferred electronically, has not been double spent.

How does the Bitcoin protocol provide users with trust and confidence, and ensure that bitcoins are not double spent? It created a method for recording transactions within a ledger that is *secured* by cryptography, *time stamped*, and *validated* by consensus from the network participants. These features together prevent fraud, allowing users to trust the ledger.

Why call the Bitcoin ledger a blockchain? On the ledger, pending transactions are verified, grouped into "blocks," and time stamped. Once verified by this consensus, the transactions within the block, or ledger, cannot be changed, and become immutable. Thus, to reverse a transaction reflected in the ledger, one has to enter into an entirely new transaction. It also means that a user who loses the data (a "private key") needed to establish the user's right to access his or her data, cannot enter into new transactions that affect that data on the ledger, and loses access to it. Because there is no central authority, there is no equivalent of a locksmith to break a lock, a banker to drill a safe deposit box, or a state treasurer holding unclaimed property until it is claimed by its owner. (In cryptocurrency, commercial wallet services may perform this function, in a tradeoff that reduces security, but eliminates or minimizes the risk of a lost private key.)

In Bitcoin, there is no running tally in the ledger of the assets owned by one participant. Instead, the ledger traces the underlying assets and their forward or subsequent movements in the system. Assets are tracked not by an owner, but by the asset transaction records, and are "moved" via the authorization of a cryptographic signature (a "private key").[2]

Bitcoin is simply one type of "distributed ledger." Unlike centralized networks with centralized servers, distributed ledgers allow multiple computers to run the same software, without a central, or even hierarchical, authority or computer. Because there is no sovereign or governing computer, in order to successfully disrupt or "hack" a distributed ledger, one has to take down more than half of the computers in the system. Therefore, the data on a distributed ledger is much more secure than data stored in a centralized network.

The level of privacy and access to distributed ledger systems may vary. Although Bitcoin is open to anyone who wishes to download the software and run it, other blockchains may be closed, or available only to participants who have permission or a credential that allows them to access the network. Think of Bitcoin as the Internet (open and accessible to all) and a private or permissioned blockchain as a law firm intranet (open and accessible only to firm employees with access credentials).

The type of data stored on a blockchain can also differ from system to system. In Bitcoin, the stored data is the ongoing chain or list of Bitcoin transactions. Think instead about using an immutable, secure blockchain to store identity documents and data, such as birth and death certificates, social security cards, health records, credit histories, the history of food in a supply chain, the provenance of wine, diamonds or art, real estate deeds, or any document or information that must be protected against theft and forgery, or for which an audit trail is desirable.

Cryptocurrency and blockchain technology are likely to transform many businesses, and thus many legal practice areas, such as:

Estate Planning
Cryptocurrencies are stored, secured, and transferred outside of traditional wills and trusts, and in a completely different manner than other nonprobate assets.

Municipal and Government
Governments are exploring issuing identity documents and storing public records on blockchains.[3]

Securities
Initial coin offerings (ICO's) were used to raise $4.6B in business capital in 2017, bypassing traditional venture capital.[4]

Utilities
Blockchains are being piloted in Brooklyn, NY to a allow residents with solar panels to sell excess energy back to their neighbors, in a peer-to-peer transaction.[5]

Tax
The IRS issued guidance on the taxation of cryptocurrencies in 2014 that leaves much unanswered.[6]

Real Estate
South Burlington, VT is piloting a blockchain for its land records and deeds.[7]

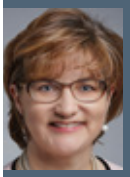
Health Care
Companies are already implementing blockchain technology for health records.[8]

Finance
Businesses and individuals may be able to settle and reconcile local and global transactions almost instantly, at a lower cost.[9]

Supply Chain and Shipping
Several shipping industry consortia have successfully tested blockchain technology to track cargo.[10]

Insurance
Insurers are already testing blockchain as a means of establishing proof of insurance[11]

These are simply a few examples of how many businesses and industries are exploring and testing this transformative technology. Blockchain is often compared to the Internet—more specifically, to the dial-up phase of Internet access (remember back to 1997). **CL**



Suzanne Brown Walsh is a Partner in Murtha Cullina LLP's Trusts and Estates Department, where she represents clients in the areas of estate and tax planning, particularly for families of children with special needs, elder law, estate and trust administration, trust modifications and trustee changes. Since 2005, Attorney Walsh has served as one of Connecticut's Commissioners on Uniform Laws.

Notes

1. https://bitcoin.org/bitcoin.pdf
2. There are many resources that describe the protocol in detail compiled at https://lopp.net/bitcoin.html.
3. https://www.coindesk.com/illinois-launches-blockchain-pilot-digitize-birth-certificates/
4. https://www.itweb.co.za/content/kLgB1MeJk2xq59N4
5. https://tinyurl.com/y74vu6tc.
6. https://www.irs.gov/pub/irs-drop/n-14-21.pdf
7. https://www.coindesk.com/vermont-city-pilots-land-registry-record-with-blockchain-startup/
8. https://medicalchain.com/en/
9. https://www.coindesk.com/swift-announces-successful-proof-of-concept-trial-for-dlt-platform/
10. https://tinyurl.com/ya3jr6ac; https://tinyurl.com/ycdksf2d
11. https://www.insurancejournal.com/news/national/2017/12/27/475346.htm