How to Understand Blockchain

Technology, Privacy, and eCommerce


BC
CAN
CHANGE
THE
WORLD


BC
CAN
CHANGE
THE
WORLD

CHEAT SHEET

- ***Blockchain.*** Blockchain is a mixture of cryptography, computer science, and economics. It is effectively a chronological series of groupings of transactions.
- ***Trustless network.*** With blockchain, the trust function traditionally performed by an intermediary is coded into the software.
- ***Smart contracts.*** Smart contracts are a software code that enables automated performance of contract terms.
- ***Protocols.*** Identify the applicable business requirements and legal obligations and compare them to the characteristics of the blockchain protocols to find the ones that meet your needs.

Cryptocurrencies grab headlines, but their underlying blockchain technology may change the world as much as the internet has, impacting our clients' businesses and our lives in ways we cannot fully predict. Many believe that distributed networks enabled by blockchains will have historic significance and replace much of the current internet with permissionless, decentralized services that securely provide trust and transparency. Herein (Figure 1) are a few examples of projects either in development or in production that, if successful, will fundamentally disrupt major industries.

FIGURE 1

Decentralized blockchain applications with disruptive potential

PROJECT	SUBJECT	POTENTIAL TARGETS	LINK
OpenBazaar	Decentralized marketplace	Amazon Alibaba eBay	www.openbazaar.org
Synereo	Content publishing and distribution	YouTube Social media	www.synereo.com
Viuly	Video sharing	YouTube	viuly.com
BitClave	Search and advertising	Google	bitclave.com/en/
Presearch	Search	Google	presearch.io
Steemit	Social media	Reddit Social media	steemit.com
Obsidian Secure Messenger	Secure messaging	WhatsApp	osm.obsidianplatform.com
Nexus	Finance	Kickstarter GoFundMe Indiegogo	nexusearth.com
Indorse	Networking	LinkedIn	indorse.io
Sapien	Social media	Facebook Social media	sapien.network

Sola	Social media	Facebook Social media	sola.ai
Shop	Retail platform	Amazon Alibaba eBay	shoppers.shop
Ecoinmerce	Decentralized marketplace	Amazon Alibaba eBay	ecoinmerce.io
SELFLLERY	Image sharing	Instagram	selfllery.com
BlockCypher	Cloud services platform	Amazon Web Services	blockcypher.com

The extent to which a blockchain is decentralized and/or permissioned has important business, legal, and practical consequences.

Enterprise organizations have been experimenting with blockchains as a way to streamline business processes and conserve resources. Figure 2 outlines a few enterprise use cases currently in development or use. Unlike the applications listed in Figure 1, very few enterprise blockchains are operated on permissionless systems. Enterprise applications generally involve the organization of participants operating across a value chain, where all participants are known and subject to an agreed upon governance framework. In some cases, enterprise applications do not require wide decentralization. Rather, the actors necessary for these solutions are determined by the value chain at issue. While not receiving as much media attention as their public and permissionless counterparts, enterprise applications likewise stand to disrupt entire industries.

FIGURE 2

Enterprise use-cases with press coverage

COMPANY	PROJECT	LINK
Walmart	? Supply chain for food ? Reduce waste and manage contamination cases	Walmart Is Getting Suppliers to Put Food on the Blockchain
JD.com	? Supply chain for food ? Manage beef imports	The Amazon of China is putting its high-end beef imports on the blockchain
JP Morgan Chase	? Inter-bank payment system	J.P. Morgan Files Patent for Blockchain-Powered Payments
Change Healthcare	? Healthcare network platform ? Claims processing	Change Healthcare's enterprise blockchain tech now available for hospitals, practices, payers
Mastercard	? Payment processing ? Blockchain payments in fiat	Mastercard Will Now Let You Pay With Blockchain—But Not Bitcoin

	currency	
Maersk	? Shipping insurance ? Auditing shipping supply chain and facilitate insurance terms	Maersk and Microsoft Tested a Blockchain for Shipping Insurance
Everledger	? Supply chain ? Provenance of luxury goods	The Diamond Industry Is Obsessed With the Blockchain
Visa	? B2B payments ? Inter-bank payments	Visa Launches First Phase of Blockchain B2B Payments
Australian Securities Exchange	? Manage settlement of equity transactions	The Australian Securities Exchange Just Made Blockchain History
Vanguard Group	? Data sharing ? Market index data for market participants	Vanguard will use blockchain to share index data
Amazon Web Services	? Blockchain-as-a-service	Amazon's new blockchain service competes with similar products from Oracle and IBM
Western Union	? Money transfer	Western Union Taps Ripple for Blockchain Trial
Sony	? Education records ? Store, manage, and share educational records	Sony wants to digitize education records using the blockchain
Lufthansa	? Digital marketplace for travel	Lufthansa Partners With a Blockchain Provider in an Investment Worth Testing
Hitachi	? Supply chain management	Hitachi and Mizuho Strike Deal for Blockchain Supply Chain

The extent to which a blockchain is decentralized and/or permissioned has important business, legal, and practical consequences. In this article, we explore the role of network access and decentralization in blockchain applications and describe blockchain applications across the continuum of network access and decentralization to provide the reader with a framework for the practical evaluation of a blockchain application.

Blockchain and blockchain applications

A blockchain results from the operation of software that complies with a particular protocol. It consists of a chronological series of "blocks," each linking to its predecessor through cryptography. A "block" is a grouping of transactions, marked with a timestamp, and the fingerprint or hash of the previous block. The block header is hashed using the network consensus method of the protocol that governs the blockchain, thereby validating the transactions. Valid blocks are added to the main blockchain by network consensus. Consensus rules are the block validation rules that full nodes follow to stay in consensus with other nodes. Consensus occurs when several nodes, usually most nodes on the network, all have the same blocks in their locally validated best blockchain. Nodes are incentivized to perform their function through rewards (or penalties) created by the protocol.

That is interesting, but what are the practical benefits of this mixture of cryptography, computer science, and economics? Though there are many potential benefits, most boil down to trust or, perhaps better stated, the creation of a “trustless” network. With blockchain, the trust function traditionally performed by a centralized intermediary, platform owner, or central government is coded into the software that implements the blockchain protocol. For example, the original blockchain — Bitcoin — eliminates the need for an intermediary (i.e., a bank) to validate Bitcoin currency transactions between counterparties.

After the publication of Satoshi Nakamoto’s pseudonymous, seminal white paper that launched the Bitcoin blockchain, individuals began imagining blockchain applications beyond digital currency. If currency can be moved between counterparties without the need for an intermediary, then what about data, records, digital goods, physical goods, and intellectual property? As innovative as the Bitcoin blockchain was and is, its utility is limited. It does Bitcoin well, but not much else. Out of this unmet need, the Ethereum protocol was launched.

Ethereum developed a scripting language that makes it easier to develop applications that use the Ethereum blockchain, thereby expanding its utility beyond its native digital currency. This innovation enables developers to build solutions to an infinite number of business problems.

Ethereum also enables the creation of so-called “smart contracts.” Smart contracts are software code that enables automated performance of contract terms, contingent on a consensus by nodes in the blockchain that the conditions for performance of the contract terms have been met. Very often, smart contracts use “oracles” to provide off-chain information (such as proof of payment or performance, or data from devices in the Internet of Things) necessary to the execution of a smart contract. Automated execution makes smart contracts self-enforcing and tamper-proof. This enables the creation of applications to manage all manner of contingent transactions — from relatively simple escrow and claims clearing, to complex multiparty supply chain and trade finance transactions. Figure 3 illustrates the “technology stack” underlying the applications that end users see. Not all blockchain protocols are designed to enable smart contracts but, as you can see from Figure 3, a different blockchain protocol can potentially be the base for any given application.

Figure 3

Basic blockchain architecture

Smartphones, tablets, desktops

USER EXPERIENCE (UX)
Start contracts (rulesets)
Distributed applications (dApps - Bitcoin)

APPLICATION LAYER
Transaction record (distributed ledger)
Consensus rules (cryptography)
P2P Computer network (nodes, mining, tokens)

BLOCKCHAIN PROTOCOL
TCP/IP infrastructure

Since the launch of Ethereum, many other protocols and their corresponding blockchains have been launched. Each builds upon and refines the progress of its predecessors. Each seeks to address unmet market needs — speed, throughput, consensus efficiency, governance, and transparency. Figure 4 identifies a number of blockchain protocols and some of their characteristics. There are many other blockchain protocols.

Figure 4

PROTOCOL	PERMISSIONED/ PERMISSIONLESS	CONSENSUS MODEL*
Ethereum	Permissionless	Proof of work, but planning to move to proof of stake for scalability
Cardano	Either	Ouroboros proof of stake
EOS	Permissioned	Delegated proof of stake
Fabric	Typically permissioned	Variable
Sawtooth	Typically permissioned	Proof of elapsed time
Corda	Permissioned	Variable/validation by trusted participants
Digital Asset Platform	Permissioned	Validation by trusted participants

*Other consensus models include proof of activity, proof of burn, and proof of capacity. Each consensus model has advantages and disadvantages. The number of nodes and the consensus model impact the “scalability” of a blockchain. Many nodes combined with a challenging consensus model (such as proof of work) make a blockchain more resistant to attack or fraud, but require more energy and other resources and take longer to process transactions. Conversely, the fewer nodes used and the simpler a consensus model, the faster a blockchain can process transactions and the less it is potentially resistant to bad actors. Permissioned networks generally use fewer nodes and less challenging consensus models to achieve greater efficiency and processing speed.

The decentralization continuum

All blockchains are decentralized to some degree. Decentralization imparts a number of unique advantages to blockchain applications. Decentralized systems are fault tolerant. That is, they are less likely to fail because they involve the use of many separate components that are not likely to fail at the same time. They are attack resistant, meaning they are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at a much lower cost than the economic size of the surrounding system. Finally, they are *collusion resistant*, making it harder for participants to collude to act in ways that benefit them at the expense of other participants.

Decentralization, however, is not an all or nothing proposition. There are varying degrees. The number of network nodes can be very large or very small. Nodes can have wide geographic dispersion or be hyperlocal. Node operators may operate under a fully egalitarian system or have asymmetric rights depending on roles and functions or bargaining power when the network is organized. For instance, a near fully decentralized blockchain (e.g., Bitcoin or Ethereum) will have thousands of nodes dispersed around the globe. Conversely, an application built to manage a supply chain may involve only a manufacturer, wholesaler, distributor, and end purchaser. How decentralized a network is, and how many nodes participate, depends in part on the degree to which the blockchain is “permissioned.”

The permission continuum

Public blockchains are permissionless. Anyone with access to a computer can participate in the consensus function. Anyone can use the blockchain by sending transactions to it and, if valid, can see those transactions included in the blockchain. The transactions recorded on public blockchains can be viewed by anyone. Public blockchains are advantageous in a number of ways. Because of their large number of validating nodes and users, the potential for driving network effects is vast. Because the scale of the effort required to effect changes to the network is great, such systems are highly censor resistant and provide confidence that the network can be trusted. Public blockchains discourage fraud. Their permissionless design allows anyone to participate and allows them to serve as the backbone for almost any democratized solution, but the processing power required to run these networks is enormous and they process transactions more slowly than alternative systems.

Semi-private or consortium blockchains are permissioned and are sometimes referred to as distributed ledger technology rather than blockchains. They do not rely on anonymous nodes to validate transactions — the consensus function is controlled by nodes determined by the consortium participants. Only those who are part of (or authorized by) the consortium and who agree to the applicable roles, responsibilities, and governance structures may participate. The right to read the blockchain is typically limited and well defined. These systems value privacy and control. They are not designed for the degree of adoption and transparency of a public blockchain, but they are much less energy intensive and more efficient. They are perfect for enforcing business rules across known participants in a value chain in a hyper-efficient manner.

> Their permissionless design allows anyone to participate and allows them to serve as the backbone for almost any democratized solution, but the processing power required to run these networks is enormous and they process transactions more slowly than alternative systems.

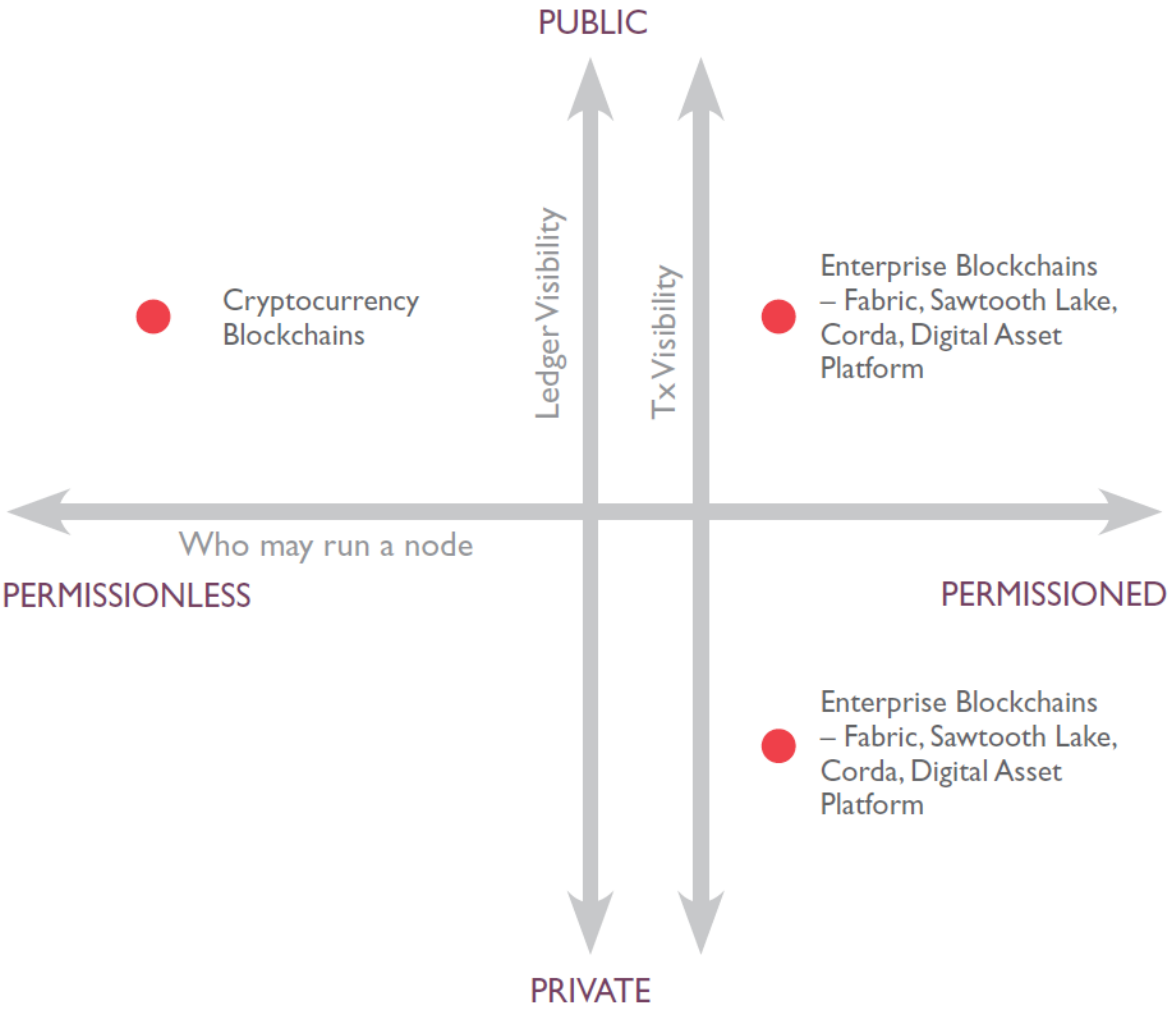
There are a variety of elements that might be permissioned in a blockchain. A protocol might require permission to initiate a transaction on the blockchain, read the information, or view the transactions on the blockchain. It might also establish limits or criteria for who can operate a node on the network. A blockchain protocol can be designed with the permission elements that address the business problems the blockchain aims to solve.

It is even possible to have a fully private blockchain controlled by a central organization and with clearly defined and controlled rights to view transactions on the blockchain. These are highly permissioned and may be unable to be accessed or read outside of the authority controlling the blockchain. The utility of these systems generally is limited to streamlining internal processes, managing databases, and auditing through cryptographic authentication.

Semi-private and private blockchains have a number of advantages. It is much easier to modify the protocol, fix software errors, or reverse transactions because the group necessary to reach a new consensus and make those changes is smaller, and the previously agreed upon governance structure provides processes for managing changes. The nodes are known and subject to a legally enforceable governance framework, so fear of collusion is reduced. Transaction validation occurs across a smaller set of validating nodes enabling the network to operate more efficiently, cheaper, and faster.

There is a correlation between the permission and decentralization continuum. Permissionless blockchains are the most decentralized. Consortium blockchains are less decentralized. Fully private blockchains are not decentralized at all. Figure 5 illustrates the public to private continuum, the permissioned to permissionless continuum, and location of selected blockchain protocols on those continua. There are many other protocols and each will have a place on the decentralization and permission continua.

Figure 5



What are some technical challenges?

Scaling to meet growing volume is a challenge for permissionless blockchains. Existing public blockchain networks do not handle nearly as many transactions as their centralized counterparts, and the speed of permissionless blockchains is impacted by their degree of decentralization. Each node participating in the consensus mechanism must validate each transaction, so the benefit of decentralization comes at a cost: The larger the number of nodes, the longer it takes to process a transaction, and the slowest node in the network can be a bottleneck. For example, the Bitcoin blockchain is estimated to process a maximum of seven transactions per second, while credit card networks process thousands of transactions per second. That volume of transactions would result in a very long blockchain and require even more energy and computer resources to validate transactions. Conversely, permissioned blockchains have fewer nodes and generally less intensive consensus protocols for validating transactions, and can provide orders of magnitude greater transaction throughput. If the current level of investment in blockchain projects continues or grows, the transaction throughput of permissionless blockchains likely will improve substantially.

Smart contracts and blockchains are implemented with software and are subject to the same challenges as any other software code. Human error — especially in coding complicated smart contracts — could be exploited. With public blockchain, if a mistake in the code is exploited, fixing it requires not only new code but a consensus among the participants to adopt the new code. If there is disagreement, a “fork” in the blockchain is likely to result. Validating nodes that continue to use the old software will see the invalid blocks, produced according to the new rules, and create a “hard fork” in the blockchain. For example, defective smart contract software allowed the theft of approximately US$50 million worth of Ether (Ethereum’s native cryptocurrency) from the DAO (an investor directed fund established on the Ethereum blockchain). To recover the Ether and fix the problem, approximately 85 percent of Ethereum miners agreed to update their software with changes to the rules used to decide whether a transaction is valid. This led to a fork in Ethereum: the Ethereum blockchain continuing with the new code, and the original blockchain continuing as Ethereum Classic, each with its own cryptocurrency. In a permissioned blockchain, defects are easier to fix because a previously agreed upon governance structure provides processes for managing change.

> For example, the Bitcoin blockchain is estimated to process a maximum of seven transactions per second, while credit card networks process thousands of transactions per second.

Generally, blockchains are not compatible with one another, meaning they are unable to share data with one another. Efforts to develop cross-chain functionality are growing. For example, Ripple developed the Interledger protocol for connecting different blockchain protocols and traditional digital ledgers using common Interledger addresses. For enterprise, blockchain might initially extend existing systems rather than replace them. For example, a transaction entered into a legacy supply chain management system could initiate a blockchain transaction involving each actor in the supply chain. The necessary integrations to each participant’s legacy systems could be challenging.

A blockchain is not optimal for containing large databases. A block on the blockchain contains a limited amount of data, and blockchains currently do not have the throughput and database query support that many use cases require. Solutions are being developed, such as BigChainDB, but have compromises. Data intensive applications could use a database that is stored off the blockchain.

> A blockchain is not optimal for containing large databases. A block on the blockchain contains a limited amount of data, and blockchains currently do not have the throughput and database query support that many use cases require.

In theory, if someone controlled more than half of the nodes in a permissionless blockchain network, that person could modify transactions and steal (or “double spend”) digital assets. Proof of work and other transaction validation mechanisms initially were performed by a relatively large number of dispersed nodes. But, as with any specialized activity, nodes have become more concentrated in large data centers and by smaller miners pooling their efforts, perhaps increasing the possibility of an effective attack on a blockchain. That centralization risk may increase as blockchain sizes increase, and greater resources are required to run full nodes. The risk of a “51 percent attack” has historically been viewed as hypothetical, but cryptocurrencies with smaller numbers of nodes have recently been successfully attacked, and attacks are predicted to increase in frequency.

What are some legal challenges?

The laws governing a client’s industry (and those governing your client’s customers) drive analysis of the legal suitability of any particular blockchain application.

For example, many financial services businesses are subject to “know your customer” requirements and obligated to implement anti-money laundering controls and file suspicious activity reports. They will be concerned about how to comply with a blockchain system. Healthcare companies may be concerned about how healthcare privacy laws, such as HIPAA, apply to blockchain transactions.

One challenge is the application of the European Union’s new General Data Protection Regulation (GDPR). Generally, GDPR makes European data protection law apply where the collection, storage, or processing of personal data related to EU residents occurs. GDPR is a challenge for blockchain because its requirements do not allow for blockchain’s unique characteristics. Challenges include GDPR’s requirement to delete personal data on request and to delete data after a contract expires or permission to use the data expires. It is impossible or very difficult to alter or delete the data in a public blockchain. Another challenge is the requirement for a written agreement between each “data controller” and each “data processor” — potentially difficult to accomplish if each node on a blockchain network is deemed a data processor.

On a private and permissioned blockchain, GDPR issues may be managed by design that complies with GDPR. On a public or permissionless blockchain, potentially anyone could access data protected under GDPR. One possible solution is to store all personal data in traditional databases (where it can be deleted when GDPR requires) and store only pointers to the data on the blockchain. However, this raises trust issues regarding the parties that maintain the data and concerns about the security of the data.

Smart contracts can facilitate commerce but not all contracts are well suited to be enabled on a blockchain. Contracts implemented in software code may not be able to capture all of the elements of a complicated agreement as not every arrangement can be translated into code. For example, the negotiation of complex agreements sometimes results in deliberate ambiguities, which may be impossible to automate with a smart contract. Smart contracts are best suited to commercial arrangements that operate on an “if/then” basis. As this area develops, expect more and more complex arrangements to find a home in smart contracts.

Some question whether smart contracts are enforceable. There are questions about how the statute of frauds impacts smart contracts, whether smart contracts are adequately signed, and about the evidentiary value of smart contracts. At least in the United States, the federal Uniform Electronic Transactions Act and state law equivalents support the enforceability of smart contracts.

Some states are adopting laws related to blockchain. A number of these laws are, very generally, aimed at supporting the execution of smart contracts on blockchain, and the admissibility of blockchain evidence. For example, Arizona amended the Arizona Electronic Transactions Act to support the enforceability of blockchain-based smart contracts related to certain UCC transactions. Nevada adopted similar amendments to the Nevada Uniform Electronic Transactions Act, which supports the evidentiary value of electronic blockchain records in legal proceedings and has prohibited local governments from taxing or imposing requirements on the use of blockchain. Other states are considering or adopting wider ranging blockchain laws. For example, Wyoming recently adopted five bills related to blockchain, including one providing that certain securities and money transmission laws do not apply to persons who sell or facilitate the exchange of "open blockchain tokens" — utility tokens as defined in the Wyoming bill.

Potentially more complicated are questions about what laws (and of what countries) will apply to blockchain transactions, what courts will have jurisdiction over disputes and the parties, and even where a smart contract is deemed to be entered into or performed. Some of these issues are more easily addressed in a private or permissioned blockchain where the parties and their locations may be known, but more difficult on a public blockchain with anonymous users.

Blockchain applications typically are based on the work of an open-source community or are open source in nature, and open-source software concerns apply when using an open-source blockchain. Managing open-source issues is a topic for another article, but some open-source licenses impact one's ability to maintain proprietary rights (including patent rights) in software that is based on or uses open-source code.

Open-source issues are sometimes tricky with blockchain. For example, the Ethereum Foundation makes different components available under different licenses and has not yet specified the license under which its core components may be used. Ethereum applications are distributed under the GNU General Public License (a "restrictive" or "copyleft" license). Ethereum middleware "will be distributed under an Affero license, likely the LGPL variant of it," intended to allow linking to proprietary software, but for integrations to be open source. Uncertainty is greatest with respect to the core components of Ethereum as the foundation has not specified the license under which Ethereum's core components may be used. We understand that the Ethereum Foundation has retained new legal personnel and expect that the foundation will maintain a liberal usage policy. But, until the Ethereum community determines the license that will govern its core components, developers must be comfortable with some risk that their work will be subject to a restrictive license.

Another concern with open-source licensing for blockchain projects is the compatibility of various opensource licenses. Permissive licenses generally are not compatible with restrictive licenses. This can impede the release of an application that uses components obtained under inconsistent licenses. For example, a potential collaboration between Hyperledger and Ethereum was abandoned because Hyperledger is available under a permissive Apache license, but components of Ethereum are available only under a restrictive GPL license.

Finally, initial coin offerings are a common way to raise capital for a blockchain project. These offerings are increasingly drawing the scrutiny of securities regulators and the plaintiff's bar. During recent testimony before the Banking Committee of the US Senate, Securities and Exchange Commission (SEC) Chairman Jay Clayton stated, "I believe every ICO I've seen is a security." The SEC has been clear that "Merely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security."

How should I think about it?

All of this may remind you of the early days of the commercial internet, and the sometimes frustrating challenge of applying existing law to a dynamic technology. Welcome back. As Figures 1 and 2 suggest, blockchain applications are as varied as people's imaginations. A blockchain solution might make sense if an important business process could be made more efficient or less expensive by removing an intermediary, reducing manual processes and potential errors, adding transparency and certainty for participants, or improving resistance to fraud or attack. Selecting a blockchain protocol requires assessing the business requirements of a use case and the legal obligations applicable to that use case and comparing them to the decentralization, permission, open source, and other characteristics of the blockchain protocols that might meet your needs. This requires thoughtful legal and business consideration but brings you one step closer to determining if your blockchain plans will satisfy your legal compliance requirements.

Further Reading

1 All terms are from Antonopoulos, Andreas M. "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" (1st Edition, 2014).

2 Nakamato, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008).

3 Lin William Cong and Zhiguo He, "Blockchain Disruption and Smart Contracts" (September 26, 2017).

4 Buterin, Vitalik. "The Meaning of Decentralization," *Medium* (February 6, 2017).

5 Buterin, Vitalik. "On Public and Private Blockchains," *Medium* (August 7, 2015).

6 Croman, Kyle; Eyal, Ittay. "On Scaling Decentralized Blockchains" (2016).

7 Bonneau, Joseph. "Why Buy When You Can Rent? Bribery Attacks on Bitcoin-Style Consensus" (2016).

8 Devan, Arun. "The Blockchain Technology Stack," *Medium* (November 3, 2017).

Les Wilkinson

General Counsel and Chief Development Officer

Hashed Health

Les Wilkinson is general counsel and chief development officer at Nashville, Tennessee-based company Hashed Health, a leading consortium of healthcare companies focused on accelerating meaningful innovation using blockchain and distributed ledger technologies. He manages strategic partnerships and corporate development.

Curtis Capeling

Member

Bass, Berry & Sims in Nashville, TN

He works with startup and emerging private companies, as well as public companies, on the protection and commercialization of IP rights and strategic transactions.