Blockchain Technology—Acquisitions & Joint Ventures

April 12, 2019

Blockchain technology continues to be a lively topic of conversation in legal, business and technology circles. This includes heated debates about whether and when the technology will deliver on its many promises and how the most common applications employing blockchain—that is, cryptocurrencies and other types of digital tokens—should be regulated in the United States and globally. Despite having experienced "crypto winter"—including a precipitous drop in cryptocurrency values, persistent skepticism about blockchain applications and a growing regulatory focus on the technology—many are convinced that the technologies underlying the blockchain are here to stay, and may hold great promise as a solution for solving certain commercial challenges.[1]

We will not add our views about the viability and promise of the technology to the existing cacophony of predictions—which range from how blockchain will revolutionize the internet to how it is little more than a curiosity. Instead, this memo focuses on several key topics for companies considering whether and how to invest in blockchain technology, either through acquisition of a particular blockchain, an acquisition of or joint venture with a company developing blockchain technology, or through financial investments in these companies. In doing so, we will also highlight some of the legal and related commercial considerations arising in transactions involving entities in the blockchain "ecosystem."

Blockchains: Different Schools for Different Trades

At its core, blockchain technology is a type of database system that employs certain characteristics designed to minimize the need among network participants to trust one central entity or record-keeper. These characteristics include (i) decentralization—both the data stored in the database and responsibility for maintaining the database are spread across multiple participants, (ii) a reliance on economic incentives, rather than on a centralized administrator, to guide users' interactions with the database and (iii) some form of anonymity, so that users may interact with the blockchain with only minimal identifying information.

Using these common characteristics, developers have built blockchains for a wide range of applications. Blockchains are being used to create and track digital currencies, manage supply chains, monetize intellectual property, protect health information and even issue complex financial instruments.[2]

For companies considering whether to use this technology, a key decision is whether to use a permissionless blockchain, a permissioned blockchain or something in between.

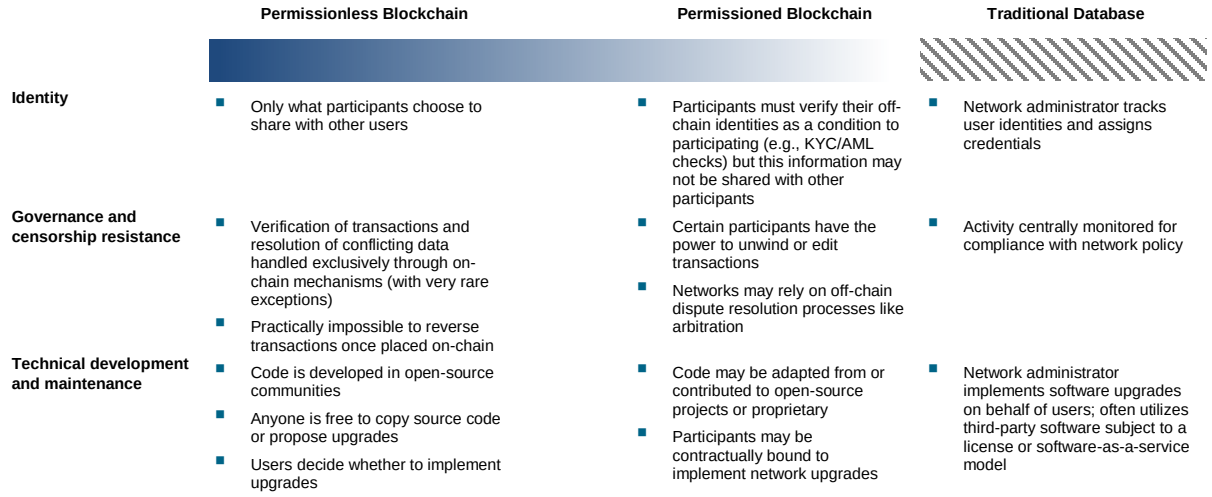
---

[1] See *Venture Capital Firms Go Deep and Wide with Blockchain Investments*, Diar.co (Oct. 1, 2018), **https://diar.co/volume-2-issue-39/#2** (noting that blockchain firms attracted about $4 billion in investments in 2018).

[2] Bitcoin, the canonical example of a blockchain built for digital currency, is discussed *infra* at note 4. A blockchain for managing supply chains is described later in this memo. Po.et is a blockchain project aiming to solve certain intellectual property-related issues. *See* **https://www.po.et/**. For a discussion of how blockchains could help manage healthcare data, *see* Kevin Peterson et al., *A Blockchain-Based Approach to Health Information Exchange Networks*, Mayo Clinic (2016), **https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf**. There are numerous applications being built on the Ethereum blockchain aiming to issue or create markets for loans, derivatives, collateralized debt instruments and the like. These are part of a larger project called "decentralized finance" (also called "DeFi"). *See*, *e.g.*, Sean Lippel, *Decentralized Finance is a Continuum*, Medium.com (March 4, 2019), **https://medium.com/@SeanLippel/decentralized-finance-is-a-continuum-179d43c6ef65**.

- **Permissionless blockchains** allow anyone to access and edit network data, as long as users run software agreed upon by a majority of the network's users.[3] The Bitcoin and Ethereum blockchains are the most prominent examples of permissionless blockchains.
- **Permissioned blockchains**, by contrast, restrict access so that only certain kinds of users can participate in the network. For example, a permissioned blockchain might be open only to qualifying companies in a particular industry, all of which must contribute capital in exchange for membership rights. **Corda** and **Quorum** are two well-known examples of permissioned blockchains.

That said, very few of the blockchains that exist today are purely permissioned or permissionless. Instead, many blockchains exist on a spectrum, blending features from both permissioned and permissionless systems. The chart below shows the key distinctions between permissionless and permissioned blockchains, and between blockchains and traditional databases. Where any particular blockchain falls on this spectrum will impact how useful it can be in an enterprise environment, as well as which legal issues are raised in potential transactions.



A spectrum comparing permissionless and permissioned blockchains. Both forms of blockchains share certain key features like on-chain identity management, censorship resistance and decentralized governance; these features are part of what makes them blockchains in the first place. However, as we move towards the right past permissioned blockchains, we eventually end up with a traditional database managed by a centralized network administrator.

Permissionless blockchains have generally not been useful in an enterprise environment. Since these types of blockchains enable anyone to access, edit and maintain the network, they are not well-suited for storing commercially sensitive information. Instead, most applications of permissionless blockchains accomplish tasks that are relatively straightforward from a technical perspective, but do so in an anonymous and decentralized way.[4] Additionally, given that these blockchains provide open access,

[3] Critically, this software sets rules on how users can edit, access and interact with the blockchain. These rules are designed and enforced using sophisticated economics, computer science and cryptography concepts, all in order to prevent dishonest users from manipulating data in destructive ways. Though a complete account of the technical principles of permissionless blockchains is beyond the scope of this memo, the essential point is that anyone is free to participate in the blockchain as long as they are running the correct software.

[4] One prominent permissionless blockchain is Bitcoin, which supports the virtual currency, or "token," of the same name. The Bitcoin blockchain is simply a ledger that tracks the amount of bitcoin tokens owned or attributable to particular Bitcoin blockchain addresses—something that can be easily accomplished using a traditional centralized database. However, unlike a traditional centralized database, any user with an internet connection can participate in the operation of the Bitcoin network, without the need (*cont.*)

many complex technical features are needed to prevent fraudulent activity and protect user data. These features generally make users' interactions with the blockchain relatively slow and expensive (in terms of computational requirements) compared to permissioned chains.[5] Thus permissionless blockchains may be designed to accomplish relatively simple tasks—for example, transferring digital units of value—but must do so through more complex processes.

Permissioned blockchains, on the other hand, may be useful to enterprises in a variety of contexts. These use cases stem from a core principle: blockchains create a shared computing environment with built-in checks against manipulation. This enables a variety of solutions to problems faced by participants in the digital economy. For example, imagine two parties to a commercial contract who must verify performance manually, even though both parties' internal operations are completely digitized.[6] Using a permissioned blockchain, the parties could design software that monitors their digital systems to assess when contractual conditions are satisfied, and then automatically facilitates the payments contemplated by the contract.[7] If the parties used a traditional database, one party would be required to serve as an administrator, collecting and verifying data, tracking costs and enforcing governance rules, which poses an obvious conflict of interest and slows down the transaction.[8]

Some permissioned blockchain projects include:

- **Hyperledger** is a governing body for a range of permissioned blockchain applications. It is unique in that it is dedicated to deploying blockchains that are open-source.[9] Hyperledger currently offers an array of blockchains that solve specific technical challenges and that are marketed to companies or cooperative bodies hoping to improve the efficiency and speed of commercial activity. For example, a trade association is using Hyperledger to unite disparate databases that have been maintained in isolation by members across the country. Though these members were initially reluctant to give up control over their data, the association used Hyperledger to enable nation-wide access to data while preserving local control.
- **A technology company and a global retailer** are working to implement a blockchain that can help manage the retailer's complex supply chains. The global nature of supply chains requires that goods be handled by multiple intermediaries and shipped through many jurisdictions, adding cost and significant time delays. At the same time, consumers expect greater transparency over what they buy at the point of sale. By combining its blockchain with other emerging technologies like internet-of-things sensors, the retailer will be able to track

---

(*cont.*)

for an account or verification from some central third party. This functionality, in turn, requires a set of complicated technical rules to ensure participants behave in ways that are generally beneficial to the network.

[5] In most permissionless blockchains, the primary expense of interacting with on-chain data comes in the form of mining fees. These fees are paid to incentivize network users to donate their computing power for network maintenance. Fee levels are not set by a central decision-maker but emerge through a market equilibrium, according to rules built into the blockchain's software. Of course, the fastest and most efficient form of database is a traditional centralized one, in which a network administrator provides a computing environment to users and monitors for fraudulent behaviors as part of its organizational mandate.

[6] This is not merely a hypothetical scenario. More and more businesses rely solely on digital systems throughout their commercial lifecycle, from interactions with banks and investors, to sourcing materials, advertising and marketing products, tracking purchases using point of sale systems, and managing information using cloud storage.

[7] This software is commonly called a "smart contract." For an overview of smart contracts and the legal issues they raise, *see* Kevin Werbach and Nicolas Cornell, *Contracts* Ex Machina, 67 Duke L.J. 312 (2017), **https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj**.

[8] The parties could instead attempt to choose a neutral third party to perform these activities. However, this adds another layer of costs, reducing the economic attractiveness of this arrangement, and it presents a potential attack vector for any would-be cyber-attacker.

[9] A key partner is the Linux Foundation, one of the most prolific open-source software consortiums in the world.

individual items through its supply chains and ensure that necessary documentation follows these items at every stage. This should not only reduce frictions as goods travel across jurisdictions, it will also enable consumers to access information about where their goods were produced.

As these examples illustrate, permissioned blockchains are also useful where there are burdensome paper-based processes that span multiple entities or countries, and where competitors would like to cooperate in limited ways to produce useful data.

Transactions Targeting Permissioned Blockchains: Acquisitions Versus Limited Investments

A firm wishing to deploy blockchain technology could either develop it itself, buy the right to participate in an existing system or buy an existing system outright. We focus below on transactions involving permissioned blockchains. Not only are permissionless blockchains a poor fit in most enterprise environments, but these types of blockchains are only rarely associated with legal entities that could serve as viable transaction targets.[10] Many permissioned blockchains, conversely, are managed by traditionally structured corporate entities, but even these must remain fundamentally "open" to ensure participation by a range of stakeholders. The deal-making environment will therefore be similar to other technology transactions in some ways, but in other ways markedly different.

We consider two different transaction forms: full acquisitions and limited investments. Acquisitions will usually pose the most novel risks when targeting a blockchain. However, because acquisitions provide the acquirer with maximum control over the target blockchain, they may make sense for companies that wish to implement a blockchain in their operations.[11] This control will enable the acquirer to modify the target blockchain so that it is interoperable with the acquirer's existing IT systems, and to implement future changes in response to competitive headwinds.[12]

The target in this kind of acquisition could be a software development company that owns proprietary blockchain solutions deployed in a given industry. These targets may be attractive since they include valuable human capital—blockchain software developers—who can help the acquirer with maintenance or further development of the blockchain. Another possible target would be a trade association or other industry group that manages a specific permissioned blockchain, though this could make for a complicated negotiating environment.[13] As in the traditional M&A context, acquirers could choose between buying the target's equity or assets, or performing a merger, with tradeoffs involved in each.

---

[10] Ownership of a company developing products or services for a permissionless blockchain would primarily be a financial asset—giving the acquirer exposure to the underlying cryptocurrency generated by on-chain activity—which raises a unique set of strategic and economic issues beyond the scope of this memorandum. Additionally, only a few permissionless blockchains have relevant legal entities that could be a feasible transaction target in the first place. Permissionless blockchains are ultimately open-source networks that invite anyone to participate. There is little by way of proprietary intellectual property or other assets that could be acquired in a transaction.

[11] For example, the acquirer might want to implement a permissioned blockchain to make its supply chain run more efficiently.

[12] As this point illustrates, operationally motivated acquirers must also be prepared to make changes to how the target blockchain is governed. This suggests a tradeoff involved in outright acquisitions: an acquirer seeking full control over management of the blockchain will cause that blockchain to be more centralized and thus less useful as a blockchain. A joint venture offers more flexibility—an acquirer with less than a full equity stake can leave some equity for other participants, and customize these stakes to include special governance rights.

[13] Since the trade association would likely involve participation by the acquirer's competitors, a potential transaction could give these competitors holdup power.

Legal and Commercial Considerations in Acquisitions of Blockchain Technology Companies

All transactions targeting blockchain technology raise special considerations, a core group of which we outline below. But it is important to note that a full acquisition poses these risks in an acute way, especially where deal value depends on integrating a permissioned blockchain into the acquirer's existing systems.[14]

- **Governance**. One important consideration relates to governance. As a blockchain becomes more centralized, it looks less like a blockchain and more like a traditional database. Elements of centralization will certainly be useful to the acquirer, but too much centralization will give the acquirer control to manipulate or unmask on-chain data. If the acquirer comes to dominate the acquired blockchain's technical or economic environment, that blockchain can no longer offer a shared landscape that facilitates the decentralization of trust from one central party—in other words, that blockchain will replicate the centralized dynamic of traditional databases, in which a core administrator controls the other users. Importantly, even the *perception* that these outcomes could occur would drive some participants elsewhere, because an acquirer that retains some latent right to unilaterally control or censor the blockchain is still an extremely centralized presence. To mitigate these risks, an acquirer could enter into agreements with other participants that contractually limit its own ability to make certain kinds of governance decisions, such as unmasking on-chain data. An acquirer could also offer participants equity in a limited joint venture formed for the purposes of governing the blockchain, or transfer governance rights to an independent nonprofit, to signal that the acquirer views decentralization as an important factor in the overall health and value of the blockchain. Finally, the acquirer could give participants the right to influence dispute resolution processes, such as the right to choose an arbitrator.
- **Post-Transaction Integration**. Related to governance, an acquirer must be prepared to spend time and resources to ensure the blockchain can be effectively integrated into its existing systems.[15] The operational and technical aspects of permissioned blockchains are still cutting-edge. Integrating these systems with an existing IT infrastructure might result in unforeseen costs or create organizational challenges. While an acquirer can minimize these by retaining the right to guide the blockchain's technical decision-making as it sees fit, this raises governance issues discussed above.[16]
- **Intellectual Property Rights**. Blockchain technology is subject to intellectual property protection in the same ways as other software and is often covered by a mix of copyright, patent rights and, particularly for permissioned blockchains, trade secrets. Permissionless blockchains typically utilize open-source software and can derive substantial value from the fact that their code is open-source and auditable by communities of users. On the other hand, permissioned blockchains are generally proprietary to their developer, but may nonetheless integrate some features modeled after or built from open-source code. An acquirer buying a

[14] Some acquirers may also consider commercializing the acquired blockchain itself, whether through licensing or through charging for participation in the network.

[15] In the licensing context, the licensee would face these integration costs—and indeed the licensor may offer integration services as a value-added service. To the extent that the acquired blockchain is being licensed, new licensors will face integration challenges, and the licensor may offer integration as an add-on service.

[16] In other words, all participants will face operational challenges in integrating the blockchain with their existing systems. The question is which participants face the steepest versions of those challenges. An acquirer might wish to minimize its costs by retaining control, with the effect that other participants' integration costs increase. If those costs are too high, participants will look for more flexible alternatives.

permissioned blockchain with some open-source elements should insist on appropriate seller representations and warranties in the transaction agreements to understand exactly which features are proprietary and which are open-source, and may consider conducting an open-source audit for verification. Additionally, open-source projects are mostly maintained by anonymous communities working for free. Open-source features of a permissioned-blockchain may face obsolescence as these communities turn their attention to new projects.

- **Cybersecurity and Attacks**. Cybersecurity poses another important challenge. All blockchains, whether permissionless or permissioned, combine principles from economics, computer science and cryptography to guide participant behavior. As a result, the acquired blockchain will face complex threats from both on-chain participants and external actors. Attackers could exploit the acquirer's blockchain towards fraudulent ends, such as spoofing on-chain data or stealing sensitive information, in ways that they could not in a traditional database.[17] If attackers target a blockchain that has already been integrated into the acquirer's systems, they could also threaten the acquirer's operations more broadly. Threats from blockchain participants can be managed contractually, for example by providing the acquirer audit rights over participants' IT systems, though external threats will be harder to address.
- **Sanctions and Illegal Transactions**. Blockchains facilitate anonymous (or pseudonymous) global interactions, creating the risk that blockchain participants could unwittingly transact with or through entities subject to sanctions or other regulatory regimes. For example, there is evidence that both North Korea and Venezuela are using blockchains to evade US sanctions, a trend which is likely to continue.[18] This risk can be mitigated in permissioned chains by conditioning participation on users providing information about their off-chain identities.[19] Acquirers should scrutinize technical mechanisms for verifying off-chain identity and consider seeking an indemnity to hold sellers financially liable if such features turn out to be faulty.

Limited Investments May Mitigate Some Risks of Full Acquisitions

The above issues are likely to emerge in any kind of permissioned blockchain investment, but some may be mitigated where the acquirer makes only a limited investment. Limited investments could take many forms, such as minority investments in the kinds of entities discussed above, joint ventures with those entities, or the purchase of licensing rights to deploy proprietary code.

These would be especially suited for investors motivated by learning—a minority investor could structure their investment to include the right to observe that blockchain's technical developments or decision-making processes, or even to unmask data about on-chain transactions. Minority investments would also

---

[17] For a review of the unique security risks faced by blockchains, see Mike Orcutt, *How Secure is Blockchain Really?*, MIT Technology Review (April 25, 2018), **https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/**. For a discussion of how these risks change in a permissioned blockchain context, see Duncan Jones, *How to Secure 'Permissioned Blockchains*, InformationWeek IT Network (Feb. 28, 2018), **https://www.darkreading.com/endpoint/how-to-secure-permissioned-blockchains-/a/d-id/1331129**.

[18] *See*, *e.g.*, Cali Haan, *Two Finance Crime Experts Say North Korea Probably Using Crypto to Skirt US Sanctions*, Crowdfund Insider (Sept. 27, 2018), **https://www.crowdfundinsider.com/2018/09/139528-two-finance-crime-experts-say-north-korea-probably-using-crypto-to-skirt-us-sanctions/**; Brian Ellsworth, *Special Report: In Venezuela, New Cryptocurrency is Nowhere to be Found*, Reuters (Aug. 30, 2018), **https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U**.

[19] A simple way to implement this would be to require participants to submit KYC/AML information over the internet, though this has a strong centralizing element.

be useful to investors who want to influence a blockchain's governance processes, but who want to avoid perception of centralization triggered by a full acquisition. Perhaps the most attractive feature of a limited investment is that it can be phased into a full acquisition over time. As with early stage investments in other emerging technologies, we expect a wave of minority investments to occur before full-scale acquisitions.[20]

However, limited investments will also pose risks, and many of those discussed above in the context of full acquisitions will apply. But limited investments change the balance of incentives, leaving ownership and control in the hands of the existing operator of the blockchain. This mitigates risks in two important ways:

- **Governance**. A full acquirer of a permissioned blockchain may end up with too much influence over that blockchain (or other participants may perceive this to be the case), threatening that blockchain's level of decentralization. On the other hand, a more limited investment may strike an effective balance by leaving existing checks-and-balances in place. Investors who wish to phase limited investments into full-scale acquisitions should consider measures to ensure other participants will still have meaningful governance rights during this phase-in period.
- **Post-Transaction Integration**. A limited investment could easily be structured to leave legacy technical resources in place. These resources will be useful to an investor motivated by learning goals or those who wish to move from minority to full ownership over time. Since the original owner retains ownership of the blockchain, incentives to maximize the value of that blockchain are still in place.

[20] For research on corporate development strategies in the emerging technology context, see Werner H. Hoffman and Wulf Schaper-Rinkel, *Acquire or Ally? A Strategy Framework for Deciding Between Acquisition and Cooperation,* 41 Mgmt. Int. Rev. 131 (2001); Edward B. Roberts and Wenyun Kathy Liu, *Ally or Acquire? How Technology Leaders Decide*, 43 MIT Sloan Mgmt. Rev. 26 (2001).

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Frank J. Azzopardi	**212 450 6277**	**frank.azzopardi@davispolk.com**
Daniel Brass	**212 450 4153**	**daniel.brass@davispolk.com**
Joseph A. Hall	**212 450 4565**	**joseph.hall@davispolk.com**
Jai R. Massari	**202 962 7062**	**jai.massari@davispolk.com**
Annette L. Nazareth	**202 962 7075**	**annette.nazareth@davispolk.com**
Byron B. Rooney	**212 450 4658**	**byron.rooney@davispolk.com**
Zachary J. Zweihorn	**202 962 7136**	**zachary.zweihorn@davispolk.com**
Daniel F. Forester	**212 450 3072**	**daniel.forester@davispolk.com**
Trevor I. Kiviat	**212 450 3448**	**trevor.kiviat@davispolk.com**

The firm gratefully acknowledges the assistance of law clerk Jeremy M. Sklaroff in preparing this memo.