Blockchain and Mitigating Corporate Risk

Authored by Alison Wisniewski, Chief Legal Officer, Epiq, with extensive instruction and input from members of The Industry Group for Blockchain + Legal

New technology is constantly being introduced into the legal environment. One of these, Blockchain, is a burgeoning technology with which general counsel and legal departments should become familiar. With the adoption of blockchain for some business functions such as supply chain management and payment services, legal departments will need to understand blockchain, including the rules and regulations around what types of transactions can be completed, as well as the types of data that should or should not be included on the blockchain. This white paper is intended to highlight questions legal departments may have when contemplating using blockchain and provide some suggested guidelines around how to address those questions.

> Legal departments will need to understand blockchain, including the rules and regulations around what types of transactions can be completed, as well as the types of data that should or should not be included on the blockchain.

INTRO TO BLOCKCHAIN

First things first – what is Blockchain? Blockchain (public or private) is a type of distributed and decentralized ledger technology where users can securely record certain types of transactions and determine who has access to such transactions. Identities of the individuals involved in a transaction may not be disclosed. Transactions conducted on blockchain are permanent and cannot be altered secretly – any alteration can occur if a party or group of parties control 51% or more of the blockchain and such alterations will be noticed by the other parties. An established protocol instructs computers on the network about when a transaction is verified and should be added to the ledger – this is the only way a transaction can become a permanent part of the blockchain.

Issues may arise if a matter has some data on blockchain and some data not on blockchain, in which case an expert may need to be consulted to determine which data is accurate.

Blockchain improves trust and communication among the parties in a transaction. It may reduce the cost, speed and risk of some business processes while increasing security. Some areas where companies are utilizing blockchain include supply chain management, trade finance and syndicated loans.

GOVERNANCE

Anyone familiar with the legal industry is quick to point out the slow pace at which the legal industry embraces change and the utilization of blockchain will be no exception. One way to speed up change is to have court opinions around the use of blockchain. One of the first questions to be asked is what will it take for the legal industry around the world to accept blockchain as a standard of truth? Will courts accept data on blockchain as truth?

Over the course of time, courts have accepted new technology. If opposing parties to a litigation signed on to blockchain and made a conscious decision through mutually accepted contractual

terms to use it as a way of transacting, courts most likely would be willing to accept it. If the parties who join the blockchain agree at the outset as to what is going into the blockchain as evidence, there should be no issue with courts viewing it as a standard of truth. Issues may arise if a matter has some data on blockchain and some data not on blockchain, in which case an expert may need to be consulted to determine which data is accurate.

Governance models within blockchain networks are evolving but an important function is to guide how participants interact with one another when using the blockchain. A blockchain network should provide clearly defined ownership, security, and resolution process strategies before inviting participants to join. When determining whether to use blockchain, the parties should consider the following questions:

· What types of roles will participants play?
· What parties will be permitted to compute on the network. What is the process of revocation if a participant wants to leave the network? Is there a mechanism to incentivize computations, and who will bear the expenses?
· What are the items people must agree upon and be comfortable with to join a shared blockchain ledger?
· What types of information should be put on the blockchain and what should remain off network?
· Who is responsible for maintaining cyber security over the blockchain?
· Is there any additional liability risk to using blockchain? If so, is it possible to structure the blockchain to mitigate such increased risk?

The core legal fundamental principles of establishing a legal approach are not that different. The questions arise when learning how to apply those legal fundamentals to a new technology such as blockchain. These questions most likely will be addressed through the negotiations of agreements where the use of blockchain is considered.

DATA PRIVACY

Global privacy laws require the party controlling personal data of an individual to safeguard the

Blockchain networks may span numerous jurisdictional boundaries, making determining legal jurisdiction, including which privacy regulations govern storage and processing of data, difficult.


privacy and security of such data. This may pose concerns for legal departments whose clients may want to use blockchain for transactions. Blockchain differs from other data storage because in a public blockchain system, no single party takes responsibility for the security of the blockchain network, and all users of the system may have access to the data on the network. In addition, blockchain networks may span numerous jurisdictional boundaries, making determining legal jurisdiction, including which privacy regulations govern storage and processing of data, difficult. There are a few questions to consider when determining what data should be put on blockchain and how access should be controlled including:

· What data is necessary to store on blockchain and what data can be stored off blockchain?
· Who owns the data submitted to the network?
· What kind of data privacy does the network need? Are the encryption and/or access restrictions sufficient to satisfy the requirements in the jurisdictions where processing will occur?
· If members leave the network, can they take their data with them?
· Where will the work be done and where are the companies who are parties to the transaction based?
· Do the parties need to contract for the processing of personal data? What are the roles of the parties (processing and validating transactions vs. pushing data to the blockchain, for instance)?
· What privacy level of access will the blockchain require? Will certain entities (regulators, law enforcement, courts) be given access to some or all of the blockchain? Are third party permissions contemplated?
· Do network participants require access to the data?
· Are there limitations on where processing, publishing, or accessing the blockchain can be implemented?
· Are there data retention concerns? Do all parties on the network agree on retention rules?

From a data privacy perspective, the right to be forgotten cannot be exercised easily in blockchain. Data remains on blockchain for the duration of the network. There may be certain kinds of information that should never be placed on blockchain because it can never be deleted or destroyed; yet it can be difficult to prohibit such information from being published to the transaction ledger. Only newer versions of the blockchain ledger can replace older versions. One suggestion to mitigate access or privacy concerns is to use a private or permissioned blockchain. All data on the private or permissioned blockchain is encrypted and each participant in such blockchain has its own key for its own data which no one else has access to. When a participant wants to leave the blockchain, the key gets destroyed, thereby protecting the privacy of the data on the blockchain and preventing access to such data from any other participant in the blockchain. The downside of a private ledger is decreased security, trust, and increased costs compared to a public ledger. However, if public blockchain is used, all participants can access all data regardless of ownership.

From a data privacy perspective, the right to be forgotten cannot be exercised easily in blockchain.
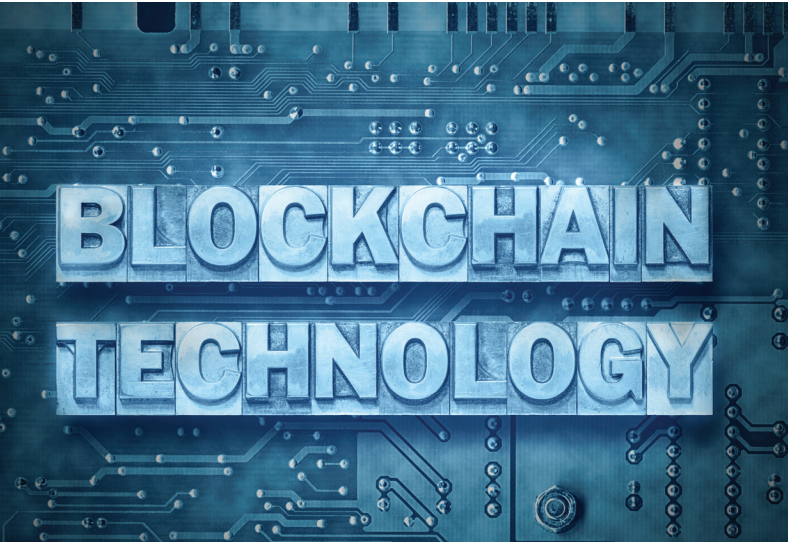
EDISCOVERY

Blockchain could very likely impose collection and review hurdles for the legal industry, as data stored on blockchain will become discoverable data for litigation and investigations and there are currently no tools to support such collections and review from the blockchain. Special protocols most likely will need to be developed in legal departments to mitigate possible challenges and potential new developments involving blockchain and blockchain data. Legal teams will need to determine what the terms and conditions are to enable the blockchain to work as efficiently as intended to protect against bad faith disputes.

Data on blockchain is permanent and can only be edited in limited circumstances. If security of data is not absolute, is the eDiscovery dispute minimized or does it become more complex and technical? Legal teams should be prepared to spend time and effort in locating proper custodians of data as there will be instances where blockchain transactions won't identify owners of data. Experts may be required to confirm identities of individuals involved in a transaction or matter as well as ratify the blockchain as being a legitimate technology to use for the transaction.

Authentication of blockchain as evidence for a case may take additional time and resources, as the technology grows and matures with time. A cost benefit analysis may need to be completed to determine if using blockchain data as trial evidence is efficient.

At the outset, legal departments may consider working with their organizations to create policies around the use of blockchain for business purposes. Having a robust data classification and data mapping program will help manage these types of transactions. In addition, monitoring blockchain developments, training staff, and keeping an eye on how courts are treating blockchain are suggested areas of focus for legal departments as adoption of blockchain continues.

BLOCKCHAIN + LEGAL
INDUSTRY GROUP

www.blockchainpluslegal.org