Distributed Ledger Technology and Cryptocurrencies

– What Secretaries of State Ought to Know…Now

These aren't new terms, but distributed ledger technology (DLT, e.g. blockchain) and cryptocurrencies went from just a few general concepts mentioned by the National Association of State Chief Information Officers (NASCIO) in 2016, to what the group is now calling the "next big transformational technology" in government. Why? Here's a few key concepts to summarize recent events and considerations to help keep the National Association of Secretaries of State (NASS) membership looking ahead.

Noteworthy Legislative Changes

According to NASCIO's program director for enterprise architecture and governance, Eric Sweden, the presentation of DLT and its association to cryptocurrency is likely to be more significant than the introduction of Internet.[1] In considering distributed ledgers and blockchain, NASCIO encourages government to take it slow. In a March 2018 NASCIO webinar that collaborated with the Association of Government Accountants (AGA) Blockchain Working Group, the key takeaways on blockchain in government were 1) the original purpose was to invest in technology that was portable and could be repurposed, to reduce double spending, 2) DLT is not an all- encompassing solution, but rather another tool in the toolbox for government technology, and 3) DLT has a lot of potential but is still relatively immature.[2]

In Colorado, the governor signed an act concerning the use of cyber coding cryptology in state records on May 30, 2018. By doing so, Colorado continues to be a government sector technology pioneer. Focusing on the protection of state records containing trusted information about individuals and organizations, all records repositories must now maintain metrics that monitor the benefits and costs of adopting distributed ledger technology (DLT) and consider secure encryption methods to advance overall data security of their records.[3] The metrics must be reviewed annually by representatives of the Governor, Department of State and the Department of Regulatory Agencies.

> "This is a very big deal… It's going to have a huge impact on how we do business, accounting, auditing – anything that has a data lineage to it."
>
> **– Eric Sweden, NASCIO Program Director for Enterprise Architecture and Governance**

Illinois is another state leading the charge, focusing their "Illinois Blockchain Initiative" on six (6) state and local agencies focused on ensuring minimal governance of the technology, supporting a blockchain system with their economic investments and promoting integration throughout state government. A pilot program is underway in the Cook County Record of Deeds office, placing thousands of vacant Chicago properties into blockchain. This put an immediate end to scammers illegally selling these vacant homes to unsuspecting buyers.[4]

---

[1] Farmer L. (2017, September). The Next Big Technology to Transform Government. Retrieved June 20, 2018, from http://www.governing.com/topics/mgmt/gov-blockchain-technology-government-services.html

[2] Blockchain in Government - A Perspective 2017 Year in Review (webinar). (2018, March). Retrieved from https://www.nascio.org/Publications/ArtMID/485/ArticleID/625/Blockchain-in-Government-A-Perspective-2017-Year-in-Review-webinar

[3] Cyber Coding Cryptology for State Records. (2018, May 07). Retrieved from https://leg.colorado.gov/bills/sb18-086

[4] Farmer, L. (2017, September).

Advantages/Disadvantages of Centralized Ledger

Most of today's databases and informational registers are founded on the principle of a centralized ledger where the ledger is maintained in a single, or centralized, location by administrators in an organization with authority to access the content of the register. Then, there is a public accessibility to the centralized ledger, but this public accessibility doesn't allow manipulation of the content.[5]
For example, in a business entity register, where corporations and other entity types must register and maintain their entity status, the Secretary of State's authorized employees have access to the content of the register. Members of the public have accessibility to the register to search, view and file documents, however, only the Secretary of State employees can manipulate the contents.

Advantages of a Centralized Ledger	Disadvantages of a Centralized Ledger
Reduced data redundancy	Greater potential for loss or inaccessibility (if the centralized location experiences an outage)
Limited access points to data for increased security	Inability to recover lost data
Centralized administration	Reliance upon network connectivity to allow access for users
Centralized end user access	

A distributed ledger, blockchain for example, addresses the disadvantages of a centralized ledger register by distributing the contents of the ledger to a network of nodes where many users utilize a software technology, called distributed ledger technology (DLT), and each node has a complete and exact copy of the full content of the ledger. In a business entity register, a node may be represented by an individual, an organizational entity, a regulatory agency or financial institution; none of the nodes may be designated as a primary node, therefore there is no equivalent to the authorized Secretary of State's employees in a centralized ledger who may manipulate ledger content.

Summary of Key Considerations

1. Platform Integration

   As it exists today, distributed ledger technology is not an out-of-the-box-type technology that can be integrated with existing government systems. According to research by the Governing Institute of KPMG, 13 percent of government agencies in the health and human service realm admit that outdated infrastructure will present a problem.[6] Preparing for the inclusion of

[5] G. (2017). Are Intelligent Automation & Blockchain Poised to Disrupt HHS? [Pamphlet]. Governing Institute (for KPMG), www.governing.com.

[6] Schwarz, M. (2018, June 19). Crypto Transaction Speeds 2018 - All the Major Cryptocurrencies. Retrieved from https://www.abitgreedy.com/transaction-speed/

distributed ledger technology will require investment in not only advanced technology platforms, but also in development of the internal skills needed to maintain and support the new technology

2. Network Size and Transaction Speed

The strength of the distributed ledger against security breaches is based upon how hardy and widely distributed the network is. More nodes mean more distribution that create a more powerful, robust network. Today, debate exists around whether this may frustrate the purpose of moving a permissions-based project to DLT. Customer satisfaction in today's online registry service offerings is commonly gauged by the overall speed at which a transaction can be completed. For a business entity or its registered agent, each annual report filing should be quick; producing a confirmation that the transaction is complete as quickly as possible. Currently, a cryptocurrency transaction, which is used to process payments in digital ledger technology, can take anywhere from several minutes to days. Cryptocurrency options include Bitcoin, Ethereum, Ripple, Litecoin, Bitcoin Cash, Monero and many others. Currently, Bitcoin transactions average 78 minutes to complete; the transaction must update all the nodes to reflect the latest additions.[7] Network load and speed must be properly measured at high volumes to minimize the time it takes to sync numerous, mirrored nodes.

3. General Data Protection Regulation (GDPR)

The European Union considers personal privacy a fundamental human right under their Charter of the Fundamental Rights of the European Union. Article 17 of the General Data Protection Regulation (GDPR), in effect as of May 25, 2018, ensure that subjects have a right to be forgotten and companies must erase any personal information that was collected for a purpose and that purpose is no longer necessary. A similar right to be forgotten exists in California, protecting minors with respect to websites and online services. Today, the concept of DLT creates a permanence in the full content of the ledger; a new DLT development or an additional technology must be built into DLT to properly comply with GDPR. The permanence of a distributed ledger must give consideration to any applicable records retention limitations and the requirements of payment card industry data security standard (PCI compliance).

4. Jurisdictional Issues

Because each node in DLT is an exact, mirrored copy of all the others, the actual location of the node in terms of determining jurisdictional standing for purposes of title, registration, regulation and contract law could lead to cross-border confusion. For example, under Article 9 of the Uniform Commercial Code, a financing statement is filed in the jurisdiction where the collateral is located. If the collateral is a cryptocurrency (e.g. Bitcoin or Ethereum), how is the filing location of the financing statement determined if nodes exist in multiple states? Because there is no primary node, parties may disagree on the proper jurisdiction for filing. In turn, perfection of the secured transaction may be called to question in a court of law.

5. Service Level Agreements

Many software solution providers specify a service level agreement (SLA) in their service obligations, explaining what they are able to perform and indicate a response time for each type of performance. For example, an SLA will define the priority of an

[7] California Business and Professional Code § 22580-81.

outage and agree to return service for a client within a specific time frame. The details of an SLA are based upon the provider's familiarity with their own system and infrastructure and usually limited to incidents not caused by a third party. Distributed ledgers introduce third party nodes outside of a solution provider's network, potentially impacting the terms of an existing SLA.

Long Term Goals

1. Avoid Re-evaluating

Every government agency intends to make technology decisions with long-term goals in mind. Every technological advancement is meant to be fit for purpose for years; Secretaries of State advancements are no exception. Start by assessing the true risks that exist in registries today. Is interagency collaboration challenged due to isolated data stores? For example, does the coordination of business formation and business licensing by multiple agencies need improvement? Is data security commonly threatened by attempted breaches or hacks? An argument can be made that a decentralized database, as exists in a distributed ledger, also decentralizes the target of the hacks and minimizes risk.

The key findings of NASCIO indicate that distributed ledger technology, or blockchain, may not be a universal remedy, rather an instrument for the future, in need of further refinement. Consideration for the overall investment in new technology and advanced internal skills is a condition precedent for government agencies.

2. Establish a Business-Focused Analysis

To date, DLT has been more technology initiative than business initiative. Success in implementation of any new technology requires a partnership of professionals with both business and technology expertise. Collaborate with your government counterparts to gather as much knowledge as possible. Each state faces both common and unique challenges and risks, many of which mirror the considerations around DLT. Conduct a use case or investigate the problem your jurisdiction seeks to overcome; in turn, you can start to build the right solution. Decide upon the business standards the technology solution must meet (e.g. Investigate potential users, evaluate current business-facing risk as well as technology risks).

A collaborative approach, focus on current and future needs and dedication to technology success will help address this decision effectively and to satisfaction...for the long term.

For questions, comments and further discussion please contact:

Justin Hygate, VP Registry Innovation
justin.hygate@fostermoore.com

Bill Clarke, EVP Business Development & Partnerships
bill.clarke@fostermoore.com