Texas Department of Information Resources (DIR) Blockchain Proof of Concept (POC)

Abstract

Key features of Blockchain technology, uses cases, and proof of concept.

Department of Information Resources

9/7/2018

Table of Contents

Overview

As the technology leadership organization for Texas State Government, DIR conducts evaluations and proofs of concept for new and emerging technologies. Rapid growth in adoption and the expansion of use cases make blockchain technology increasingly relevant for private and public organizations. DIR launched an internal Proof of Concept (POC) in late 2017 to assess the viability of Blockchain technology as a tool for solving complex business problems. This whitepaper outlines lessons learned and offers a new approach to the POC specifically for blockchain technology.

What is Blockchain?

A **blockchain** is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. To be clear, blockchain is not another term for Bitcoin. Rather, Bitcoin is an application that runs on blockchain technology. Blockchain enables Bitcoin transactions to take place on a decentralized, distributed, and public digital ledger. Bitcoin's use of blockchain-based transactions made it unique among currencies when it was first created, which contributed to its rapid growth in popularity.

Blockchain itself is an open source distributed ledger technology (DLT) suited for the secure storage and retrieval of data. It is based on peer-to-peer network architecture with no central authority. This represents a shift away from centralized database technology and essentially eliminates the single-point-of-failure scenario, which is problematic with centralized systems.

In terms of key value-added features, these three were at the top of our list:

1. **Shared / Unchangeable Ledgers –** Records cannot be altered retroactively
2. **Smart Contracts –** Automated business logic can be embedded in the blockchain
3. **Trust Factor** – All Transactions are validated by all nodes on the network

These features made a compelling case for investigating blockchain as a technology for solving complex business problems.

Key Blockchain Features

Capabilities	Key Features	Benefit
Network Protection	• **Peer-to-peer network** • **Geographically distributed nodes**	• **Decentralized authority** • **Eliminates single point of failure**

Data Protection	• **Each record in the ledger is assigned a unique Transaction ID dependent/linked to previous record's ID (i.e., chain)** • **Ledger is replicated across all nodes (i.e., Blockchain)** • **Transaction validation via majority-consensus approval/governance algorithm** • **Data encryption; ledger is encrypted to restrict access to authorized parties only**	• **Immutability (no edits allowed)** • **Transaction validation mechanisms based on consensus algorithms (e.g., proof-of-work, Byzantine Fault Tolerance, etc.)**
Business Value	• **Potential to replace traditional intermediaries (trusted third parties) with the collective verification of the network** • **Every transaction is visible to anyone with access to the system** • **Enables global business transactions with less friction and more trust**	• **Cost savings** • **Increased efficiency, transparency, and traceability** • **Increased security and speed**

Anatomy of Blockchain Application

The general architecture and anatomy of a Blockchain application can be viewed as a 3-tier system:

Bottom Layer

- Contains **nodes** arranged in **Peer-to-Peer (P2P) network architecture**
- E.g., **Use of server virtualization**, environment **containerization**, **PKIs,** etc.

Middle Layer

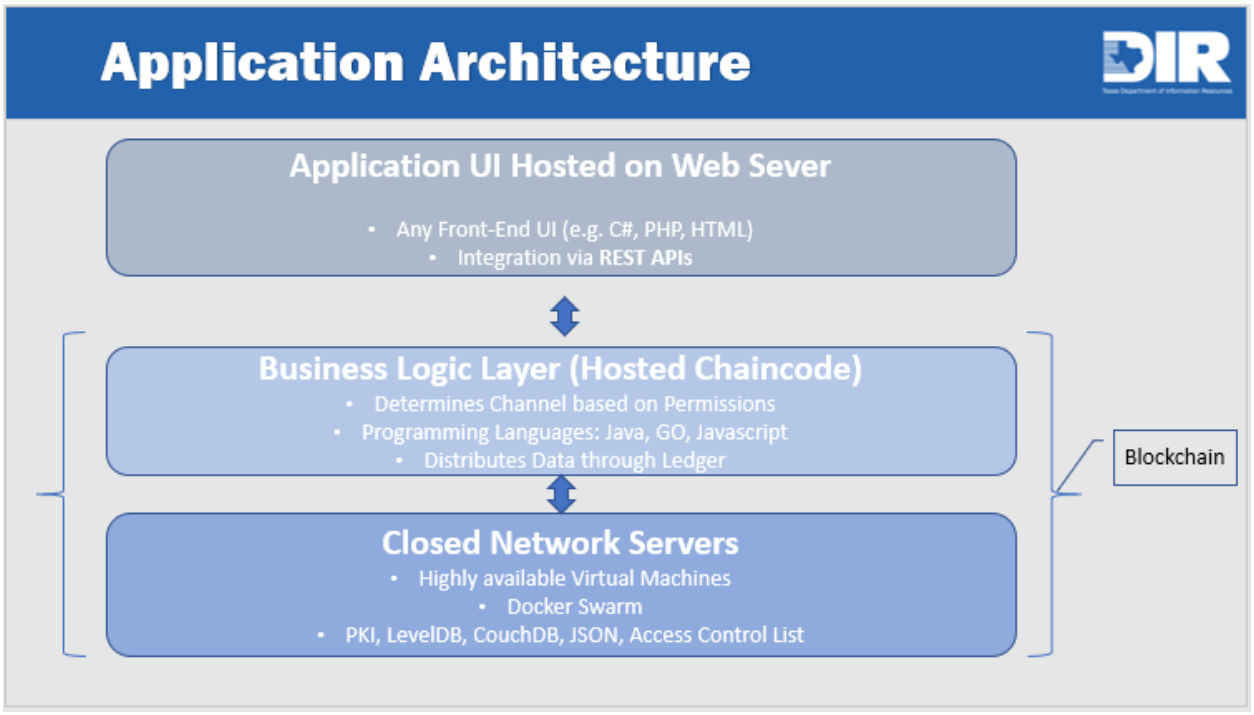
- Composed of: **participants, assets, transactions, and events.**
- **Automation of business logic/rules to create "smart contracts"**
- Access to this layer controlled by **REST APIs**

Top Layer

- User interface, built using standard programming languages, e.g., **HTML**, **C#**, **PHP**, etc.
- This layer communicates with the Blockchain via **REST APIs**

- Note: Most breaches to date have occurred at this level

The following diagram illustrates the 3 layers of a Blockchain solution.



Execution

DIR completed the blockchain POC on an open schedule using an entirely internal team. DIR also accessed free hands-on seminars and educational materials provided by IBM Austin, which was instrumental in ensuring the project benefited from the latest knowledge in this rapidly changing field.

To start the project, DIR assembled a cross-functional team comprising representatives from the agency's technical and business divisions, with three key objectives:

1. **Evaluate blockchain technology in state government context** – Consistent with DIR's mission as an agency
2. **Provide professional development opportunity for DIR employees –** As a training investment in DIR resources to remain current with new technologies
3. **Share lessons learned with DIR customers and the broader technology community –** As part of DIR's Mission, DIR contributes to sharing lessons learned with their Customers and the Technical Community in general.

Use Case

The following factors were crucial to ensure the POC addressed business needs:

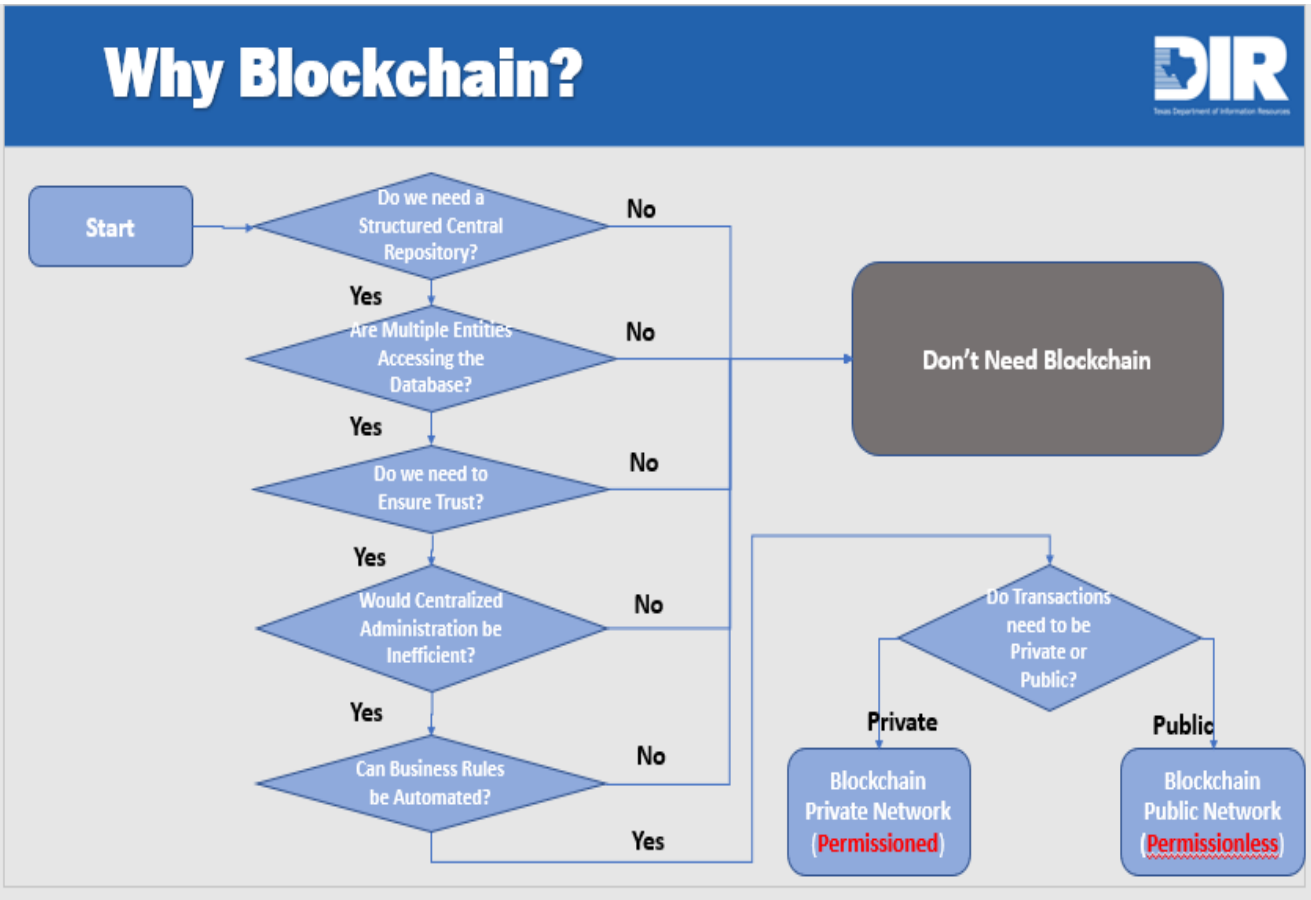
1. **Executive Level Sponsorship** – The agency's Chief Information Officer (CIO) and Information Resources Manager (IRM) initiated, and sponsored the project, which was instrumental in maintaining momentum.
2. **Multi-Divisional Project** – The project was highly collaborative, leveraging resources across the agency, including: IT Services; Communications Technology Services; Data Center Services; Technology Policy, Planning, and Governance; Enterprise Services; and a host of subject matter experts and advisors who contributed throughout the software development lifecycle.

DIR selected an **Asset Tracker Solution** for the POC. DIR's Information Security Team recently launched a new security remediation service for its customers. This new service is based on the sharing of information security training material (seats), which is made available to DIR customers per recommendations from security assessments also provided by DIR. DIR has a pool of 50 seats which are assigned to customers on a 90-day rotation.

DIR's Asset Tracker Solution leverages Blockchain technology to authorize and track the assignment of these virtual assets (i.e., information security training seats). DIR's Blockchain solution is a private network (permissioned membership) based on the **Hyperledger Fabric** development platform.

POC Results

Blockchain Decision Model



As organizations start to leverage blockchain for business applications, they can benefit from exploring simple use cases that offer an opportunity both to evaluate the technology and to better understand the boundaries and limitations of the technology. Having a decision model to assist the use-case selection process saves time and helps teams focus efforts on use cases that provide the greatest value to the organization.

DIR's Blockchain decision model follows a standard template and reflects the results of internal discussions with the DIR POC team. It centers on five simple questions to evaluate the use-case as a candidate to benefit from a blockchain platform. The decision model should be guided by business needs and constraints. Use cases will vary in risk, complexity, and cost.

DIR Blockchain Decision / Considerations Model

Blockchain Technology	• There is a need for a structured central repository • There are multiple entities accessing the database • There is a need to ensure trust • Centralized administration would be inefficient • Business rules can be automated **--> Potential to benefit from leveraging Blockchain**
Network Configuration	• Limited number of known participants • There is a need to have more control over membership assignments • Tolerance for risks is low (e.g., initial proof of concept) **--> Select a private network configuration (Permissioned)** • Participants are unknown and anonymous • Use case supports an infinite number of participants **--> Select a public network configuration (Permissionless)**
Popular Development Platforms	• Financial applications with cryptocurrencies, coins, and tokens • Transaction validation based on mining consensus algorithms (e.g., proof of work) as incentive for peers to validate transactions. --> Use **Ethereum**, a platform similar to Bitcoin that runs smart contracts on a custom-built Blockchain; this is designed as a consortium with greater focus on open source public networks and governance • Traditional transaction processing solution • All peers need to validate all transactions but not every peer needs to execute the contract. Ethereum leverages endorsement policies to define which peers should execute which transactions. --> Use **Hyperledger Fabric**, which supports the use of one or more networks, each managing different assets, agreements and transactions between different sets of member nodes; This is an open source consortium under the Linux Foundation targeting private enterprise Blockchains
DLT Features to Exploit	• **Smart Contracts** – replaces traditional intermediaries (administrators, lawyers, brokers, and bankers) via automation of business logic • **Guaranteed Traceability** – creates ledger stored across all Nodes and Records cannot be altered retroactively • **Improved Security** – uses peer-to-peer network architecture with no centralized authority; eliminates single point of failure scenario prevalent in centralized networks; transactions are validated by all nodes on the network

Popular Use Cases	• **Financial**
	  • Streamline and automate traditional manual workflows
	• **Health care**
	  • Improve access to medical records
	  • Ensure patience privacy
	• **Government**
	  • Improve visibility and transparency in budgets and spending

	• Identity management

DIR Blockchain POC Recommendations

DIR provides the following recommendations for teams looking to create a Blockchain POC:

1. Ensure use-case is a good **DLT candidate** (**leverage a decision model**)
2. Select the right **development platform (**e.g., Ethereum – suited for financial applications with coins and tokens; **Hyperledger** – suited for general transaction processing**)**
3. Select appropriate **network configuration** (**private** vs public, number of physical sites, number of nodes, etc.)
4. Include **business representation**. Don't make this an IT-only project.
5. Choose a **simple use case** to allow your team to balance all pertinent project factors: **risk**, **complexity**, **budget**, **schedule**, etc.
6. Identify key **Blockchain features** to explore in your POC (e.g.**, smart contracts, trust factor, unchangeable ledger**)
7. Develop **smart contracts** by focusing discussions around **participants**, **assets**, **transactions**, **and events**.
8. Keep it simple!

Conclusions

The DIR Blockchain POC provides insight into how Blockchain might create efficiencies and other benefits. Those benefits include:

Network protections – A Blockchain network is based on a P2P network architecture that is decentralized, distributed, and composed of two or more nodes. Blockchain networks leverage several nodes to provide superior redundancy and fault tolerance over traditional centralized database architecture. Early results from our POC proved that we can instantiate several nodes from each virtual machine to provide adequate network protection. Because Blockchain is a parallel processing system, adding more nodes to the network will improve the network security stance, but will not necessarily improve network processing performance as transactions will be executed concurrently.

Data protections – Blockchain employs cryptography as an encryption tool to protect data stored on the network. To ensure data validity, all transactions are validated by all the nodes on the network as a mechanism to prevent the insertion of corrupted data into network. Additionally, once the network validates a transaction it is assigned a unique transaction ID which is linked to previous related data blocks; hence, the "chain." This linking or chaining of transaction IDs provides increased visibility into the lineage of all records stored. Through this POC, we can appreciate that these measures, coupled with the storing of the ledger across all

nodes and the prevention of altering records retroactively will increase data protection over mechanisms prevalent in traditional database technologies.

Cost savings – the following areas, if leveraged properly, could yield efficiencies that translate into cost savings:

- **Smart contracts** – Automation of business rules embedded in the Blockchain
- **Channels** – Allows efficient usage of Blockchain networks by logically partitioning a single Blockchain network to support multiple applications.

Appendix

Glossary of Terms

Ledger	An append-only record store, where records are immutable and may hold more general information than financial records.
Node	Any computer that connects to the Blockchain network.
Token	A digital identity for something that can be owned.
Membership Services	Membership Services authenticates, authorizes, and manages identities on a permissioned Blockchain network. The membership services code that runs in peers and orderers both authenticates and authorizes Blockchain operations. It is a PKI-based implementation of the Membership Services Provider (MSP) abstraction.
Word state	Also known as the "current state", the world state is a component of the Hyperledger Fabric Ledger. The world state represents the latest values for all keys included in the chain transaction log
Smart contracts	A smart contract is code – invoked by a client application external to the **blockchain** network – that manages access and modifications to a set of key-value pairs in the World State. In Hyperledger Fabric, smart contracts are referred to as chaincode. Smart contract chaincode is installed onto peer nodes and instantiated to one or more channels.
Cryptocurrency	A form of digital currency based on mathematics, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Furthermore, cryptocurrencies operate independently of a central bank.
Endorsement Policy	Defines the peer nodes on a channel that must execute transactions attached to a specific chaincode application, and the required combination of responses (endorsements). A policy could require that a transaction be endorsed by a minimum number of endorsing peers, a minimum percentage of endorsing peers, or by all endorsing peers that are assigned to a specific chaincode application
Distributed Ledger Technology	A system, most commonly a **Blockchain**, for creating a shared, cryptographically secured database.
Consensus protocol	A process, encoded in software, by which computers in a network, called **nodes**, reach an agreement about a set of data.
Mining	The process by which **nodes** in Bitcoin, Ethereum, and many other **Blockchain** systems (those that use the **consensus protocol** known as **proof of work**) add new **blocks** to their respective chains and generate new **crypto-tokens**.
Permissioned Blockchain	A shared database with a **Blockchain** structure that requires participants to obtain permission before reading or writing to the

	chain. Contrast this with **permissionless** blockchains, which anyone can join.
Permissionless Blockchain	Public network, where anyone is allowed to join
Proof of Work (POW)	The **consensus protocol** of choice for Bitcoin and many other **cryptocurrencies**. To add a new block, miners must calculate a **hash** for it that meets certain narrow criteria. Doing so requires an enormous number of random guesses, making it a costly process that deters attempts to commit fraud.
Smart Contract	A computer program stored in a **blockchain** that automatically moves digital assets between accounts if conditions encoded in the program are met. It serves as a way to create a mathematically guaranteed promise between two parties.
Peer-to-peer	Refers to the decentralized interactions that happen between at least two parties in a highly interconnected network. P2P participants deal directly with each other through a single mediation point.

References

https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b
https://medium.com/kokster/hyperledger-fabric-endorsing-transactions-3c1b7251a709
https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/
https://www.ca.com/us/why-ca/mainframe/blockchain.html
https://hyperledger-fabric.readthedocs.io/en/release-1.2/glossary.html
https://www.technologyreview.com/s/610885/a-glossary-of-blockchain-jargon/
https://hackernoon.com/blockchain-dictionary-f4d098c9ef89
https://www.grantthornton.global/globalassets/1.-member-firms/global/insights/blockchain-hub/blockchain-glossary.pdf