STONEBLOCK

The Future of e-Government is Now

Blockchain Assessment Framework

Introduction

Blockchain or distributed ledger technology (DLT) is nothing short of a revolution, rivalling perhaps the revolution of Internet itself. Blockchain technology brings together for the first time a number of concepts, data structures, and computing algorithms, to solve long-standing problems in the field of economics and computer science.

In the same way that the Internet was touted as the technology that would fix all of societies ails back in the mid-1990's, the blockchain, too, has been sensationalised and mistakenly represented as a replacement for centralised databases.

This document provides a clear and concise framework consisting eight key questions to ask to establish whether a use case can be resolved by the application of blockchain technology.

Innovations in Blockchain

Specifically, DLT consists of four new and innovative capabilities, from the fields of economics and computer science which make it substantially different from a database. These capabilities must be understood in order to make sense of the blockchain assessment framework of questions used to sort out sensible use cases for the application of DLT from those use cases that are best implemented using well-known and established e-government architecture, secure federated databases and interoperability and data exchange middleware.

First, distributed ledger technology uses peer-to-peer networking to replicate a number of internal data structures which represent the distributed but shared ledger. The peer-to-peer networking is a service that is overlaid on standard Internet protocols. The protocol can be thought of as similar to the peer-to-peer networking protocol used in the Bittorrent application, used for peer-to-peer file sharing and distribution.

Second, most blockchain protocols depend on a computer scientific method to validate the history of a transaction in the ledger, called the Merkle Proof. The Merkle Proof is used to validate transactions in the ledger, in particular to ensure that a party in a cryptocurrency transaction had the appropriate balance of cryptocurrency to spend in a transaction being validated. The method provides a fast way to verify that an entry in the ledger is valid even if the ledger grows tremendously large.

Third, the most widely adopted blockchain protocols use a trivial (but effective) computational problem - solving the problem is called a "proof of work" - which is to find a solution to a one-way hashing function by 'brute force'. By proving that this work was done it implicitly signals a user's interest in preserving the integrity of the peer-to-peer network. The user is rewarded for this work and the output of the work is used so others in the network can see that it took place. The time it takes to solve the problem also provides peers in network with enough time to notice a malicious users attempt to double-spend.

Fourth, and finally, almost all DLT protocols uses asymmetric key cryptography to generate unique addresses from private keys. Addresses are used to send and receive transactions on the distributed ledger.

The Problem

The blockchain assessment framework provides a systematic method for determining if a use case is best solved by the application of distributed ledger technology. Neocapita suggests that the effect of the four features of blockchain technology (as listed above), gives rise to the following questions, the answers to which will determine whether or not a use case makes sense to move to a blockchain.

The Assessment Framework

1. Is it necessary to share data across multiple agencies and/or locations?
While it is common for a federation of databases and the accompanying interoperability and data exchange middleware to be used to exchange data across the firewall, there is considerable time and resources needed to implement this inter-organisation infrastructure. Often in the case of blockchain technology, a simple wallet application is sufficient to read from and write to the universal blockchain, providing a more time and cost efficient way to share data across organisational boundaries.

2. Is there a need for multiple writers to the database?
While a database management system can obviously cope with multiple writers to the database, blockchain technology can be implemented in a way that places identity and permissions associated with that identity at a lower level, inside the wallet application, and so are much harder to circumvent and use to compromise the data.

A database management system however depends on the database administrator and the chain of trust established in the organisation, in order to manage identities and accounts that are used write to the database in a trustworthy manner - but there are many instances where this degree of trust has been misplaced. A blockchain application can embody the rules for writing to the blockchain in code and no administrator is manage access control to the data.

3. Is there inherent or natural mistrust between writers/readers to the database?
If there is mistrust between parties who write to a shared database, there are implications for the assurance that can be asserted about the integrity of the data parties write. Multiple copies of the shared ledger in a blockchain ecosystem and a consensus mechanism overcomes inherent mistrust between writers.

4. Is it more efficient to avoid an intermediating stakeholder?
Is the database being implemented to provide a source of trust and therefore acting as an intermediary that would be otherwise unnecessary if counterparties trusted each other?

5. Are transactions linked to each other or do they have a natural relationship with each other chronologically?
In a database, transactions or rows are not naturally and logically connected to others. There are no innate dependencies between rows. If application data has this characteristic then a distributed ledger may be better suited.

6. Are there identifiable and consistent business rules that apply for a transaction to be considered valid in the database?
The software that runs on a computer in order to participate in the distributed ledger ecosystem is often referred to as wallet software or node software. One cannot "see" the distributed ledger unless there is a piece of software running and through which local copy of the ledger can be interacted with. The business rules for what constitutes a valid transaction is defined in the node software. When the node software participates in the health of the network by validating transactions, it applies a set of business rules that define how the ecosystem works in a consistent way. If the transactions to be stored in the application possess this quality, then a distributed ledger may provide greater assurance that data in the ledger is consistent with the business rules.

7. Is there a subset of ecosystem stakeholders that can be considered "validators" – i.e. more authoritative than other stakeholders?
In the case that validation can be distributed to multiple points on the network, as opposed to a single point, then distributed ledger technology may better suit the use case. If doing so increases the throughput of the ecosystem as a whole, then again, use of a distributed ledger may be more effective and lower cost overall.

8. Is there a unique real world "asset" or "document" or "entity" represented by valid transactions in the database?
Finally, if there exists a unique real world "thing" corresponding to the entities in your use case and if these things were countable and valuable, it may make more sense to use a distributed ledger. After all, this is the reason DLT first invented to provide a global ledger for accounting of transactions in digital cash.

Conclusion

Neocapita developed the blockchain assessment framework to standardise and systematise a method to determine the suitability of distributed ledger technology to the use cases it encountered, and in particular, to determine the suitability of its Stoneblock distributed ledger application to manage 'documents of value' born from government-to-citizen transactions.

Contact Us

Neocapita is a privately--owned firm incorporated in Estonia with offices in Vienna, Austria and Bucharest, Romania. Connect with us via email: info@neocapita.com, to learn more about Stoneblock and to arrange a demonstration.

Visit us on the web: neocapita.com.

NEOCAPITA