DATA PRIVACY PHILIPPINES

Blockchain and Government Efficiency

By Disini & Disini Law Office – November 5, 2021

https://www.privacy.com.ph/blockchain-and-government-efficiency/

It is no secret that the Philippine bureaucracy is inefficient. This is shown by the long line of driver's license applicants in the Land Transportation Office (LTO) in East Avenue. Up to now, the LTO still employs personnel to manually input applicants' personal details into the computer, charging generously for this menial and non-essential task. This is the kind of inefficiency that plagues most government agencies which can ultimately be traced to the lack of automation even for simple processes.

In addition, government services in the Philippines also suffer from a lack of systematization and coordination, especially in handling of data. A phone call to a government office for a simple request for information would see one having to talk to ten different government agencies in seriatim, with each one referring you to another department more obscure than the last. Each office also has different methods of tracking and tracing documents, some employing more effective systems than others. Individual agencies tend to build their data in unprotected, but non-transparent silos, quite open to data breaches but closed off to the discerning public.

These recurring issues in the handling of critical data – insufficient security, lack of transparency and integrity, and the non-sharing of data between government agencies – are easily addressed by blockchain technology. Blockchain technology allows digital information to be distributed but not copied. It is comprised of data records, or "blocks".[i] This means each individual piece of data can only have one owner while being stored in a public database. The information is constantly reconciled and stored in multiple locations and updated instantly. The records are public and verifiable, and since there is no central location, it is more difficult to hack. Moreover, once the "blocks" of data records are collected in a chain, they cannot be changed or deleted by a single actor; instead they are verified and managed using automation and shared governance protocols.[ii]

A key-feature of blockchain-based technology is transparency through decentralization wherein participating parties are able to see and verify data. Transactions are recorded chronologically, forming an immutable chain and allowing for the full traceability of every transaction. Hence, the recurring issue of lack of government transparency is effectively managed by providing a sufficient "digital trail" to identify illicit or fraudulent activity.[iii] In addition, by leveraging a shared and distributed database of ledgers, the need for intermediaries is eliminated.[iv] This reduction in red-tape and discretion strengthens the integrity of government services and data management.

This level of transparency is balanced by the security provided by the blockchain. Nowadays, criminals can easily gain access to government databases and steal or manipulate records due to the low level of security or encryption that the government employs in protecting critical data. Oftentimes this data is not digital, hence a simple photocopying of records will leave one vulnerable to identity theft or fraud. To address this type of security issue, the nation of Estonia for example, is rolling out a technology called *Keyless Signature Infrastructure* (KSI) to safeguard all public-sector data. KSI creates hash values, which is akin to fingerprints for files. The contents of a file (which may or may not contain large amounts of data) is processed using an algorithm and a unique numerical value – the hash value – is produced.[v] This hash value can be used to identify records but cannot be used to reconstruct information in the file itself. Multiple hash values (i.e. representing multiple files/ data sets) are then stored in a blockchain and distributed across a private network of government computers.

Whenever an underlying file changes, a new hash value is appended to the chain, and this information can no longer be changed. The history of each record is fully transparent, and unauthorized tampering from within or outside the system can be detected and prevented. KSI allows government officials to monitor changes within various databases—who changes a record, what changes were implemented, and when they were made. The electronic health records of all Estonian citizens are managed using KSI technology, and the country is planning to make KSI available to all government agencies and private-sector companies in the country.[vi]

The problem of redundancy and disorganization is also solved whereby the blockchain serves as an "online ledger" where data can be verified and reconciled.[vii] Governments could create central repositories or enterprise systems using blockchain technology for sharing information across agencies. Of course, not all of these data are accessible by the whole world. What is needed is an environment where data can easily be accessed across systems but at the same time, individuals and organizations can take back ownership of their data and control the flow of personal information. Emerging blockchain technology may support such a scenario. Each person or organization would have all relevant data about them (basic personal information, for instance, or records of previous interactions with government agencies) stored in a dedicated ledger within an encrypted blockchain database. Individuals or companies could access these ledgers through the Internet. End users could then give government agencies the authority to read or change specific elements of their individual ledger using public- and private-key cryptography.[viii] India[ix] for example, is upgrading their National Unique Digital Identity system (called "Aadhaar), a system that generates a single digital identity for its citizens (consolidating all relevant information across all involved agencies), using biometric technology and blockchain.

While the Philippines has experienced an incredible increase in internet foot traffic since 2000, researches from the Philippine Institute for Development Studies (PIDS) still noted a relatively weak uptake of ICT services in our country.[x] Thus, it is no surprise that though we are dubbed as the social media capital of the world[xi], the Philippine ICT environment remains significantly below international standards.[xii] On a positive note however, this means that there is a potential for improvement, especially considering the speedy developments happening in blockchain technology.

A promising application of blockchain technology in the Philippines would be automating and tracking high-risk transactions, such as public contracts, cash transfers, and aid funds. Government payment systems and cash transfers are particularly vulnerable to corruption. They have multiple points of human discretion that make them vulnerable to fraud and falsification and create opportunities for bribery. Limiting the physical interaction between citizens and officials will reduce opportunities for rent-seeking. Moreover, many governments distribute benefits without appropriate controls or verification mechanisms, hence, falsified claims by recipients are not uncommon. Conditional cash transfers and aid flows are such examples. In Jordan, the UN World Food Program recently conducted a pilot project using blockchain to manage cash-based transfers to Syrian refugees to increase transparency, eliminate leakages, and reduce transfer costs.[xiii] The same could be done to the Conditional Cash Transfer (CCT) being implemented in our country.

Technology solutions should first be implemented to provide end-to-end transparency in government payment systems, allowing one to detect red flags, fraud and malversation. Blockchains only add value to an already technology-driven system and can do little for systems that have yet to be digitized.

It appears that the main problem in implementing blockchain solutions in the Philippines lies in the fact that blockchains only strengthen already existing institutions[xiv]. This means that if the current institutions are inherently faulty, corrupted or primitive, adding on a blockchain system to digitize the same will not help solve problems in inefficiency. In fact, it may even aggravate the same. This suggests that the value of introducing blockchain in any weak government system is questionable. Resources may be better spent in fixing and strengthening institutions instead.[xv]