TMT KNOWLEDGE

DATA PROTECTION AND THE BLOCKCHAIN TECHNOLOGY

KAA
KAMPALA ASSOCIATED ADVOCATES
Celebrating 20 Years

Data protection and the Blockchain technology: Is a centralised legal framework adequate for a decentralised Technology.

One of the most talked about technologies in today's mainstream media within the context of the fourth industrial revolution is the blockchain technology and many of its applications. In simple terms, Blockchain is a distributed ledger of transactions. All the transactions in the blockchain are encrypted and synchronized between the participants. In this blockchain technology, members of a blockchain network are called Nodes. Each node has the copy of the full ledger and use Peer to Peer Network for synchronization. By design, blockchain eliminates the need for a Centralized Authority to validate transactions by performing peer validations before any transactions

The value of blockchain stems from its ability to among others share data in a fast, cheap, secure way among entities -- without any one entity having to take responsibility for safeguarding the data or facilitating the transactions.

As with every technology, there are both advantages (some of which are mentioned above) and disadvantages that come with the innovation. Some of these disadvantages however are short term in nature and can be remedied through the continuous innovation and refinement that can be embedded with further technological improvements. In the short term however, technology being inherently, a disruptor of the prevailing legal, social and technological status quo, will always be viewed in some circles with a lot of fear and apprehension.

One of the areas in which the blockchain technology has upended its very foundational basis and relevance is data protection law. In Uganda for example, the Data Protection & Privacy Act contains a set of principles that Organisations, government and businesses have to adhere to in order to keep someone's data accurate, safe, secure and lawful.

Whereas blockchain technology is in principle designed to create an unalterable record of transactions with end-to-end encryption, which shuts out fraud and unauthorized activity and whereas blockchain can additionally address privacy concerns better than traditional computer systems by anonymizing data and requiring permissions to limit access; the very foundational basis for blockchain technology in many ways runs contrary to the policy and statutory set-up of data protection law principles and as such renders the current legislative framework both outdated and untenable within the context of blockchain technology for the time being.

Analyzing blockchain technology and some data protection principles

One of the ways in which the Data Protection and Privacy Act, though not an old statute, technologically outdated, is that it's entire framework is based on the notion of "centralization" while the blockchain technology is based on a "decentralized" architecture. In this "centralized" framework, the presumption is that the data controller possesses full and ultimate responsibility over data processing and storage, with any data processor under the controller's full control.

On the other hand however, blockchain by design eliminates the need for a Centralized Authority and is based on a "Decentralized" Distributed Ledger.

According to Wikipedia "A distributed ledger is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage."

To this end, the key foundational framework embedded within the law for the identification, registration and regulation of a data controller becomes impracticable if not impossible task and legal requirement particularly with public and unpermissioned blockchains. This is furthermore worsened by the fact that the nodes are normally located in different countries with varying levels of data protection legislations. This in itself upsets the jurisdictional set up of data protection legislation which is framed on the basis of territorial data collection, control and transfers.

The second issue is that data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Blockchain technology on the other has no option for any time bound processing of data. Once data is added onto the blockchain, it remains a part of it in perpetuity. This therefore runs contrary to the principles on storage limitation.

The third and related issue is relation to the exercise of the 'right to be forgotten'. The 'right to be forgotten' is the right to have private information about a person be removed from Internet searches and other directories under some circumstances. As already mentioned, transactions, once recorded on the blockchain, can't be changed or deleted. On the blockchain, all transactions are time stamped and date-stamped, so there's a permanent record. This character of the blockchain technology therefore renders the enjoyment of this right to be forgotten almost impossible especially in the absence of a centralized data controller through whom data requests can be made.

Is data protection & privacy a lost ideal with blockchain technology?

It is easy to generally claim that the aspirations of the Data Protection and Privacy Act are at odds with the foundational framework and workings of blockchain technology until you look at the underlying principles which ultimately show that the two are not mutually exclusive as far as ideals are concerned. It is only the paths used that remain at odds.

While the traditional businesses have generally used and collected key personal data such as names, addresses, emails, phone numbers, age, bank and credit card details for their business objectives, blockchain enables an unprecedented amount of individual control over one's own digital data. Individuals and individual organizations can decide what pieces of their digital data they want to share and with whom and for how long, with limits enforced by blockchain-enabled smart contracts. This boosts privacy for the individuals.

Secondly, blockchain uses cryptography to make all the transactions/ data extremely safe and secure. Cryptography is used for obfuscating (encrypting and decrypting) data. Very often, there are certainly potential problems with storing pseudonimysed personal data in a blockchain, however one should be looking at the particular circumstances: which source-data is pseudonimised, encrypted or hashed, where is it stored, and can it be related to other on-chain events, what happens if you delete the source-data, and how strong is the entropy?

To find solutions for this challenge, it is important to consider both the technical and the legal aspects, and seek for a balancing act between the need to protect the rights of individuals and also enabling technological innovation and advancement. One way through which this balancing can be done is by implementing Privacy by Design: ensuring all privacy controls are implemented right from the start, and making sure products, protocols and their apps and User Experience (UX) are designed in a privacy friendly way.

Author

Augustine Obilil Idoot
Partner
aidoot@kaa.co.ug

Caveat

The contents of this article are intended to convey general information only and not to provide legal advice or opinions. The contents of this website, and the posting and viewing of the information on this website, should not be construed as, and should not be relied upon for legal advice in any particular circumstance or fact situation. An Advocate/ attorney should be contacted for advice on specific factual legal issues.

Celebrating 20 Years