REGULATION (SECURITY) vs DECENTRALISATION (PRIVACY): THE CRYPTO CONUNDRUM

MAY 2023

BLOCKCHAIN AND CRYPTOASSET (K) LTD.

Authored by: Patrick Kiragu Mwangi *BA, BSc., MA*

'Ultimately, in objectively accessing the benefits of a decentralised system, it is imperative to understand the privacy implications of decentralised architectures and whether the privacy gains resulting from decentralised coordination are greater than the privacy costs emanating from the disclosure of metadata that may involve revealing personal information and breaching existing data privacy laws.'

INTRODUCTION

Blockchain is a technology that enables the secure validation, recording, and sharing of data. Rather than storage in a centralised database controlled by a single entity, the data is stored within a distributed network database with multiple copies of that database continuously being updated in real time across the network of participants. Not only does this eliminate one single point of failure risk, but it also makes tampering with the data a significantly more onerous task. An intrusion would need to tamper with all copies of the data near simultaneously in order to invalidate the network.

As this technology gathers pace and the use and investment in cryptoassets built on this technology grows to match this pace, the need for regulation by both governments and industry becomes imperative. The combination of the rapid growth of the crypto market—valued at its most recent height at roughly $2.9 trillion in November 2021-, continued private sector initiatives at developing new crypto projects and world-wide governmental efforts to launch Central Bank Digital Currencies (CBDCs) have all helped galvanize governments to attempt to act on industry regulation. A further impetus for regulation is the threat of nefarious actors taking advantage of the decentralised nature of the technology to commit crime- money laundering, evading tax and financing terrorist acts, thereby creating the need to align regulation of this nascent technology with existing AML/ KYC laws.

Critically though, the ethos behind the development of blockchain technology was a move away from centralised control by building a decentralised network that allowed for peer-to-peer engagement away from the watchful gaze of governments and their proxies. This was thought to be a step in the right direction in enhancing user-privacy and allowing innovators the space within which to advance technology. A conflict, therefore, inevitably emerges between those who wish to engage in initiatives that move away from centralised power by allowing individuals to interact directly without a controlling centre while at the same time enhancing user-privacy, on the one hand, and a system that is both centralised and regulated on the other.

The question to be addressed is, therefore, how much of central-based scrutiny and control to employ through regulation without unduly defeating the whole purpose of decentralisation and user-privacy inherent in the technology. How this will fit in with governments' mandate to protect consumers, promote competition and create safes spaces for technology users is of no lesser significance.

BLOCKCHAIN AND PRIVACY

As the use of blockchain technology continues to gain momentum, data privacy has seen a sharp uptick in global attention with the very nature of the technology raising interesting issues around privacy laws and their application to the technology. Since data breaches have become somewhat prevalent especially with the prominence of online service platforms including e-commerce and social media platforms that collect, aggregate and analyse data, advocates of blockchain technology continue to make the case for its adoption due to its inherent ability to enhance user-privacy, data protection and data ownership.

However, certain blockchain features bring the technology at odds with existing privacy laws. One key feature- immutability in particular, means that data stored on the blockchain cannot be subsequently altered or deleted. This feature, in particular, contravenes EU GDPR rules, for instance, which stipulate that *data subjects retain control over their personal data, including how it is collected and stored, and that persons collecting and storing such data agree to hand over, correct, and delete that data on request*. Other areas that may also be in conflict with the same GDPR are in regards to data minimisation and storage limitation.

The above, notwithstanding, there is an area of convergence between existing GDPR obligations and blockchain technology, namely 'pseudonymisation' as a security measure and risk mitigation technique. With pseudonymity, the identity of the person(s) associated with the action or transaction on the network cannot be (easily) established. This has the effect of promoting, at the very least, data minimisation.

Complete privacy and anonymity, however, are unachievable where a backdoor or a bug in the technology exists that limits even the abilities of the most sophisticated encryption techniques to protect user-identity or privacy. Further, with decentralised systems, the onus remains with the individual user to keep their data private where an operator or exchange is absent. Such data may become compromised through inadvertent disclosure by the user or a leakage through an improper use of a platform or tools.

Ultimately, even with blockchain-based systems that employ encryption technologies, these are only as secure as the ability of users to securely manage their passwords and/ or private keys.

THE POLICY QUESTION

There have been continued calls by industry and market participants, in both the tech and finance space, for legislative clarity or at least guidance from relevant authorities to reconcile data privacy laws with emerging decentralised technologies like blockchain.

From a policy perspective legislators, regulators, and technologists are faced with the difficult task of giving realism to the benefits of regulation without creating a central database that irreversibly connects all persons to all of their transactions thereby heavily impinging on individual privacy. While it is possible to benefit from a decentralised system like blockchain that conducts processes electronically without revealing data about the transacting parties, questions remain relating not only to how to reconcile the different perspectives on anonymity and pseudonymity and how they affect the applicability of various data protection and privacy laws, but also how to reconcile transaction immutability and data preservation in blockchain applications with individual rights.

THE MISCONCEPTION

Contrary to popular narrative, bitcoin and other cryptoassets do not provide a high degree of anonymity or privacy. Bitcoin is pseudonymous, meaning transactions are linked to the user wallet address rather than the name, hence making transactional records viewable by the public. In fact, the more wallet addresses are used, the more the information that can be inferred from these addresses. Crypto forensic and analytics companies (like Chainalsyis, Elliptic, and CipherTrace) also exist that are able to attach identities to illicit transactions making the blockchain network not as private as it is made out to be.

As a result, and where the intention for establishing decentralized architectures like blockchain is to protect user privacy and provide data sovereignty against the ubiquitous surveillance of states and corporations, such infrastructures might turn out to be just as vulnerable to governmental or corporate surveillance as their centralised counterparts. Data mining techniques applied to the analysis of public blockchain transactions could be just as intrusive as standard surveillance techniques on centralised platforms. This is an irremovable contradiction of the public ledger design that the blockchain requires for its very existence.

DECENTRALISATION- A MIXED BAG

With the current state of telecommunication technologies, it is becoming harder to communicate on the internet without leaving traces or disclosing information to centralised third parties —be they governmental agencies or private companies. When carrying out transactions, users put trust in these parties' ability to hold their transaction data securely and execute transactions. However, with such centralised structures, these not only constitute a single point of failure but large amounts of such data are prone to security risks where the authority's system may be hacked or mishandled or data lost or stolen.

Blockchain technology aims to remove this reliance on central authority (and hence a single point of failure) through encryption and by enabling nodes or devices within the blockchain network to confirm the validity of a transaction rather than a central or an external third party doing so. Further, this set-up also helps to preserve privacy and confidentiality while also contributing to the promise of libertarianism to further individual freedoms and greater end-user autonomy.

Network transparency that comes with decentralised systems also enables users to collectively verify the legitimacy of every network transaction while also ensuring the users' fundamental right to privacy is protected. As such, the more decentralised an infrastructure is, the less it relies on trust and the more transparency within that system becomes indispensable.

Network transparency is, however, not without danger as it allows for third party analysis of data which is publicly disclosed on the network meaning that decentralised infrastructures - designed to promote privacy and autonomy- can actually end up being just as vulnerable to governmental agencies or corporate scrutiny as their centralised counterparts. Such openness and transparency of a decentralised network can also make information more vulnerable to nefarious third-party grab.

Decentralised systems, therefore, present a mixed bag. On the one hand, they reduce the dependency on centralised service providers while improving the ability for users to protect their own data from nefarious actors. On the other hand, however, the degree of transparency necessary for a decentralised system to function requires disclosure of significant amounts of metadata to be made available to the overall network. Further, the lack of a formalised hierarchical structure within a decentralised network, means that power may consolidate into unofficial clusters where it becomes difficult to establish who is actually in control.

Ultimately, in objectively accessing the benefits of a decentralised system, it is imperative to understand the privacy implications of decentralised architectures and whether the privacy gains resulting from decentralised coordination are greater than the privacy costs emanating from the disclosure of metadata that may involve revealing personal information and breaching existing data privacy laws.

DANGERS OF SILO-TYPE REGULATION

Regulation is key in ensuring that the corporate structure, governance, internal controls and record-keeping of organisations are well-organised and do not impinge on the interests of customers or clients. However, in an interconnected world, such regulation needs to be structured in a manner that overcomes the confines of jurisdiction for it to have true meaning.

Factoring in the reality that any enacted regulation relating to blockchain technology and its 'derivatives' like cryptoassets will have to work in harmony with existing data privacy laws, it is more than worthwhile to take a look at the structure of existing data protection legislation.

The EU takes an expansive and omnibus approach with its GDPR which seeks to protect EU residents against less stringent data protection standards in other countries while allowing member states to make only minor derogations. By contrast, the US approaches data privacy in a patchwork, sector-specific fashion at the federal level. The UK, for its part, has chosen a more pragmatic approach that puts more reasonable burdens on organisations to protect individuals' privacy, rather than placing the onus on consumers to exercise their privacy rights. Similarly, data protection reform conversations in Australia, Canada and Asia continue to avoid imitating GDPR and instead lean towards accountability principles embodied in the UK model.

This silo-type legislation that sees various jurisdiction opting to handle data privacy with varying levels of accountability and scrutiny will in all likelihood feed into any legislative initiatives aimed at housing blockchain technology and the cryptoassets built on this technology.

Evaluating jurisdiction and applying regulations to decentralised blockchain implementations is, therefore, not a straightforward exercise. In particular, the distributed nature of blockchain technology not only poses a challenge regarding the applicability of various jurisdictions' laws, but it also raises tensions with those that restrict cross-border data transfers.

With this in mind, it will be some time before we see universal rules on how to treat and manage blockchain and cryptoassets across the various jurisdictions if current application of privacy laws is anything to go by. This notwithstanding, the fact that nearly all global jurisdictions read from the same hymn sheet in regards to AML/ KYC legislation, is a positive sign.

THE CONCEPT OF 'CONSENT'

Under existing privacy laws (e.g GDPR), data controllers are required to request consent from their users or data subjects in order to access or store their personal data. This consent must be *freely-given, specific, informed, and unambiguous*. However, even where these privacy requirements on the part of data controllers are met, data subjects can withdraw consent at any time without explanation.

If blockchain technology adherents are to take account of existing privacy laws, they must consider scenarios like consent withdrawal. The fact that blockchains may store personal data in a way that is extremely difficult to remove means that these new technologies may need to depend on a basis other than consent when handling personal data.

THE UPSIDE OF REGULATION

The core reason for any industry regulation is to protect consumers and investors. Within the growing blockchain and cryptoasset space, investors should be able to enjoy the promise of participating in transparent, fair and robust marketplaces with the protections that they would get in conventional finance. If implemented correctly, companies involved in blockchain development would benefit from being able to bring new services to market with regulatory certainty and without being burdened by unnecessary compliance or operational costs.

Linkages between blockchain technology and associated assets, on the one hand, with traditional finance, on the other, are beginning to emerge and these linkages may threaten

financial stability if they are not managed well. Stakeholders in the industry, primarily regulators, must not wait until the point of financial instability for them to develop the frameworks necessary to prevent a crypto shock that could have a much greater destabilising impact. A case in point is the recent FTX collapse which appears to have triggered some level of contagion and negative sentiment in the finance and the crypto industries respectively.

Innovation also benefits from regulation and regulatory clarity in that scale can only best be achieved within a framework that manages risks to existing standards. Regulation would allow for a seamless integration between existing financial infrastructure and new functions in the blockchain and cryptoasset space. As an example, integration or transition to 'smart contracts' (as pioneered in the decentralised finance- defi space) from existing legacy systems would allow for the functions of trading, clearing and settlement of tokenised financial assets to be combined into a single, instantaneous contract rather than being carried out in sequence by three separate institutions over a number of days. This would not only lead to efficiency gains but also help reduce risks associated with time lag.

THE CASE FOR SCRUTINY

Given privacy as a primary motivation for the adoption of blockchain technology, whether to circumvent capital controls or just to avoid the "pastoral gaze" of state or corporate surveillance, regulators continue to view the technology with great suspicion. Further, the pseudonymous nature of crypto wallets means that these are incompatible with the AML/ KYC regimes of most countries, which require financial institutions to track the identities of participants transacting above a certain threshold.

Going forward and as the digital asset market moves closer to mainstream finance, financial institutions handling these assets, directly or indirectly, will therefore want to ensure proper AML/ KYC procedures are in place for both compliance purposes and to avoid unwittingly being used as funnels to move money by bad actors.

THE COMPROMISE

Given the apparent conflict between decentralisation and privacy, on the one hand, and regulation and scrutiny on the other, the most desired outcome may be a framework that is risk-based so that the level of regulation is contingent on the level of risk. Where there's a greater threat of nefarious acts to circumvent the law, stricter regulation and greater scrutiny of specific decentralised applications should be employed to match existing AML/KYC regulations.

Low-risk decentralised applications, say identity verification and authentication, which merely seek to confirm a user's identity, for example, would therefore attract less strict regulation and minimal scrutiny. Such a development, however, would require a collaboration by all industry stakeholders, including the private sector, so that such regulation does not inadvertently stand in the way of innovation.

In addition, to further ensure that the changeover from legacy systems to these new decentralised technology is as seamless as possible, institutional involvement will be key. Although, this at face value appears to defeat the whole purpose behind decentralisation and user-privacy enhancement, lessons learned with traditional legacy infrastructure would be key in ensuring the transition from centralised to decentralised networks is a seamless as possible.

The fear, however, on the part of users especially privacy-minded individuals, would be that the regulated financial institutions that operate the system might secretly collude to compromise the anonymity of their clients.

LAST WORD!

The debate surrounding the arrival of innovative technologies like blockchain and cryptoassets boils down to decentralisation vs regulation or, more precisely, privacy versus security. This debate will only continue to gather momentum as these technologies become ever more mainstream in consumer and commercial settings. Enterprises seeking to maximise opportunities presented by this nascent technology will, however, need to remain abreast of new iterations of the technology as well as evolving data privacy reform and regulations. Failure to do so won't just impact their bottomline, but also have the potential to bring their businesses to a standstill.

Increased regulation may at first appear as halting technological advancement thereby causing negative market sentiment, as it implies there is a need for regulation in the first place. However, in the long run, the uptake in blockchain technology and related assets is likely to increase because there will be more consumer confidence in this technological output and related investments.

As blockchain technology continues to be integrated into various industries, governments will impose regulations to ensure the accountability and transparency of these systems, requiring companies to explain their blockchain decision-making processes and to provide a human review mechanism for certain decisions.

From a policy perspective, as adoption grows, privacy concerns will not altogether disappear. It is, therefore, essential that both policymakers and regulators work with industry experts, private businesses, civil society and academia to develop evidence-based, future-looking strategies to realise the benefits of, and mitigate the risks of, these technologies. Such engagement will also allow the industry to demonstrate to governments and industry watchdogs that blockchain and allied investments are not detrimental to either privacy or AML efforts while at the same time providing regulators the space to allow for innovation.

Blockchain technology then becomes, not an innovation wrought in risk, but rather an opportunity.

This said, the decentralised nature of the technology will continue to feed into doubts as to whether the use of permission-less blockchain can deliver the necessary level of assurance for activities that are integral to the stability of the financial system. Regulators will need to remain open-minded and innovative in thinking to explore whether, and if so, how the necessary level of assurance – equal to that in conventional finance – can be attained.

Predicting the future direction and pace of blockchain and cryptoassets will not be an easy task. Promising technologies can fall by the wayside and unexpected ones can flourish. However, the technologies that have been pioneered and refined in the crypto world, such as encryption, tokenisation, smart contracts, atomic settlement and the like, not only seem unlikely to go away any time soon as the globe digitalises but will rather enhance the potential to improve efficiency, functionality and reduce risk, at the very least, within the financial system. However, technologies are only as good as the rules, programmes and structures which organise their operations. It may well be some time before blockchain and allied assets are deployed at scale and attain the global reach enjoyed by legacy systems.

In concluding, blockchain technology, which seeks to provide users with the ability to access, view and submit transactions with minimal central oversight, must see this benefit balanced with the need for organisations, that adopt it and that have business models built on it, follow consistent data privacy practices and comply with applicable laws and regulations.

Sources

City A.M. (2020) *Privacy laws and blockchain.* London: City A.M.

Forbes (2021) *Crypto Investors Defy Regulatory Uncertainty to Profit*. Jersey City: Forbes

Goodwell, G & Aste, T (2019) *Can Cryptocurrencies Preserve Privacy and Comply with Regulations?* London: Centre for Blockchain Technologies, University College London

Thomson Reuters Practical Law (2022) *Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies*. London: Thomson Reuters (Professional UK) Limited

PYMNTS (2021) *Debate Looms Over Crypto Privacy, Security and Regulation.* [online] Boston: PYMNTS Available from: https://www.pymnts.com/cryptocurrency/2021/debate-over-privacy-security-regulation/

World Economic Forum (2022) *Privacy concerns loom large as governments respond to crypto*. Geneva: World Economic Forum

Disclaimer!

This is a promotional document and as such the views expressed do not constitute investment (or any other) advice nor a recommendation to buy, sell or trade cryptocurrency. Blockchain and CryptoAsset (K) Ltd. does not guarantee its accuracy, completeness or timeliness and as such the information is subject to change.

Past performance is not a guide to future performance.

Investing in cryptocurrencies is inherently risky and could lead to huge or even total monetary loss. Investors should, therefore, only invest money which they can afford to lose.

We accept no liability for any actions taken, or not taken, as a result of the information contained in this material. Reliance upon this information is, therefore, at the sole discretion of the reader.

Any research in this document has been obtained and may have been acted upon by Blockchain and CryptoAsset (K) Ltd. for its own purpose.

May 2023