IIAC ACCVM
Investment Industry Association of Canada Association canadienne du commerce des valeurs mobilières

Cryptographically Enhanced Commerce

The following article is an excerpted compendium of a brief series of articles on cryptographically enhanced commerce, inclusion, CBDCs and regulatory framework authored by Thomas Kalafatis and Richard Nesbitt over 2002 and Spring of 2023.

Thomas Kalafatis is founder and CEO of Aegis Sports Labs

Richard Nesbitt is Chair of The Inclusion Initiative at LSE and former CEO of Toronto Stock Exchange (edited - Thomas Kalafatis, June 15, 2023)

An Introduction - Cryptographically Enhanced Commerce Is Here to Stay and Why

How will cryptographically enhanced commerce ("CEC") improve or compromise organizations and societies? When many of us read articles about crypto currencies we find them mysterious. What are these ideas all about, why do they exist, and what is the end game? No one really knows their future, but there is no question that something is happening that could be very big. We try to map where we are, to demystify some of the controversy, and chart some path of how the environment may evolve.

Firstly, cryptographically enhanced commerce is here to stay. The supply of the technology is too widespread, and its demand too pervasive to be reversed. The owners of crypto-currencies now number in the hundreds of millions. The underlying code, which can be cryptographically protected is now in the "wild". As cryptographic technology inexorably moves forward and is intertwined with other technologies, the best that can be hoped for is for its negative externalities to be kept under a measure of control.

The advent of cryptocurrencies is a natural evolution of the development of the Internet. Web 1.0 was the internet's first wave. It was an open architecture created by public institutions for public use. This resulted in such products that are used universally today such as email and also the HTML language for the purposes of displaying documents on the Internet.

Web 2.0 is a term that can it be applied to the development of commercial applications for the Internet as many commercial requirements around security were not contemplated by the early Internet's open architecture. Over time a public domiciled activity moved to a more private, commercialized and centralized set of activities which was more secure, safe and convenient. The networks created by companies such as Apple, Meta, Google, Amazon and Microsoft that have become proprietary properties of these organizations. They have generated massive profits and wealth for those involved in their development and funding.

Web 3.0 means to many a further set of developments for Internet technology which are moving the pendulum back to a more decentralized environment while maintaining the improvements in safety and security of Web 2.0. It promises a more open and more available architecture using technology such as blockchain as the various rights required for distributed software to function are enabled by distributed programming languages such as Solidity (Ethereum's programming language). Cryptocurrencies are examples of this decentralized creation of technology for financial (store of value) or nonfinancial instruments of exchange (NFT collectibles). Blockchain potentially promises decentralized holding of these instruments as an important characteristic as the value created by the network is owned by users of the network itself.

A critical attribute of money is the need to safely, and securely transport and verify its purpose. From serial numbers, to anti-tampering papers, special inks and technologies, cryptographic techniques are critical in securing our paper money for centuries. Furthermore, our digital representation of money has

also benefited from crypto-graphic techniques. From our ATMS, to trading on the stock exchange, to payments on our mobile phones, encryption keys and technology are critical to providing the convenient portability coupled with security modern commerce demands. Crypto-currencies can to a degree be considered an extension of these crypto-graphic techniques down to the Unit or singular level, but in a decentralized way (no central authority validates the money). (We bundle all of these past, present and future technologies into the concept of Crypto-graphically Enhanced Commerce, as the macro issues are not tied to a particular currency – Bitcoin, or even type of cryptography – Blockchain).

Crypto-currency transaction units can be utilized to exchange stores of value, or to utilize the transaction processing capacity of new networks. Crypto currencies we are now seeing an explosion in the number of transactions. There are millions of developers applying skills in this new space. The next successful social media or cloud services company may well be centred around cryptographically enabled commerce distributing and decentralizing power. From organizations attempting to decentralize cloud services (Filecoin) to social media (Mask Network) no one corporate or government entity controls this evolving Web 3.0 universe and, therefore, is much different than the cloud applications provided by companies like Amazon or Apple.

The world cannot pack it all up and declare cryptocurrency a failed experiment even if it wanted to! In many countries there is strong public demand for alternative currencies instead of their own, given the level of mistrust they have for their governments and banking systems. After all bitcoin still exists at a price greater than zero, meaning many hundreds of thousands of people ascribe a utility value to this instrument.

We suggest that crypto-currency is analogous to a high-utility technology, but with clear negative externalities whose costs (fraud) need to be managed (much like carbon–based energy, which had massive utility, but whose externalities were understood much later).

We believe that ultimately the pursuit of controlling these societal costs will become more aggressive and involve regulating not just the coins themselves but also eventually the very programming code that creates them.

Fraud is Fraud – Regulating the Negative externalities of Decentralized Markets

We have seen that uncontrolled applications with less transparency present greater risk of negative externalities - fraud. More specifically, it can feel as if all of the financial frauds in history are being relearned with cryptographically enhanced commerce. From the “salting” of commodity currency, to theft, kiting, “pump and dump”, and Ponzi schemes, does the world need to “relearn” how to manage through all of these in order to push development of cryptographically enhanced commerce. Is this not some form of deadweight loss to the economy? Or negative externality?

On one hand the new sets of technology offer the possibility of improved inclusion – banking the unbanked:

- Distributed data bases are not under central control of commercial or government entities and can be constructed to spread their benefits to the largest number of people. New products such as Non-Fungible Tokens may create new business models. Both may create value for large groups of people who are currently shut out of the existing mechanisms for getting products to market.
- In societies that have unsophisticated banking systems, poor monetary policy or confiscatory governments, new stores of value may bring millions into a world where they can share the benefits of technological change.

On the other hand, there are forces in our society that will seek to control the future of cryptographically enhanced commerce for their own benefit:

- It is likely that some parties will seek to control these cryptographically enhanced commerce processes. That is the usual way of human development. This is often done for commercial reasons but can also be a way for state sponsors to maintain controls on illicit activities such as money laundering.
- It may be that cryptographically enhanced commerce is as prone to concentration and lack of an inclusiveness as our current systems as a self-re-enforcing loop. Today a small number of people control the vast wealth ("whales") that has been created from crypto activities merely by getting there first. Do we once again rely upon whether these are good actors or bad actors, much like the current market-oriented paradigm, in how they share the benefits with society at large?
- Taxation authorities are often unable to collect revenues from the new industry which means that the burden of public spending falls on a smaller base of those in traditional activities who end up subsidizing their very own displacement from new untaxed industries who benefit from the public commons.
- There may be just as many unpriced negative externalities in the cryptographically enhanced commerce world as there are in the existing world of finance and business. For example, it was recently reported that 8% of the entire electricity consumption of Kazakhstan (Wired, Jan 22, 2022) was being used for mining crypto currencies. Not only is this having a negative effect on carbon dioxide emissions at a time we are trying to reduce these globally it would also imply a use of electricity where the benefits are narrowly shared in that country.
- Regulators are not yet able to fully protect the public as they do not have the laws, technology or geographic footprint to cope with a new borderless industry.

Our proposition above is that the various private forms of cryptocurrencies and cryptographically enhanced commerce raise a number of issues and problems which may in fact be no fairer than the current system of currencies, cash, securities, commodities and financial markets. The pursuit of monopoly power, taxation, or issues with the environment are not as commonly related to crypto-currency as the last item – fraud.

To deal with fraud - Market participants simply need to ask whether crypto-currencies such as FTT (whose insolvency contributed to the downfall of the cryptocurrency exchange FTX) or BNB (which financially supports Binance) are deposits or securities. They are either one or the other to the extent they are exchangeable for other financial instruments. (We understand the argument that certain coins such as BTC can be considered commodities – and we will decipher the distinction in a future article – but for simplicity sake – BTC itself is not exchangeable for services by an "issuer" and was not developed by an organized group of people "in pursuit of profit"; even while profit may have occurred). In either case, they need to be subject to the same regulation as other traditional forms of deposits or securities or the providers of those services are left at a disadvantage. And investors need to assess them as deposits or securities.

Furthermore, those purporting to put themselves out as exchanges need to be regulated as such and should not custody assets on behalf of counterparties. Broker dealers or custodians, not exchanges, should hold assets. They are each subject to different regulations and inspection, given the operating risk of their activities. Counterparties ought to assess the risks as they would with traditional exchanges, brokers and custodians. (Editors' note - While obvious to innumerable market participants prior, this has recently become highlighted as the core of the SEC's developing case against Coinbase).

Despite the current chaotic situation, we have learned nothing that we did not know before. Financial markets are prone to fraud by a small number of unscrupulous actors whenever they are left unregulated as they blur the lines between roles and use the fog of the "new and innovative" to gloss over the reasons why these regulations were created in the first place. Even with the best of regulation, financial services organisations are still prone to the actions of people who seek to cheat when incentives to do so are high.

Yet, while the de-centralized technology may be harder to regulate, the people and the on-ramps to the technology are centralized under governing authorities. Perhaps unscrupulous actors will "re-learn" this fact as well and over time they will be replaced by good actors.

Regulation via Programming Code

Our final point is, therefore, that there will continue to be more and new frauds until the general public's latent demand for the benefit of cryptographically enhanced commerce is met by honest actors and through more uniform and less arbitrageable regulation.

One of the early detractions of Bitcoin specifically over a decade ago, as it was positioned as a Virtual currency to replace Fiat currency, was that its very success could lead to its very demise. That is, that if it truly threatened fiat currency, central banks would not allow it to develop further. It was perhaps more surprising and a testament to our democratic institutions that the cryptographically enhanced commerce ecosystem was allowed to develop.

Yet, the last few months feel like a more concerted effort across regulators (CFTC and SEC), central banks (ECB), the IMF, and governments (U.S. Department of Justice) are on the attack in regard to bad actors as well as "threats" to the financial system. An example of one such threat to the system is DeFi.

Decentralised finance (DeFi), which is often an attempt to bypass regulated finance through the lack of intermediation, regulation, administration and corporate governance via distributed servers is still coded by individuals. It may be that DeFi is targeted by future legislation to regulate code. Its current structure may be treated as malicious. There is much legislation that already exists where malicious code and their coders are treated criminally. DeFi may literally find itself on the wrong side of cybersecurity law.

The U.S. government, via the U.S. Treasury, set precedent in its sanctioning of cryptocurrency mixer Tornado Cash. Historically, code has been protected based on case precedent as free speech. But in this instance, where Tornado cash was an application which "tumbled" and "reprocessed" coins with the purpose of making senders and recipients unrecognisable, the code was arguably malicious. There were allegations that North Korean hackers laundered some $100 million via the tool. The coders were sent to jail while they await trial.

We believe regulation and enforcement may intertwine with national security and political interests. This could lead to the regulation of "code" itself, including how it is used and whether it can be used at all. New laws around code can obviously always be proposed and legislated. That is cyber-security law, anti-money laundering and securities law will intersect to protect the common interest.

Conclusion

The future in a specific sense is unknowable. It may be that Bitcoin is eventually replaced by an as yet to be invented crypto currency. Perhaps Coinbase and others will win their various cases. Yet in a macro sense, as long as commerce is transacted, and as more of it is done electronically, the need for crypto-graphically enhanced commerce is here to stay. We would argue it will inexorably grow. Yet, as large parts of commerce require by definition opacity, negative externalities – the risk of fraud – is here to stay as well. But the fraudsters are not decentralized and virtualized. Governments and regulators are positioned to meet the challenge and, if necessary, will use new tools to find and stop them.