Cryptotwilight Productions © 2023

ZK Sera

What could happen when blockchain and crypto go wrong

"...You as an individual should not have to study to be safe to rely on the devices that you use every day…" - Edward Snowden[1]

[1] Edward Snowden on the Importance of Privacy (11/10/2016), https://www.youtube.com/watch?v=WRzm7wrk_FA, accessed 15/05/2022

Introduction

The following paper is a treatise on some of the worst outcomes that could result due to the adoption of cryptocurrency and blockchain on a mass scale. The paper will cover a review of the original aims of the space, what the space has achieved to date and where it is headed, followed by a projection of outcomes and consequences.This paper will then move on to discuss the decisions that need to be made by participants in space along with projects that need to be created to address the perceived challenges. The paper will conclude with a commentary on the risks of inaction or inadequate action both for the crypto and blockchain industries as well as society as a whole.

What Cryptocurrency and Blockchain seek to achieve

The primary aim that drove the adoption of blockchain was bitcoin which was in the beginning an attempt to liberate individuals from the perils of the global banking system through self custody, openness, transparency and permissionless access[2]. This was then quickly followed up by the creation of the Ethereum blockchain which sought to bring application level functionality to the blockchain enabling another dimension of transactionality based on the same founding principles of openness, transparency, self custody, and permissionless access[3]. However with the subsequent influx of massive capital leading to multi billion dollar levels of circulating supply the bad actors, surveillance actors and indeed the regulators were not far behind in following the budding revolution that threatened to upend the global order. Indeed in several states the use of cryptocurrencies was banned[4] whilst more backhanded methods to suppress the movement such as denial of bank accounts to cryptocurrency businesses, and onerous regulation to its use were used by more advanced states to slow the adoption of this latest trend[5].

[2] https://financialgym.com/blog/2021/1/2/bitcoin-101-what-is-bitcoin-and-why-was-it-created, accessed 15/02/2022

[3] https://www.cointribune.com/en/who-created-ethereum-and-why/, accessed 15/02/2022

[4] https://www.euronews.com/next/2022/08/25/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2, accessed 15/02/2022

[5] https://www.linkedin.com/pulse/where-open-business-bank-account-europe-crypto-mark-van-rijmenam/, accessed, 15/02/2022

What is being achieved

Despite the impediments and hurdles, the blockchain and cryptocurrency industry has made a lot of great strides in a variety of fields such as sustainability where we have organizations like the Climate collective[6] and Open Earth Foundation[7] which are actively using blockchain to battle climate change in tangible ways. Following on from this we've also seen the rise of Regenerative Finance organizations like AeraForce[8] and Kollektivo[9] which are using new financial primitives enabled by cryptocurrency to invest in projects that produce tangible outcomes and business exits.

We have also seen new disciplines being created such as MachineFi which is where blockchain meets mechanical, digital and electrical technology, in short it is where blockchain meets the internet of things. Alongside this we have the Mobility Open Blockchain Initiative[10] which is looking to integrate blockchain into spaces like automotive going beyond simple provenance to aspects such as usage fueling and carbon offset.

[6] https://climatecollective.org/, accessed 15/05/2022
[7] https://www.openearth.org/, accessed 15/05/2022
[8] https://www.aeraforce.xyz/, accessed 15/05/2022
[9] https://www.kolektivo.network/, accessed 15/05/2022
[10] https://dlt.mobi/major-automakers-startups-technology-companies-and-others-launch-mobility-open-blockchain-initiative-mobi/#:~:text=MOBI%2C%20the%20Mobility%20Open%20Blockchain%20Initiative%2C%20announces%20its,global%20vehicle%20production%20in%20terms%20of%20market%20share., accessed 15/05/2022

The current trajectory

Despite all these exciting developments in the space, the elephants in the room are those of governance, privacy and regulation.

Governance

The cognitive dissonance that exists in the blockchain and cryptocurrency world today is that you can have governance with permissionless access. Quite simply governance implies control and hence permission. Permission further implies some form of centralisation of power be that in a collective majority of votes or a core team. The challenge here is that of classical moral hazard[11] which has plagued the blockchain and crypto industry since the DAO hack[12]. Quite simply as the push towards mainstream adoption of the blockchain and crypto space grows there increasing incidence of unethical and in further cases blatantly corrupt behavior will rise. This is evidenced by the recent debacles[13] in the space which threatened to destabilize the global financial system.

Privacy

The use of open public blockchains has been immensely popular as the permissionless access has meant that anyone with the know-how can effectively make themselves at home onchain without having to request permission from anyone. However the implicit price of this domicile has been that of privacy. Indeed in years past blockchain activity could be highly pseudonymous as onramps and off ramps where not as guarded by KYC and AML regulations as they are today. Indeed short of giving a crypto exchange your bank details your onchain activities where essentially between you and the community. Even with advanced trackers it would be hard to determine your identity and hence your activities. However that has now changed and not in a good way. Simply with the closure of several major peer to peer off ramps such as Local Bitcoins[14], knowing what you are doing on chain has become a simpler matter of getting access to your Centralized Exchange or regulated off ramp identity. With that a surveillance capitalist or otherwise can quite easily understand everything that you do as a user or customer onchain legally without your permission creating an even more frightening map of activity than is available today to platforms like Facebook et al.

[11] https://www.britannica.com/topic/moral-hazard, accessed 15/05/2022

[12] https://www.gemini.com/cryptopedia/the-dao-hack-makerdao, accessed 15/02/2022

[13] https://www.nytimes.com/2022/11/10/technology/ftx-binance-crypto-explained.html, accessed 15/05/2022

[14] https://www.makeuseof.com/localbitcoins-announces-closure/#:~:text=LocalBitcoins%2C%20one%20of%20the%20first,close%20on%2016%20February%202023., accessed 15/05/2023

Regulation

Finally regulation. As mentioned above regulation has been tacitly weaponised to reign in the adoption of cryptocurrency. We have yet to see regulation specifically targeting the use of blockchain technology for example smart contract oriented statutes. The trajectory here is quite bleak as despite efforts by some administrations to appear accommodating and progressive towards the blockchain and crypto space, the tendency of regulators is typically to follow the path of least political and operational resistance. In short, regulators are not reasonable because they want to be, they are reasonable because it reduces the consumption of resources associated with enforcement of the regulations. The challenge here for the blockchain and crypto space is that advances in technology also reduce the consumption of resources associated with enforcement and when propositioned by what is effectively open data the ability of the regulators to enforce is increased exponentially for a nominal investment in tooling.

The projected outcomes

It would be nice to say the outcomes are projected however we are already seeing the implications of the above three elephants going on stampede. The first example is that of post hack blacklisted addresses. On the surface this seems like a good thing like in the old western movies, until you realise that said movies represent the catalogue of a genocide. Similarly the black listing of addresses means that anyone can be targeted regardless of transgression, whether committed or not. We've also seen the implementation of the social credit system in China which has a devastating effect on the ordinary citizen when they fall onto the wrong side of the law even with minor infractions.

Looking further forward without concerted action from the community the issue of corrupted and perversely centralized governance will ride roughshod over users and communities. Compounded by the abuse of open data we enter a world whereby heinous infractions against individuals are perpetrated by autonomous organizations leading to draconian legislation that is out of the imagination. Even with progress being made in technologies such as Zero Knowledge proofs, the challenge of how to deal with exchanges and how to deal with inference fingerprints still remain. Again the understanding here is that the privacy of the individual in present society is antithetical to enforcement of the law over an individual.

The final and most telling outcome of the three elephants' rampage is the rise of cartels and caged innovation. In this outcome we see blockchain and crypto innovation caged into a direction that can be controlled much like we've seen with previous incarnations of technology such as digital. In this space there are only a handful of significant players whilst the balance of the market is reduced to towing the line or else facing censure or sanction. Whilst it has been possible to escape this hegemony using blockchain and crypto, were this hegemony to establish itself in the blockchain and crypto space it would be quite difficult to escape, for an extended period.

Decisions to be made

This leads us to a choice about the decisions that need to be made to avert the above dystopian nightmare. Like the turning of an aircraft carrier, the decisions and actions need to be made now else should the above occur we will be already lost. It is in this vein that we consider the three elephants and the decisions that they require from the community today and not at some later point in time.

Decisions on Governance

With respect to governance the decision that needs to be made is on what is the definition of permissionless governance? Is such a concept even possible and if not at present how do we iterate towards it in a culturally diverse and inclusive decentralized web.

Decisions on Privacy

For privacy the community needs to decide how do we think about open systems i.e. how do we share data in the open and protect data that could potentially be harmful if left in the open. In this space we're also thinking about how we avoid the false choice between centralization and decentralization. In short there is a balance that needs to be achieved, as well as a calibration to that effect.

Decisions on Regulation

Presently the blockchain and crypto communities have taken different approaches to assisting regulators in understanding the blockchain and crypto proposition. This has been mainly focused on aspects around the financial implications of the space. However as a mainstream entity the blockchain and crypto space will impact everything to do with daily life. If instituted as Central Bank Digital Currencies, the space stands the very strong possibility of being globally outlawed. So the decision that needs to be made by the community is how do we proactively expand regulatory engagement to include those areas in which we are innovating but have yet to establish clear solutions.

What needs to be built

This leads us to what needs to be built. What we are looking at here is how do we move to a situation whereby all world communities are adequately represented in decisions on how to deal with the three elephants. Quite simply there is no global one size fits all, however there are common lessons and sharing that can be done to speed advancement of thought and practice in areas where institutions and levers are slow to evolve. There are three archetypes which need to be built to adequately deal with the three elephants in a globally permissionless and decentralized context. They are

- Governance Archetype
- Privacy Archetype
- Regulatory Archetype

The idea here is that each archetype can be taken and adapted in full knowledge of the impacts of various decisions on community compatibility with the wider decentralized world and also effect on the community itself. Fundamentally each Archetype seeks to bring together the diverse cultures of humanity by binding them to common shared values that are found across the world. Whilst this might seem lofty this is necessary to remove unconscious bias and neo colonial constructs, which are still prevalent in educational systems across the world today.

Governance Archetype

This product is a blend of global philosophies of governance distilled to a model that enables decentralized blockchain and crypto groups to establish authentic and accountable governance regimes where individuals and the collective can be held appropriately responsible for failings.

Privacy Archetype

This product is a blend of global perceptions of privacy which vary considerably across the world. The idea of this archetype is to enable blockchain and crypto groups to understand and effectively build and communicate their stance on the different and expanding aspects of privacy that new technology is bringing to the fore.

Regulatory Archetype

This product is a blend of the different global regulatory regimes, divining their commonalities and divergences. This archetype is important in that it enables blockchain and crypto groups to better understand how to shape their regulatory engagement in light of the other two archetypes and decisions around them.

Concluding Remarks

The blockchain and crypto space is indeed extremely exciting. By providing a viable alternative to payment and settlement that avoids the more expensive banking system, it is certainly poised to become a dominant force as the decades move on. A failure by the blockchain and crypto communities to act with adequacy and with force to address the challenges that have led to the recent and not too favorable headlines will lead to a perversion of the space into the aforementioned horror of a rampage by the three elephants. This is a risk that will have Orwellian consequences.

"… if you want a picture of the future, imagine a boot stamping on a human face forever. The moral to be drawn from this nightmare situation is a simple one don't let it happen it depends on you" - George Orwell 1903 -1950[15]

[15] Orwell's final warning - Picture of the future, https://www.youtube.com/watch?v=9k_ptxWsadI, accessed 15/05/2023