International Journal of Scientific Research and Management (IJSRM)
||Volume||09||Issue||08||Pages||EC-2021-604-610||2021||
Website: www.ijsrm.in ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v9i08.ec01

The End of all Taxation and Censorship using Blockchain technology

Tanmay Munjal

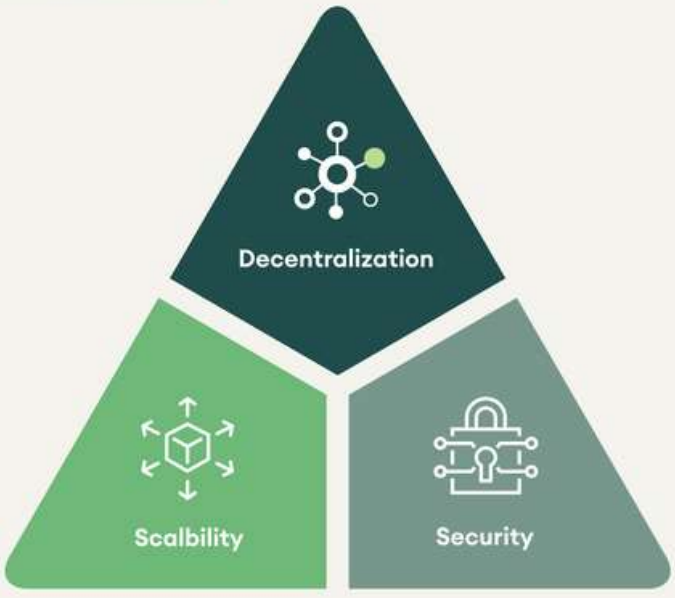
Abstract
Large scale censorship and control over the free flow of information on the internet that was already implemented on a large scale in many authoritarian countries in China in the past few decades has started to work its way through the more liberal and western countries including India, US, etc. especially in the last decade raising concerns over privacy issues and the possibility of a dystopian future of tyrannical governments empowered by the use of digital surveillance technology to increase their power and make them essentially undefeatable on a level unforeseen in the history of humanity among many great thinkers in our era. In this paper, we wish to outline a method to not only combat but to eliminate both the possibility and current usage of all censorship and control over the flow of information on the internet, hence heralding an era of free flow of information throughout the world and destroying practically all mind control that tyrannical governments can hold over their people, in essence ending the era of propaganda and tyranny from the face of this earth forever, using blockchain technology.

Keywords : Monero, Blockchain, I2P network, Decentralization, Death of taxes

Introduction

Blockchain technology refers to a decentralized ledger-based system that surpasses the double-spend problem classically associated in computer science with decentralized systems of finance and accounting. Many cryptocurrencies have been based on it including Bitcoin, Ethereum, Monero, etc. and also many decentralized applications have been rendered on it, most famously the Brave browser.

Figure 1: The blockchain trilemma



Source: SEBA Bank AG

In recent years, blockchain has grown exponentially in popularity and started to have widespread adoption in the financial world and even in the life of an average civilian in some countries. Yet, a major problem with current blockchain architectures is the fact that up to this point, each and every blockchain developer has had to sacrifice at least one of the following three functions- Decentralization, security, or scalability. In essence, until this point in time, we have found no method of creating a decentralized, secure and scalable blockchain-based network. Furthermore, another problem has been the problem of privacy on an open ledger though this has been solved to a large degree by Monero and the corresponding private platform of Kovri that can be used to use Monero rather than conventional internet methods to completely anonymize the identity of the user.

In this research paper, we wish to present a solution to the abovementioned problem of implementing a blockchain-based system that can efficiently perform all three of the major functions while being private and completely anonymized, in essence transcending the famous scalability and privacy problems of blockchain and allowing widespread adoption of completely private blockchains throughout the globe hence ending all censorship and restriction on the flow of information permanently without resolve except if a tyrannical government was to stop all supply of electricity in a nation and return to a pre-industrial age era which in this paper would be considered a possibility with a probability of occurrence as null due to obvious considerations.

Atlantia- A solution to the scalability issues

The first consideration in the design of such a cryptocurrency is the process of making it as private as possible. In essence, this is a practically solved problem already using Monero and Kovri. In essence, Monero uses several cryptographic techniques such as Ring Signatures, Ring confidential transactions, and Stealth addresses to obscure the identity of both the sender and receiver of the payment and also the amount transferred while making it possible for the entire blockchain to verify it as such. This left the problem of the possibility of detection of the IP address of sender and receiver at the point of interface between the computer and the wider Monero chain and for this purpose the Kovri platform was created.

Indeed, the method of tracking IP addresses is how China's Great Firewall functions, one of the most sinister plans to control the flow of information and create a tyrannical government, and even though VPN networks are available, they are often liable to correlation attacks or coerced to give an individual's private information. As such, the issue of solving the problem of IP address tracking is a major issue to solve to take down China's Great Firewall and many others like it though none as extensive and sinister as it which are being built by many governments throughout the world including even many "liberal" and "democratic" European and Asian nations.

In essence, Kovri is an I2P network, a class of networks that work by a private overlay network over the internet to enhance privacy, and Garlic Routing and encryption hence making it far harder to hack than even other privacy-based networks such as Tor and many others. This is not to say Kovri might not have any issues as it was still in development when it was abandoned by its developers, but it must be noted that implementation of I2P may be practically unhackable and private given the efficiency and strong privacy of such networks.

At this point, we have discussed how to create a privacy-focused coin but the problem of scalability is still an issue. In essence, several methods like sharding, proof of stakes, and other second-layer solutions have been discussed in the past but the main issue with them is the fact that they are generally accepted to be less decentralized than the main chain and hence more vulnerable to manipulation and attacks.

But it must be noted that this might not necessarily be the case, indeed even highly accepted cryptocurrencies such as Bitcoin have been reported to have only 4 or so miner pools controlling more than 51% of attacks. This is not to say that such cryptocurrencies are not a step above the general large digital corporations of today but this is not the complete non-censurability that was imagined in the minds of idealists of the cryptocurrency world.

Furthermore, Pos and other methods to scale blockchains may also suffer from a small number of nodes controlling the network. Though methods may be implemented to change such nodes quickly and set up incentives against cheating against any particular client, the power of a centralized government to do so despite the wish of the node and extreme harmful conditions that the node may suffer from losing its funds and even loss of access to cryptocurrency if caught cheating especially if the node is barred from a widespread and mainstream adopted cryptocurrency. This in essence might allow a centralized government to control the flow of currency and information even more closely than ever possible before.

It seems to me that an unlikely mixture of different technologies may be used to combat this problem in a method that to the best of my knowledge and research has not been used before. In essence, using layer two scaling on a completely anonymized blockchain network using techniques mentioned above on a well-created I2P network with necessary modifications shall create a completely private chain where sender and receiver address and amount of transaction shall not be known even to the miners.

Hence, this will eliminate any chance of selective censorship by a centralized authority with great physical force and also it must be noted that some of the same methods, with some little innovation to adapt these methods, may be used to obscure the identity (IP addresses specifically) of the miners hence disallowing a government authority from interfering in the mining process while the standard methods discussed in the wider blockchain community may be used to ensure lack of corruption and a great level of decentralization in the system.

Hence, this shall lead to the creation of a completely anonymous, secure, scalable, and highly decentralized blockchain network, one that might be far more decentralized than the current networks which may be controlled by a small number of mining pools that are vulnerable to centralized government control. Furthermore, adding some functionality within the blockchain for storage mechanisms and network data transfer using current and future innovations and setting the appropriate incentive structure within the blockchain may allow such a blockchain to host entire websites and applications, in essence over time growing to full-fledged completely private, secure, and uncensorable payment channels, browsers, social media, etc. ending the era of censorship forever.

It might be argued by some that the ideas presented in this paper until now have all been known ideas but it must be noted that this combination of ideas for creating a completely secure and anonymous network resistant to all forms of government censorship has not been proposed or built at any point before this research paper to the best of the author's knowledge and hence constitutes a new technology with a prospect of adding value to the human civilization. As long as the former premise is accepted to be true, the author wishes to debate no further.

The death of taxes and the new world

In essence, the technology detailed above can be used to create a completely anonymized internet and digital currency, hence ending all censorship and mass tyrannical state control on the flow of information and currency, the two assets that each and every tyrant and dictator requires to rule and dominate a nation. Yet this same technology has a massive implication for the future of democratic and liberal countries as well and in general any type of country, a massive implication, the death of taxes.

We have all heard the ancient proverb "In life, only death and taxes are certain.", yet here the technology we are discussing can herald a new era, revolutionizing and restructuring all of human civilization, the end of taxes. In essence, the completely anonymized nature of information and currency possible using such technology will render the current capacity of the government to discern how many funds each citizen has or how many funds have moved hands impossible hence making the collection of taxes impossible.

Some may argue that such technology must be banned but it must be noted that it will not be possible for the government to discern which of its citizens are or are not using such a technology, hence the government cannot ban or track it and hence it lies entirely beyond the power of the state to regulate or ban it, it is impossible to do either.

It must be noted that though that the worldwide implementation of such a technology would require network capacities far greater than current infrastructure or technological capacities can handle but given the profit

motive and the fast rate of technological growth, this barrier may be surpassed in as little as 6-10 years, a short time frame for man to prepare for the death of taxes, the greatest single tool it has used until now to build up and manage its civilization since all of recorded history.

As such, accepting the inevitable nature of such a massive revolution lest we wish to ban all of internet and communication technology and perhaps even electric technology and returning to a pre-1800s time, we must think about what the post taxation world shall look like for if one is to not greet this simultaneous challenge and opportunity with the respect it deserves, mankind may fall into the archaic chaos from which it has differentiated itself with so much effort and violence through the past few millennia.

Indeed, the death of taxes is an event of such importance in the history of humanity that history from henceforth may be stated to belong to a new period, a higher history.

In this research paper, we shall call such a future post taxation world, the new world. We do not claim to provide a full and final analysis of how such a new world shall look like but merely spark discussion and debates throughout the world for such a great discussion which shall shape the future of all human civilization and do an elementary analysis of an optimistic possibility that the author believes to be a possible state for mankind after the death of taxes.

Following the death of taxes, even though some minute quantity of state power may be maintained using independent methods of earning revenue by the state, a massive reduction in size and power of the state is likely to be seen and a massive simplification and reduction of all laws and regulations as the state shall no longer possess the resources necessary for implementing such complicated laws and regulations, in essence, it is very likely that most of the legal code shall be reduced to bare essentials of banning murder, rape, and death by industrial negligence while most other offenses shall have to be settled by the free market itself for the state shall not have the capacity to implement complicated codes any longer. It is also likely that some level of violence as long as it does not constitute a permanent disability or death shall be made legal for the state is unlikely to wield the resources necessary for maintaining such laws. Furthermore, the heads of states shall cease to be regarded with the seriousness they are currently by the general public and shall lose practically all of their power, indeed they may no longer be regarded as the heads of nation anymore but only its state which shall have limited control over the nation. A massive fall in military size and complexity is also likely as states shall no longer have the capacity to maintain huge militaries.

It might be possible to develop taxes to be levied using the cryptocurrency itself but given the personal motive and personal freedom of deciding on your currency by each individual, it is likely that the cryptocurrencies with no taxation are likely to dominate in the long term over cryptocurrencies with tax rates even if the latter proves to be more beneficial for the social structure as a whole.

What is more likely to occur given the scenario, the known facts of human nature, and the loss of heads of states as true leaders of nations is that man will attempt to find new leaders both local and on the large scale. This will likely be perceived as an increase in strength of religious movements though many other secular movements may rise but historical experience has shown that secular movements are generally far more unstable than religious movements in the long term, generally produce weaker communities, and are in general not suitable to the task of providing leaders generations after generations that the general populace may feel related to and support.

As such, it is likely that religious movements shall dominate over secular movements in the long term in the new world. Indeed, it is likely that the priest/priestess within the major places of worship shall gain a massive amount of support and power in the new world.

It is furthermore likely that it will be a far dangerous place than our current world for there will be far fewer laws, both of unnecessary tyrannical nature and those that produce helpful defenses of justice, and far fewer resources with the state to implement said laws. Some laws may be implemented strictly by new religious institutions based on warrior religions using voluntarily donated funds and using the help of voluntary officers. This is likely to provide some order to the massive growth of chaos in this hypothetical new world.

It is also likely that a massive increase in rural communities will occur and the power that the leaders in such communities hold is also likely to increase, communities that will likely provide man with safety, comfort,

and trust in one's neighbors and some level of order in the absence of other methods while taking a proportion of their earnings as taxes. Taxation at the level of very small rural communities with local judges shall still be possible as everyone in the community will have a good rough estimate of the earning of their neighbors earning using local news. But the same may not be said for people living in urban areas or taxation to a centralized government where the judges are not aware of the local situation, for in such cases which constitute practically all if not all taxation in practically every state in the world (Afghanistan may be an exception) today, the collection of taxes shall prove impossible.

In essence, this would lead to the constitution of comparatively safe, though dangerous by current standards, local communities surrounded by far more dangerous regions outside where some law and order still exists but is not properly implemented. In essence, the closest resemblance to the above-mentioned situation maybe how the wild west in America looked like in the 19th century. Indeed, this might be the closest possible comparison to the likely new world which shall appear in the post taxation era.

Conclusion

All in all, in this paper I have ventured to introduce a new technological system based on the blockchain architecture that allows man to end the censorship and allow free flow of all information and currency without state or government overhead or/and a massive corporation being necessary or even possible while maintaining complete and total privacy and anonymity. This presents a major perhaps fatal injury to the way tyrants and dictators have always controlled the populace but also disrupts and completely shifts our systems of governance forcing us to ponder and create a new world that will undoubtedly be radically different from our current system. Furthermore, I have tried to present a scenario that I consider in my convictions to be the most likely scenario of such a massive shift in mankind's social and economic structure. I do not claim this to be exact or even accurate analysis and indeed it will take large amounts of debates and discussions before any solution to such a massive problem is likely to present itself to us.

None of us can claim to be away from this massive wave of change that falls onto our civilization nor is it useful to judge this wave as good or bad for it is not possible to stop it, it cannot be banned or regulated, but all that can be done is to prepare and plan for this incoming wave so that we may not be swept away by it but be strengthened by it and for this purpose, the news of the upcoming death of taxes and censorship must reach the ears of man and for this purpose, this research paper has been written.