A Search For The Optimal Cryptocurrency to Replace Fiat in Business and Fiscal Sectors

1st Batıkan Bora Ormancı
Computer Engineering Student
Turkish-German University
Istanbul, Turkey
batikanor@gmail.com

***Abstract*—Replacement of fiat currencies has been considered throughout the history of mankind, for the monetary standards of our life have always been controversial. With the rise of cryptocurrencies in popularity, some individuals and groups of individuals have either tested or considered a switch to cryptocurrencies. Throughout this study optimality metrics will be determined and evaluated for comparison of different blockchain-related financial solutions, and scenarios of cryptocurrencies replacing fiat money for countries, businesses and individuals will be examined. Said examinations will include solutions for differing forms of problems and problem stakeholders.**

***Index Terms*—blockchain, business, fiscal, fiat, crypto, currency**

I. Introduction

Cryptocurrencies have been developed and proposed with countless differing motivations, a good portion of which are with the explicit or implicit aim of replacing fiat in business and fiscal sectors.

Throughout this study, the possibility of such an emergence will be researched. The main problem hereby addressed will be about how some factors preventing this change from happening, such as taxing and scalability, can be challenged and which quality requirements are to be met for potential mass adoption of a conventional money alternative.

II. Methods

III. Determination of Optimality Metrics

To be able to talk of 'Optimality', comparative metrics were to be determined beforehand. These were hereby dichotomized as follows:

A. Technical and Motivational Innovations

These aspects question if finance should be decentralized and how, to which extent. Should blockchain only help centralized finance scale better, or override its predecessor. There are no limits whatsoever to innovations. Should transactions be capable of depending on turing-complete conditions, or is a peer to peer electronic cash system sufficient, while the rest could be built outside of it just like regular programs are. The questionability of these matters makes every single one of them worthy of its own discussion. A good example would be ethereum, which literally started blockchain 2.0 revolution with the innovative addition that is smart transactions (it should be noted that -contrary to common belief- the bitcoin protocol actually already had a simple version of smart contracts before the introduction of ethereum) [1]. However, some common features of cryptocurrency related innovations could be extracted for use within the aim of this paper. Note that some of these features are strongly correlated with one another, which will be ignored for this study. Hereby the following were extracted:

1) **Attractiveness:** Twitter or reddit activity related to respective technology are some of the most prevalent indicators of attention. Any kind of interest and reaction people may show to an innovation will hereby be counted as attractiveness.
2) **Marketability:** Ideas can be worth money. They may be worth exact amounts of money, or their price may be open to speculation. Either way, every stakeholder will consider the marketability of an innovation before supporting it.
3) **Eco-Friendliness:** This aspect could be seen differently by many different types of individuals. Some people would like to save the environment, while some would like to feel like doing so while making things worse. Some other people reject the idea of there being any environmental risks approaching and some people don't really care about these issues, but care about the marketability of eco-friendliness. Either way, eco-friendliness usually comes with a big trade-off, usually related to either consensus or decentralization. Proof of Work algorithm of bitcoin makes it so, that it is hard to create bitcoin and the hardness of the process can be proven. Also there is no need for a central authority to issue or certify the creation of coins. Imagine an application where submission of cat noseprints (which are known to be unique, just like human fingerprints) are rewarded, and

the supply of coins is limited to number of cats on earth. Such a project wouldn't require much processing power, could be build further to take huge care of all the cats on earth, but at the cost of decentraliztion. You would need a central authority to tell the geniuneness of a cat noseprint, because these can be faked, even in an universe where they couldn't be easily faked, it would be hard to represent the whole of a cat in binary form and ensure security (which is required for a decentralized solution). However Nonce solutions to a cryptographic hash function cannot be faked, which deems bitcoin to be a financial revolution and my cat noseprint idea a funny example.

4) **Religious Conformity:** Religions bring rules, and cryptocurrency projects may be shaped to be conforming of these rules, or otherwise.
5) **CSI: Capability and Strength of Independence:** A good portion of people don't understand that the cryptocurrencies they buy and sell at exchanges don't directly use their respective blockchain technologies. They are processed exactly the same way normal virtual money -or any centrally secured virtual asset- would be. This makes them dependent of that marketing platform. It is the provable fact that they are backed by other notions than 'trust in government' that makes cryptocurrencies different, and that is not being satisfied to its full extent when there are authorities who are capable of limiting the trading and holding rules. If a cryptocurrency project is both capable of being independent (blockchain technology pretty much enables that) and is strong enough on that aspect, that it may become a reality whenever necessary, then that project will hereby be considered to have CSI.
6) **Should Crypto Replace or Assist Fiat?:** The answer of this question may vary depending on the stakeholders. While some U.S. banks have been enjoying Ripple (XRP) integration [2], probably most cryptocurrency enthusiasts want banks to be replaced instead.

B. Quality Requirements

In addition to the aforementioned features that were extracted from Technical and Motivational Innovations, there are some relatively more practical quality requirements that cryptocurrencies are -on differing levels- conforming of. Some of these requirements will be extracted from cryptocurrency whitepapers (a whitepaper in this context is an academical article that is usually published around the same time a new blockchain project comes into existence, to explain about its innovations). The original bitcoin paper has a focus on security and privacy, due to the cryptographic fundamentals being crucial for the first cryptocurrency (E.g. the original bitcoin paper states that frequent payment receiving companies are likely to emphasize on security, for which they will e.g. run their own nodes [3]). However, one of the most central motivations of bitcoin and cryptocurrencies in general, that is decentralization, is interestingly not a word that is present in the bitcoin whitepaper. Which alone is sufficient proof that only extracting these terms from whitepapers would be misleading, therefore some terms will be added from other sources at the author's own discretion.

Such requirements are listed below:

1) **Decentralization:** According to many, decentralization is a must for blockchain and cryptocurrencies. Some say that a centralized 'blockchain' cannot even be counted as a blockchain. After all, linked data structures have been present in computer science since quite a long while and naming a node 'block' and connection 'chain' is also an option. But without any introduction of an aspect related to decentralization, is it really blockchain? How decentralized a cryptocurrency is is definitely a very important metric to evaluate.
2) **Scalability:** As the usage rate of a project increases, new challenges arise. This concept is summarized with one word in many domains: scalability. As the number of transactions in a blockchain increase, problems arise. (E.g. if there are not enough validator nodes, people may have to wait for a new block to be mined for their transaction to be confirmed, which simply makes it all quite slower... [4]) Almost all cryptocurrency communities are aware of the importance of scalability and solutions are being proposed at a really high pace.

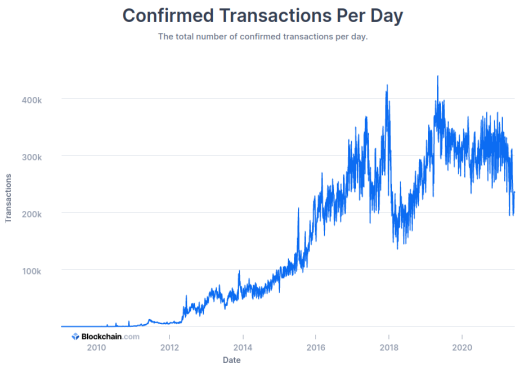

Fig. 1. Confirmed Bitcoin Transactions Per Day [5]

3) **Security:** Security is also an essential part of the blockchain technology. Cryptocurrencies have

strong cryptographic primitives that are keeping them secure, but there is definitely room to improve.

4) **Privacy:** Some projects such as Monero (XMR) and Verge (XVG) hide and obscure information really well, keeping their users anonymous. But Bitcoin (BTC) is only pseudonymous. [6] Complete lack of trackability obviously makes currency more useful for illegal actions, but all your financial data being tracked doesn't really sound exciting for most.
5) **Volatility:** Some projects have great potential, but the instability of their price level is a really demotivating factor for their investors or potential daily users. Therefore volatility is a really important aspect to consider.

IV. Sample Scenarios

Cryptocurrencies may bring differing solutions to same problems. In this section some sample scenarios will be built and comparisons will be made w.r.t the aforedescribed metrics of optimality.

A. A Country with a Failing Economy

Zimbabwe has had a lot of economic issues, and after massive macro-inflation decided to abandon its official currency Zimbabwean dollar in 2015. [7] Instead they adopted a multiple-currency system where other fiat currencies were used instead. The question to ask is: Why use a currency that can be printed by some other authority as much as they please, while you could have one that is decentralized? Countries definitely have more power above their people when they print their own money, because they can make everyone poorer and the government richer if their inner systems don't somehow prevent it. But when that system fails, what is the point of choosing a multiple-currency system over a decentralized system? A.1 Attractiveness, A.5 CSI, B.1 Decentralization, B.2 Scalability, B.3 Security and B.5 Volatility would probably be of the biggest importance in such a scenario. Only metrics among these that are hard to be satisfied today according to the authors discretion are metric A.5 and metric B.5. While low CSI levels present today make it harder to make people trust in these currencies, the actual deal breaker would probably be volatility. It would be too big of a gamble for a country to risk having all their citizens make an investment that may lose a lot of value in a really short notice after having survived a huge devaluation rally. So, such a country should consider switching to a cryptocurrency with a possibly low volatility, which could be Ethereum according to the latest statistics. [8]

B. A Communist Country

Leaving the good and bad sides of the communist system aside, a cryptocurrency that would best fit their needs would need to emphasize A.5, A.6, B.1, B.2, B.3, B.4 and B.5. Of course, features like A.3 and A.4 may also be important for specific cases, but this is more of a general scenario. A communist country would argue that B.4 Privacy is a dangerous aspect. They wouldn't want cryptocurrencies like XMR and XVG to gain fast adoption, because when the transactions or wallet balances are all encrypted, it would make it almost impossible to track how much money some individual may have. When people are given the freedom to buy and sell all they have, and have it not be tracked, financial state inequality is unavoidable. The whole 'decentralization' approach is somewhat individualist, and it is probable that a communist country would only like to use cryptocurrencies to assist their current monetary systems. As the Aspect A.6 tends towards assisting fiat, they would try to find a cryptocurrency that also has good levels of security, scalability and volatility. Ripple (XRP) can be used by banks as an intermediate currency for transactions [9] and would probably be the first solution that comes to mind due to its popularity. However, the features of a cryptocurrency are more important than its name, and it is important to note that the evaluation of aforedescribed features for these scenarios doesn't have to imply the proposal of a specific cryptocurrency. This country would probably end up creating its own centralized 'blockchain', however converging decentralization with communism would be a completely different topic of research.

C. A Company Caring About Its Image or The Environment

Companies care about their images, and while all other aspects (A.1 to A.6, B.1 to B.5 and beyond) would be important for more specific scenarios, aspects that have a close effect on image are A.1, A.2, A.3, and A.4. Such companies would tend to choose attractive, marketable, and eco-friendly solutions. While eco-friendliness requires a huge tradeoff of one or many of the quality requirements such as decentralization and security, which makes the blockchain one that cares less about aspects that make it a 'blockchain', and perform worse in that sense, eco-friendly cryptocurrency projects still exist. However none of them managed to gain enough recognition, therefore such a company would probably invest in existing popular solutions and try to make the developers make eco-friendly changes on the repective blockchains. A similar scenario has been happening with Tesla and Dogecoin, but of course, with a very complex background.

D. A Libertarian with Strong Monetary Independence Wishes

To cut it short, they would prioritize all quality requirements with privacy being a must. Individuals should have the freedom to own value and transact without oversight. Examples could be XVG and XMR.

E. A Country with a Currency That Is Indexed on Another Fiat Currency

The financial implications of having a currency indexed on another can be quite complex, but it can be argued that above almost all others, the aspects of B.1 decentralization and B.5 volatility would be important. Such countries should study the implications of adoption of cryptocurrencies with acceptable levels of these attributes, and at least consider a switch. Somewhat valid examples would be BTC and ETH. However, countries may even choose to start their own cryptocurrency - which is currently being considered by a good amount- and shape it accordingly to their needs.

V. Conclusion

While the future of cryptocurrencies, and therefore the whole monetary system of the world, are full of uncertainties, there definitely is some use case to cryptocurrencies today for individuals, countries and companies. All of these parties naturally tend to do what is good for them, and if cryptocurrencies could improve on some deal-breaker aspects, many of them could challenge any other method of transacting value. At this point, after a lot of cryptocurrencies having managed to reach huge communities, it wouldn't be realistic to say that only one would remain in the future, for they present solutions to different problems. Within this research, the determined optimality metrics had allowed certain scenarios of cryptocurrency evaluation to be considered in a simple way. In reality, specifications of individual cryptocurrencies would play a higher role than these optimality metrics that are extracted simple features. However these methods definitely could be reused in order to make fast evaluations to consider replacing fiat in business and fiscal sectors. A final remark would be that businesses and countries are not yet completely ready for major cryptocurrency adoption, and vice versa. But some countries are slowly starting to accept cryptocurrencies as official currencies (e.g. El Salvador [10]), and individuals and companies are mostly excited about what may happen next.

Acknowledgment

I would like to thank Prof. Dr. Adem Alparslan from FOM University for his enthusiastic encouragement, patient guidance, and useful critiques of this research work.

References

[1] V. Buterin. (2013) Ethereum white paper. [Online]. Available: https://ethereum.org/en/whitepaper/

[2] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *International Conference on Trust and Trustworthy Computing*. Springer, 2015, pp. 163–180.

[3] S. Nakamoto. (2009) Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[4] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2018, pp. 122–128.

[5] (2021, Jun) Confirmed bitcoin transactions per day. [Online]. Available: https://www.blockchain.com/charts/n-transactions

[6] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 2017, pp. 1–3.

[7] P. Makena, "Determinants of inflation in a dollarized economy: The case of zimbabwe," 2020.

[8] (2021, Jun) Least volatile cryptos. [Online]. Available: https://finance.yahoo.com/u/yahoo-finance/watchlists/crypto-volatility-low/

[9] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, pp. 45–54.

[10] T. Wilson, "In a world first, el salvador makes bitcoin legal tender," Jun 2021. [Online]. Available: https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/