Letter of Transmittal

To: Thomas Geary

From: Kevin Kilgore

Date: July 11, 2019

Re: Decentralized Social Media Platform Technical Report

Dear Professor Geary,

Enclosed is a feasibility report on decentralized social media which use blockchain technology. Decentralized social media platforms are an alternative to traditional social media platforms which have a growing number of concerns and problems. I would like to thank you for your time and consideration.

Sincerely,

Kevin Kilgore

Decentralized and Blockchain-based Social Media

Platform Feasibility Report

By: Kevin Kilgore

For: Professor Thomas Geary

July 11th, 2019

Table of Contents

Table of Figures

Abstract

The ultimate purpose of this report is to evaluate the feasibility of decentralized social media platforms using blockchain compared to the current social media platforms. This will be accomplished by first providing an introduction which explains the drawbacks of current social media platforms to illustrate why a viable alternative might be needed. Then the report will examine and explain how a decentralized social media platform would function. An evaluation of the feasibility will be provided on factors such as scalability, performance, and monetization model effectiveness. A comparison of decentralized social media platforms and centralized social media platforms in terms of advantages and disadvantages will be provided to reach an informed conclusion.

Introduction

Social media plays a ginormous role in the world around us. "3.48 billion" people use social media which is "45% of the total world population" (Newberry, 2019). Every day it is used for communication, news, expression, public discourse, branding, and advertising. Social media companies hold incredible power over speech, public perception, and user data. With public trust in social media companies already on the decline it is time to consider a trustless system as an alternative. Unlike the current social media platforms, decentralized media would be open-sourced and have full transparency.

Problems with Current Social Media Platforms

Social media companies have had some major missteps particularly on data privacy. Just today on July 12th, 2019 the FTC announced it would fine Facebook 5 billion USD for "mishandling users' personal information" (Kang, 2019). Since Facebook is a friends and family social media network its users' information is incredibly personal. Facebook has undergone scandal after scandal recently. Recently it was revealed that Facebook shared data with a "Chinese firm that was flagged by U.S. intelligence" (LaForgia & Dance, 2019). Google, the owner of Facebook, continues tracking location history even when the users turn on the privacy setting to stop tracking. Although privacy is important, people in governance are even more concerned over social media platforms influence on public sentiment and even elections. Some have called for said companies to be broken up to address the issue.

Background

Blockchain

Blockchain is a distributed ledger which is immutable and uses cryptographic hashes. Blocks which contain transactions are verified via a consensus of nodes on a peer-to-peer network and appended to the chain. This might sound complex but just imagine it just like any other ledger like a financial ledger. Instead of being stored in a centralized location the ledger is distributed, and thus decentralized, upon many computers, mobile devices, and servers which are users of the given blockchain. The ledger is kept up to date on all online machines. A single computer or device is called a "node" of the larger network. As you can see in Figure 1, a peer-to-peer network is a type of decentralized network which is merely a direct connection between nodes of the network. This peer-to-peer network is used to complete tasks such as validation of transactions or updating the ledger.
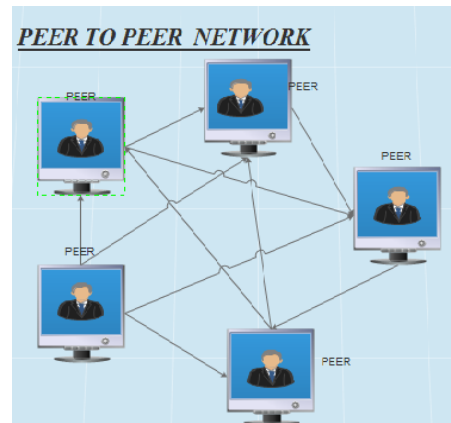

Figure 1 Peer-To-Peer Network Architecture

A hash is a way to store date of a size that is unknown or arbitrary into a fixed size. For example, suppose you have the string of text "Mary gave Joe $5" using the MD5 hashing algorithm the hash generated is 51f90f9fb8f4729724d3eb61f3b770b8. This might look unspectacular in this instance, but no matter how big the string of text is even if it was 1000 words it would still be able to be represented as a 32-digit hexadecimal number. In addition, every string of text generated has a unique hash there cannot be a string of text that is different yet has the same hash. Blockchain not only hashes a given transaction, but it also hashes it with

the hash of the previous transaction. This allows all the transactions on the blockchain to be represented by one number.

Since blockchain uses consensus approval to verify transactions as legitimate it is vulnerable to what is called a 51% attack. Where a person or a group of people collude to own 51% of a network to do fraudulent things. During a time, they control 51% of a networks hash rate they can conduct fraudulent transactions or disapprove legitimate ones. As such, consensus algorithms were devised to further secure the blockchain.

Proof of Work

In Proof of Work, a complex mathematical problem that requires intensive computer resources must be solved for a person to introduce a new block in a process known as mining. A miner receives a monetary reward for his efforts. In this system, a 51% attack can only occur if someone owns 51% mining power. This makes the Cost of Attack (COA), which is oft associated with security, extremely high. For example, the most well-known cryptocurrency in the world Bitcoin which uses Proof of Work costed "$1.4 billion" to attack in 2018 (Moos, 2018). Proof of Work by its very design necessitates the expenditure of a lot of energy to ensure security of the system. Bitcoin mining "consumed power at an annual rate of 32TWh" which is "about as much as [the country of] Denmark" (Lee, 2017). Due to this concern, an alternate consensus system in Proof of Stake was born.

Proof of Stake

Proof of Stake relies upon choosing stakeholders as validators based on wealth to propose new blocks. To be given a chance to be chosen as a validator one must stake a certain portion of his or her wealth in the currency. While staking the wealth they have cannot be used if they

validate a malicious transaction then they will lose their staked wealth. They are rewarded for validating transactions by given parts of the network fees. In this system to carry out a 51% attack someone must own 51% of the currency. This makes the Cost of Attack high because market forces dictate that anyone which tries to by that volume of currency will need to buy it at an exorbitant price. In addition, having those with a lot of wealth in the given currency means that they have extra incentive to be good actors. Proof of Stake is much more energy efficient and faster as Proof of Work was designed for it to be difficult to validate a new block. This makes it used in the particular use case of social media over Proof of Work. Particularly relevant in the decentralized social media circle is Delegated Proof of Stake (DPOS) in which instead of every holder of the currency being able to validate, holders of the currency can choose delegates to be the new validators. Below in Figure 1.1 is a visual comparison of Proof of Work and Proof of Stake.
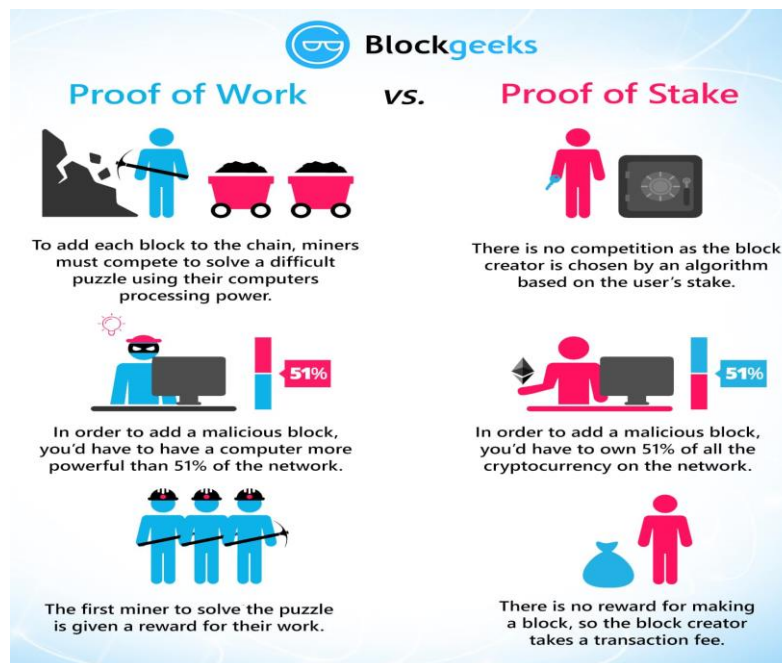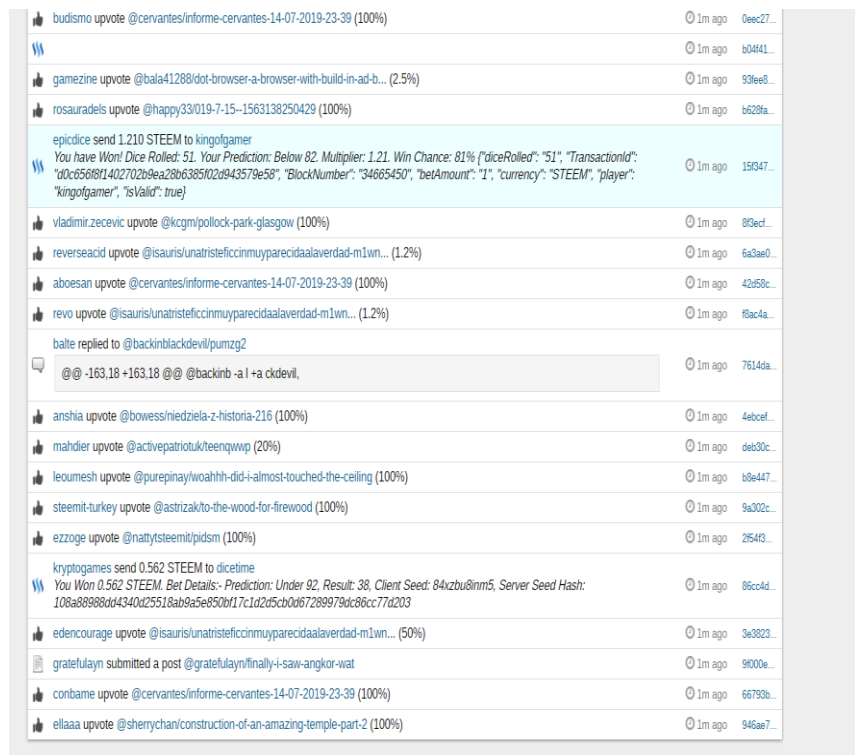

Figure 2 Proof of Work vs. Proof of Stake

How the Platform Would Operate

Back-End

The blockchain functionally is the back-end in a decentralized social media platform which incorporates blockchain technology. It replaces what would be a centralized database. On the blockchain rests users' posts, comments in response to a given post, and upvotes all sort of information and data which one would typically expect on a social media platform. In figure 3 is an example of a block within the Steem blockchain which is the blockchain behind the Steemit social media platform. As you can see upvotes, post, replies, and even the currency transactions with the Steem token are recorded. The information is not presented in any sort of appealing way and all the information is just presented as the most recent transaction. Also, interacting with and viewing the blockchain are

Figure 3 Steem Block Example

harder tasks then we expect social media users to complete. As such, a front-end for the social media platform is necessary.

Front-end

Because the blockchain is public there can be many different front-ends technically the picture in Figure 3 is a front-end, granted one that is intended to view and explore the blockchain itself rather than make it into a full-fledged social media site. The front-end website allows people to easily make interact with the blockchain, presents content in an ordered visual manner, and assists users in content discovery with trending topics, searching, and recommendations. In figure 4 you can see the homepage of SteemIt.
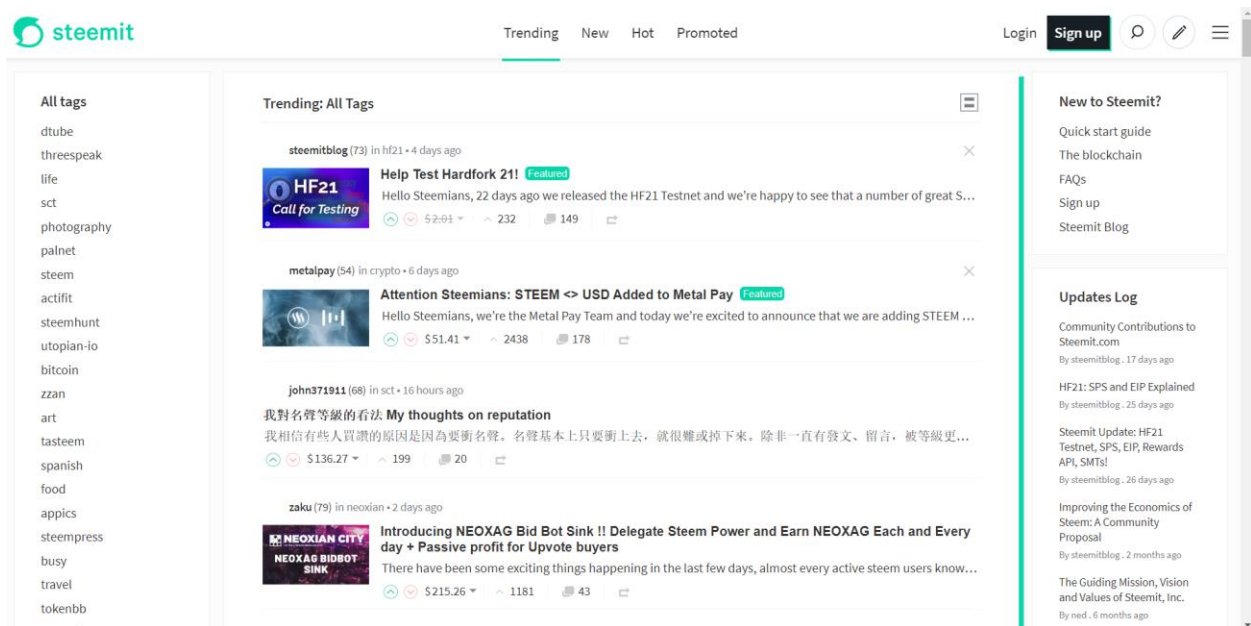

Figure 4 SteemIt homepage

Quite the contrast to the block view you can see trending posts, tags for certain topics, sign-in button, a search button, a post button, how many comments or upvotes or money a post made.

Rewards Pool

This a topic which will be expounded upon later, but since Figure 4 displays how much money a given post made it would be appropriate to introduce it here. Although blockchain can be used in various scenarios, the best use of the blockchain currently is in cryptocurrency which is a digital currency. As such, it makes sense for blockchain social media companies to create a digital token associated with the platform that they use to incentivize user-content by paying their users via a reward pool. Users that generate content that is popular are rewarded with more of the digital currency which creates an incentive to make enjoyable content on the site. Users may also be able to tip their favorite content creators as well. A lot cryptocurrencies use small transaction fees as a way to combat spam, but since in this use case since it is a social media site companies have to get more creative or provide an alternate centralized system for feeless transactions.

Feasibility

Scalability

Scalability is one of the most talked about factors within blockchain traditionally as it is presented as its biggest challenge. The reason for this is simple as blockchain traditionally requires all nodes in the network to vote in order to validate a transaction. Thus, the time it takes to validate a transaction is directly proportional to how big the given blockchain's network is. There are ways to make blockchain scale; however, most notable is limiting the pool of nodes involved in validating a transaction. This is what makes a Delegated Proof of Stake (DPOS) system so efficient and scalable. A much smaller group of chosen delegates is used to validate transactions. This is analogous to a direct democracy versus a representative democracy like we

have. Imagine if we had to convene a national vote whenever we needed a new law or for the government to take some action it would be costly and slow. Steemit, the decentralized social media platform mentioned early, uses a DPOS consensus algorithm which is capable of up to "10,000 transactions per second" (TPS) which is considered very good for a blockchain (Steem, 2018). There's a blockchain called "Futurepeia" which is capable of "300,000 transactions per second" (Mushtaq, 2018).

The real question of scalability is whether a blockchain-based platform would be able to keep up with the current social media giants either currently or soon. There is lack of full data in order to make a comparison due to the closed nature of pre-existing platforms. In the Steem white paper, they also mention that if Reddit were using blockchain it would need around "250 TPS on average as reddit's users make "23 comments per second", "220 votes per second", and "2 submissions per second on average" (Steem, 2018). Steem's transactions per second are well-above that. Twitter has on average about "6,000 tweets per second", but had an incredible peak of "143,199" tweets per second (Sayce, 2019). That is not something that would be remotely easy for a blockchain to match and that's not including likes or retweets as well. A social-media blockchain likely has other transactions as well such as currency transactions, tips, and reward pool payments. With the inconclusive data that is available it is reasonable to conclude that a well-designed social media platform built on blockchain will be handle to handle most likely the average scale of the very large social media sites that exist currently. Although it would struggle to keep pace with the absolute peak of such platforms. At the very least, it will not make the platform unfeasible and it will be able to handle a lot of users. Blockchain-scaling is something that has constantly improved over the years and will continue to in the future.

Legal Compliance and Regulatory Challenges

Blockchain faces some challenges from a legal and regulatory perspective. Many politicians dislike encryption and privacy because they believe it enables crime. The old "nothing to hide" mantra that many have heard before. One of the features of the standard currency is that it is easy to track which comes in handy for those committing crimes. That is why criminal organizations must launder money. Cryptocurrencies powered by the blockchain can make it easier to go undetected when gaining or using money in illegal ways due to encryption. Digital fingerprints are always left so it is by know means a fail-safe way to do illegal things. Despite all of this, currently blockchain faces no legal or regulatory burden in almost all of the western world though Bitcoin, the most popular cryptocurrency, partially cracked down on throughout Asia and the Eastern world. Very few countries have outright banned it, however.

Blockchain-use in a social media platform is a bit different from within a cryptocurrency like Bitcoin. Unlike Bitcoin, a blockchain used for social media purposes is permissioned. Not everyone can make transactions, only users can. Thus, true anonymity is not afforded only pseudo anonymity much like the current pre-existing social media platforms. In addition, because it is permissioned technically it is not fully immutable like Bitcoin. The blockchain can be hard-forked and transactions can be made invalid for example if the transaction was illegal. This is not necessary though.

Many people have tried to proclaim that if a blockchain contains illegal content such as say child pornography then the users of that blockchain are criminals because users of the blockchain will have a full or copy partial of the blockchain and the immutability of a given blockchain makes it impossible to remove that content. Luckily, this is not how the law works

Mens Rea is a legal principle which first year law students learn. Mens Rea, intent, along with Actus Rae, the act, are the necessary components for something to be a crime. One might recall the Latin phrase which such terms derive from: actus non facit reum nisi mens sit rea. Which translates to "the act does not make a person guilty unless the mind is also guilty." Furthermore, the whole reason we have a legal system is to deal with circumstances like this a judge would never make a ruling that would make hundreds of thousands of innocent blockchain enthusiasts into hardened criminals. Common sense and practicality are principles that factor into legal rulings as well. Although it may seem easy to see look at a blockchain given the fact a screenshot was posted of a block on the Steem blockchain earlier in this report that is only because someone wrote a web-based front-end called a "block explorer". The front-end used to display transactions in the blockchain can easily censor or remove illegal content. That is indeed what current front-ends like Steemit.com do. Someone would have to write their own script or program even view any transactions on the blockchain at minimum.

Currently there are no major legal or regulatory challenges poised to a blockchain social media platform right now. There is certainly a risk of future laws and regulations and how a given platform would be able to adapt is unknown. It would be fair to note that there is also a risk of future laws and regulations regarding the current social media giants due to concerns over algorithmic manipulation, privacy abuse, and other things. CEOs and executives of companies like Twitter, Facebook, and Google have been asked to appear for congressional testimony many times as of late.

Monetization Schema

There is nothing that necessarily prohibits a decentralized social media platform from monetizing its platform in the same way that current social media companies do. With the platform being open-source and transparent that would exclude shady data mining and selling; however. The immutability of the platform may make it hard to attract big-name advertisers who advertise on only on "advertiser-friendly" platforms. The best monetization system there is for a decentralized social media system is a form of in-house advertising system where users can spend to boost their content or voting power on the social media platform. Companies who created the digital token associated with the platform usually hold large swaths of the token. When social media platforms gain prominence, the currency shoots up in value by large amounts. This is analogous to how growth-based companies like Amazon became so rich via the stock market by focusing on growth despite technically losing money every year.

Advantage and Disadvantage Comparison

Decentralized social media platforms have both advantages and disadvantages over current social media platforms. The biggest advantage and ultimate reason for decentralized social media platforms is that they are transparent and free from worries of algorithmic manipulation, privacy abuse, or censorship. A user is not required to trust the company behind a decentralized social media platform to act appropriately. The biggest disadvantage is scalability. Although, decentralized social media platforms can handle a lot of users they would struggle keeping up with the peak usage of current social media platforms and performance would dip. Meanwhile we have not really seen near the limit of current social media sites they handle peak usage with ease. Another big advantage over traditional social media platforms is the way they're able to incentivize users to contribute to the platform with good content. The only other

social media platform which tries this is YouTube. Making high-quality YouTube videos on a regular basis is a very hard process that is basically a job. Also, monetization only applies to the thin sliver and ever-shrinking content believed "advertiser-friendly." YouTube content creators are still underpaid and exploited much like the users of other social media platforms. A disadvantage of decentralized social media platforms is content discovery. Although it is possible to track user's activity on the platform and make recommendations based on that it would go against the spirit of the platform and upholding privacy. Traditional social media also hold an edge in monetization as selling user data, while unethical, is incredibly profitable. In theory, decentralized social media platforms should be less costly to run since they are distributed and thus part of the cost is distributed as well.

Conclusion

Overall, decentralized social media platforms are a feasible avenue which address some of the concerns held with current social media platforms such as privacy abuse, algorithmic manipulation, and censorship. Decentralized social media platforms even hold some advantages over current social media platforms such as incentivizing users to post good content, cost to run, and transparency.

References

Kang, C. (2019, July 12). F.T.C. Approves Facebook Fine of About $5 Billion. Retrieved from

https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html.

LaForgia, M., & Dance, G. (2018, June 5) Facebook Gave Data Access to Chinese Firm Flagged

by U.S. Intelligence. Retrieved from

https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-

china.html

Lee, T. (2017, December 6). Bitcoin's Insane Energy Consumption, Explained. Retrieved from

https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-

explained/

Moos, M. (2018, November 29). Analysis: Bitcoin Costs $1.4 Billion to 51% Attack, Consumes

as Much Electricity as Morocco. Retrieved from https://cryptoslate.com/unregulated-

okex-derivatives-impacting-400-million-in-trades/.

Mushtaq, M. (2018, December 10). Top 5 Fastest Blockchains w.r.t TPS Speed for 2019.

Retrieved from https://medium.com/futurepia/fastest-transaction-speed-mainnet-

2eb3799bbed2.

Newberry, C. (2019, March 5). 130+ Social Media Statistics that Matter to Marketers in 2019.

Retrieved from https://blog.hootsuite.com/social-media-statistics-for-social-media-

managers/.

Sayce, D. (2019). Number of tweets per day? Retrieved from https://www.dsayce.com/social-media/tweets-day/. Steem. (2018, June).

Steem an Incentivized, Blockchain-based, Public Content Platform [White Paper].   Retrieved from https://steem.com/steem-whitepaper.pdf.

.