Decentralized Social Media in Blockchain

Muhammed Said Kaya
Department of Computer Science
Hacettepe University
Ankara, Turkey

Harun Alperen Toktaş
Department of Computer Science
Hacettepe University
Ankara, Turkey

İsmail Ateş
Department of Computer Science
Hacettepe University
Ankara, Turkey

Oktay Uğurlu
Department of Computer Science
Hacettepe University
Ankara, Turkey

1 Introduction

Throughout the period from the beginning of the world to the present and future moments, humans have been living beings in an effort to socialize by nature. In researches, people have expressed the concept of language for their singular characteristics that distinguish them from other living things. We can verify the accuracy of this research by the constant desire of people to interact. As a result of the development of language skills resulting from this desire of people, the communication revolution has been replaced by social media environments. At the beginning of the process, the telegraph, radio, and television used in communication left their places to the internet. The most important thing that distinguishes the internet from other communication assets is that people can add content and get instant response in this process.

Internet and social media usage is increasing in the world. Today, people use the internet network as an environment where they can do research, carry out their professional activities rather than use it only for communication and communication purposes, by distributing content and earning money in return, for shopping, advertising, and similar purposes. The fact that the internet is easily accessible and its cost is low are also factors in people's preference for companies. For example, some companies that care about the use of this internet network in the advertising sector can achieve more goals than large companies. In this way, they benefit from the ability of social media to reach large audiences compared to traditional media tools.

In this paper, the concerns of the privacy problems created by the social media ecosystem and the internet platform and the solutions that can be offered for these problems, and the Blockchain technology required for these solutions are emphasized. By analyzing Social Media platforms that have already been created using Blockchain technology, a model for the solution of existing problems is presented.

2 Traditional Systems

2.1 Problems in Traditional Systems

In the digital age, the use of the internet and social media platforms, where all data is stored in a central unit, brings many conveniences to our lives, as well as some drawbacks and problems. Information is rapidly spreading on social media and the fact that the information loses its accuracy in this

Fig. 1. Facebook Data Sharing Scandal[5]

rapid distribution and the resulting loss of accuracy of the social media analysis that can be made, and also the fact that some social media companies care about the data belonging to the end-users, the ownership of the users on the data can be shared with third parties and companies and the end-user The fact that the data is not deleted from central units despite being deleted by the internet and the use of this confidential data and the suggested advertisement content are the privacy problems caused by the internet and social media.

2.2 Internet - Web 2.0 - Web 3.0 / History of Traditional Systems

It is necessary to take a look at the history of this network in order to understand how the internet network in the digital age suggests advertisements by using the private data of the individual and the problems of keeping all data in a central unit occur.

The Internet, also known as the World Wide Web (WWW), was invented by Tim Berners-Lee in 1989 and has achieved a huge breakthrough compared to the communication resources of the era, radio, and television. The usage area of the Internet was contented with military affairs at the beginning of the process. However, the ease of communication and data storage caused the large mass to turn to them due to the low cost of long-distance calls to servers in other parts of the world. As the World Wide Web became popular, desktop applications such as CompuServe and Prodigy used in the previous period gave way to web-based applications. The Internet has become a unique platform with the mobile communication devices used in wireless communication following this system.

In the age when the Internet emerged, the end-users' purpose was to make more research and to use the Internet as a step in the process of accessing any information and data. However, in this digital age, as we have mentioned before, as a result of people's desire to communicate, which is a requirement of their nature, they have made people participate in this network and produce content.After exceeding the threshold required for the Internet to remain an unchanging and always usable technology that has not lost its importance, the Web 2.0 label has become new and the complexity rate of the information it contains has increased. In this process, people would now be able to use the Internet not only to search for information and do research, but also as an environment where they could interact, upload and share their own content. This situation necessitated the singularity of the entities loaded into the system, with each entity having its own address, and in this way, people would be able to perform more comfortable inquiries for these data.With the revolutionary features that Web 2.0 provided to the Internet network, progress was made. Day by day, the complexity and growth of the data held by the Internet caused unnecessary data stacks. The fact that these data can be made meaningful has caused humanity to meet Web 3.0, a new version of the Internet. The fact that meanings can now be deduced from large-scale meaningless data has caused this version to be called the semantic Web. The ability to make sense of data has offered new approaches to new sectors. The suggestion system that could be used in the advertising industry could be made from people's own information scanning and history. This situation revealed the privacy and data privacy situations and problems in social media, which is the reason for mentioning this content.

Today, social media platforms that keep data belonging to their end users in a central unit do not see a problem in analyzing people and sharing these data with third parties, regardless of privacy and control over data. This situation necessitated the creation of liberal platforms where people can control their own data. The fact that everyone participating in the system provided by the blockchain technology has an equal right and the anonymity it provides, is the reason to be preferred during the creation of social media platforms.

3 Blockchain Technology

Blockchain, under the name of blockchain, consists of interconnected blocks. All data are kept in these blocks. Blocks are the structures that make up the chain in blockchain architecture. The blocks are linked and join each new incoming block chain by connecting the previous one. Blocks are structures that contain all transactions and ensure the security of transactions. For this reason, there are control areas inside them that provide all this security.A Block consists of a Block Header and Transactions that define that block and contain its summary. Blocks contain their hash values and the hash value of the previous block they were linked to. Each block is linked to the previous block and added to the blockchain. The starting block of the chain is called the genesis block. The first block is not linked to any block.We can compare hash to a fingerprint. . Hash method indestructible and unpredictable encryption of data given to it. We can basically understand the word hash as encryption or scrambling. Hashing of a message can be thought of as its encryption.When we pass a message or a data through the hash function, when we apply the hash operation, we eventually have an encrypted data and it is not possible to reach the message using this result value. Even if a character changes in the message, the hash changes completely. That's why it's a good way to compare two very long messages with their hashes.The hash of a message is always the same. In other words, the message returns the same result every time it is hashed. In short, the hash value is the proof of the integrity of the message we have. When a block is created, its hash

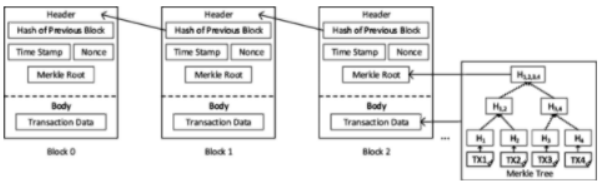


Fig. 2. Block Structure

is calculated. Changing something inside the block causes its hash to change. In other words, hashes are very useful when you want to detect changes in blocks. Since each block contains the hash value of the previous block, these blocks form a chain and are very reliable. If we interfere with any block from outside, it will cause the hash value of that block to change. The hash value will cause the changed block to mismatch with the hash value of the previous block in the following block, and the chain will break. This is a sign for us to understand that the block has been changed. But today, since computers have high processing power, the

hash values of all other blocks can be calculated again with the changed block. There is proof-of-work to prevent this. This is a mechanism that slows down the creation of new blocks. The purpose of Proof of work is to provide a certain amount of 0 at the beginning of the hash value to the miner that creates the hash value of the block. Doing this requires considerable processing power, and the only way to do this is to find the nonce (number only once used) value by trial and error. There is a certain time limit for calculating the required proof of work and adding new blocks to the chain. This mechanism makes dealing with blocks very difficult because if you intervene in a block you will have to recalculate the proof of work of all subsequent blocks. Therefore, the security of a blockchain comes from the use of hash and proof of work mechanism. Blockchains also have one more way to secure themselves, which is that they are distributed. Although blockchain is perceived as a database at first glance, it actually has protocol features. In other words, blockchain data is kept in a database and there are copies of this database on multiple computers, and these computers are interconnected by the P2P network. So there is no center or server. All connected computers constantly keep an up-to-date copy of the Blockchain database. In other words, every full node connected to the network keeps the full copy that includes all transactions from the beginning. Blockchain is kept synchronized thanks to end-to-end computers connected to each other, that is, all changes on data are transmitted to connected computers and synchronization is ensured. In this way, it is clear that the blockchain will be better protected compared to keeping it in one center. Even if computers in one part of the world crash at the same time, the computers that survive due to this structure will keep the processes going.

4 State-Of-Art

As we have mentioned before, a large amount of important data accumulates in the hands of these centralized structures by marking the small boxes related to personal data privacy and security without being read by the users who are integrated into the system. It has been revealed that these centralized structures try to do social engineering by using the data they have for their own interests[1]. Learning the behavior of large communities and, most importantly, due to their misuse, such as misdirection of society towards certain ideas; It has been an inevitable necessity that systems with a distributed system (where data cannot be collected in a monopoly) and where users have a say about their own data.

In the first stage, these systems tried to find solutions for 3 basic problems. These are based on solving the problems of privacy of personal data, where and how data is stored and who has access to these data. The use of blockchain technology in solving these problems is a highly preferred method.

Blockchain, by its nature, has a technology that is far from the central structure (where all information is collected and stored in one place), and that can provide security and privacy. This is why blockchain is the technology that plays a key role in solving the problems that traditional social media has inherently.

These blockchain-based systems create a cryptocurrency-based economy for the information that users produce, share or publish within the system, while solving the problems arising from traditional social media structures. In this way, it tries to encourage users with a reward-based system by enabling users to produce content to integrate them into this blockchain-based system that allows users to express their opinions as they wish, rather than traditional media platforms. (Yes, you can be anonymous on Twitter, Facebook, Instagram etc. but they still have your data like your connection information, IP etc.) As a general structure, the purpose of these systems is to establish a decentralized, distributed system where people can share whatever they want, can message freely, and all kinds of data belong to them. SOTA (State of The Art) systems established for this purpose are as follows.

4.1 Steemit

Steemit is the first blockchain-based social media structure that is not connected to a single center, rewards its users according to the interest of the content they produce, and stores all kinds of information of its users using blockchain-based technology. Market capacity is currently worth 67,413,460 USD dollar [2]. With this value, it has a large share in blockchain-based social media applications.

As we mentioned before, blockchain-based decentralized social media platforms are economically supporting both their users, content producers and those who process the stored information in the chain with the cryptocurrency they create. In this way, the continuity of the system is tried to be maintained by creating an economy within the platform. First let's talk about how this economy works.

4.1.1 Steemit: Service as a Monetizer

Steemit offers its users the opportunity to earn money in 3 different ways. The first of these is the award given to the authors. If you, as a user, produce content, that is, a blogpost, and this content is liked and upvoted by other users, your content will both appear on the front page and be noticed by more people, and the system pays you a certain amount of money,(actually is mix I will tell about more next), for this content. The second prize is given to curators. When it comes to the curator, it is not necessary to understand something different, in fact, every user is a curator. Curators vote on whether posts will be upvote or downvote. This ensures system-wide control in terms of quality. There are a number of rules for the curators to take a share of someone else's post, and within the framework of these rules, the share they receive with Steem Power is determined.

The third prize is the producer award. This award is given to those who save all the information generated in the system on the block chains. Just as those who write transactions in bitcoin receive rewards, the same system is also valid here. One of the most important features of Steemit is the identification of the authors of these transactions, that is,

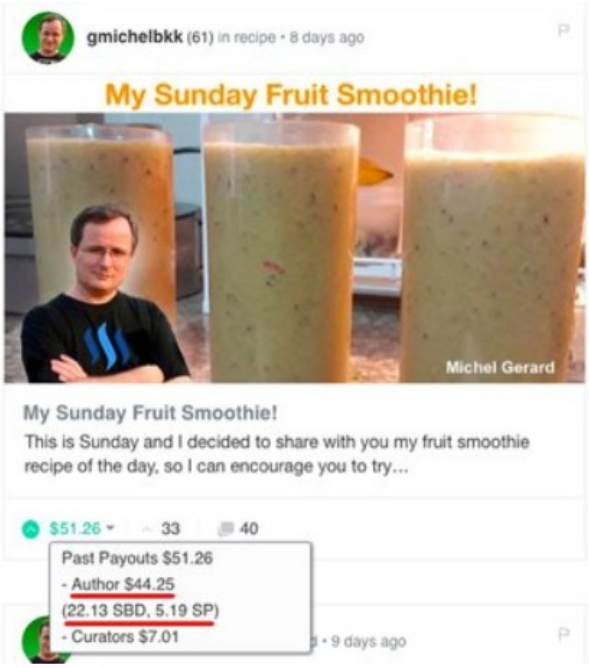


Fig. 3. A blog post example and Reward Share [8]

the structure of the consensus algorithm.

4.1.2 How System Works

As in every blockchain-based platform, the information collected about the system is processed in blockchain on the Steemit platform. However, since Steemit is a social media platform, unlike bitcoin, it generates more transactions per second (bitcoin: 7transaction / sec, GSP(general social media platforms): 5000 tweet / sec etc.).This situation creates a new system (DPoS) for processing the output produced faster.

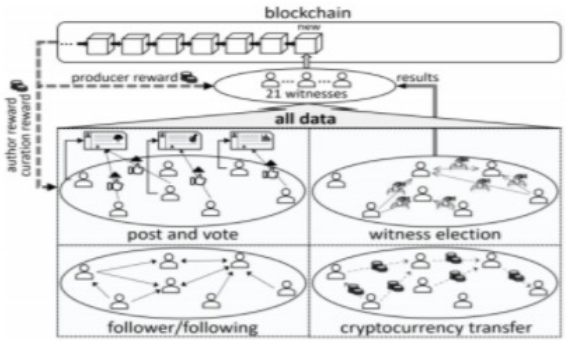


Fig. 4. How System Work Scheme [6]

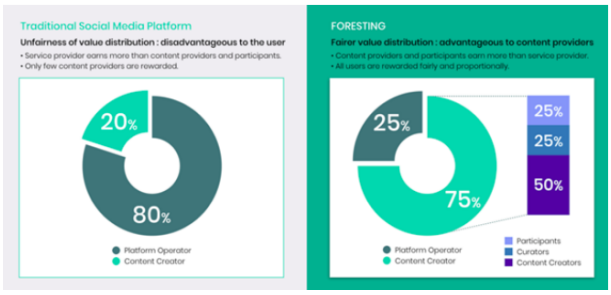
4.1.3 Witness election and DPoS

Users who produce blocks in the system are called witnesses. The number of these producers is 21 people in total. These 21 people are chosen by the vote of each user(DPos: Delegated Proof of Stake). Even though the system appears to be fair in its current form when directly observed from the outside, it contains major problems. Each user votes up to 30 people. We can pretend to say Yes for 30 people. Among these nominated persons, top-21 is selected as witnesses for production.

Here, the part that disrupts the democratic system allows the weight of the vote to be counted more when voting is cast for one person, if the voter has a greater share on the steemit.This allows large shareholders to keep their own people or the people they want in the producer chain and increase the profit they earn through the system.Although it tries to establish a system that is far from centralization, the distributed structure suffers with the increased value of the votes of large shareholders.

4.2 Foresting

The foresting project is one of the popular examples of decentralized social media which is started in early 2018. The system serves on the Etherium blockchain In the other example, the main motivation of this platform is that rewarding all participants for their activities fairly. The Foresting Network comprises three different blockchain services which are Foresting Platform, Foresting Bank, and Foresting Lab.



Foresting Platform: The Foresting Platform provides a public social content sharing platform. The participants can post in various content types, and the contents are joined to the currency evaluated by curators. After posting, the other users can upbeat or downbeat the contents by using their PICKs, which is kind of right to vote. In each day, only 24 PICKs are served to the users, thereby the usage of the bot accounts to get more upbeat are prevented. The upbeating is important in regards to the content creator since the creators earn Berry rewards that increase the content creator's level, also called Forest Interaction index (FI). Besides, the Berry rewards can be exchanged with PTON tokens. The PTON token is an Etherium based coin to be used in rewarding the content creators, curators, and any other participants. The total rewarding is served out 50In the Foresting, the content creators can choose any advertisement by themselves.

In this way, the funds come from the advertisement directly transferred to the content creators. Besides, the advertisement management on the platform can be managed by the content creators.
Foresting Bank: As an additional platform, Foresting Bank contributes to the creators and curators of the Foresting Platform. The bank provides a digital banking system for users who need financial support to create content. Here, the Forest Interaction index system takes a role to determine the user's credit ranking. The users increase their FI index posting contents with their activities on the platform.
Foresting Hub: The Foresting Hub is a support platform for innovative content creators who need technical support for their content ideas.

Different from the other distributed social media platforms, the followers can donate to the content creators by using their Berries, which is called Shooting. The foresting stores the data and functionalities on Ethereum blockchain. Each block that stores the content are processed by the proof-of-stake consensus algorithm and The Practical Byzantine Fault Tolerance algorithm. The stakeholders should put a value to the system to be part of the block creation by voting and gaining from this generation. Also, the consensus algorithm tried to improve the performance by decreasing eliminated blocks. Other outstanding features of the foresting is that master node-based P2P Transaction and real-time trade Function through Embedded Exchange. Master node-based P2P Transaction is the main feature of the foresting that uses the peer to peer approach for distribution. The master node takes role as load balancer, as optimizing the block generation by blocking the slower nodes and giving to nodes have more available. These master nodes are connected to the Foresting on the etherium channels such as state channels and payment channels. These channels provide peer to peer transactions on the Ethereum contracts. The management of coin access is provided by the RPC module which controls the coin access to the master nodes.

4.3 Sapien Network

4.3.1 Introduction

Despite the Blockchain idea came up in 2008, it is still used mostly in financial systems. However, It can be used for social media platforms to provide transparency, privacy, and equality among users who join the system.

The problems with traditional social media platforms are mentioned below.

Fake News: The studies at Stanford University shows that over 30 million fake posts have been shared in 2016. [3]. It is inevitable that people care about quality content without worrying about the authenticity of news being shared. Moreover, the recent advances in deep learning applications also resulted in generating realistic fake audio and visual data, which produces a serious threat to the transparency of journalism.

Unified Media Portal: Traditional journalism struggled to survive as advertisements disguised as insightful articles spread. Many news sites have turned to paywalls where users have to pay to access articles. The modern internet user may find it difficult to justify paying a subscription to access a single news source with such a wide variety of information feeds at hand.

Tokenizing Virtual Goods: Another consequence of the digital age is the supply of virtual goods. These goods have an isolated marketplace for exchanging. The authorities declaring the real value of virtual goods as isolated marketplaces cause financial and confidential problems.

4.3.2 Sapien Platform

A novel approach for social media supported by blockchain. Sapien is a partial blockchain-based communication platform that holds millions of content producers and people who are in the system and consume these contents together and transfer certain rewards, placing emphasis on democracy and liberation. It is based on the Ethereum Platform, so it uses Proof of Stake(Casper) consensus mechanisms.

Characteristics of Sapien Network

Privacy: While the personal Internet network brought by Web 3.0 technology is beneficial in terms of advertising and the creation of personal interfaces, the abuse of users used in the creation of interfaces for this person violates the concept of privacy. "We don't collect your personal data or track your click habits — we respect your privacy and digital autonomy," they said.[4]

Democracy: The requirement that everyone participating in the system have equal rights has existed so that those with greater ownership in the system cannot do whatever they want.

Customizability: One of the core features that Sapien Network offers to its users is that the system can be modified specifically for them. This situation causes everyone to have their own social experience.

4.3.3 SPN Token

Token(The cryptocurrency which is compliant with ERC-20 is a protocol that defines the standards and rules framework), which is used for any transactional work, powers the network, and encourages the users on the platform. There are two types of SPN tokens. The staked SPN tokens, bought during the crowd sale provides the functionalities such as posting and commenting of users on the platform and also rewarding. These tokens can be gotten while investing in a smart contract(ICO is a cryptocurrency version of crowdfunding) for nearly 12 months. In this duration, the user can not use the invested tokens. After these one year completion, staked SPN derives to an unstaked situation.

4.3.4 Reputation - Rewarding Mechanisms

In return for functional situations such as commenting and post sharing on the Sapien Network, an SPN token is rewarded. In order for these rewards to be received by the users, it is necessary to stake a certain amount of tokens on the Sapien platform. In detail, it is required to stake a token between 1-10 for voting, 10-100 for posting, 5-50 for commenting.If we explain the rewarding mechanism through the example, if a user bets 1 SPN token for voting for a certain period of time and the shipment is accepted by the system and is written to the chain, it will receive more than 1 SPN token.

A protocol named Feedback runs in the Sapien Network. With this protocol, the contribution value given by a user to the system can be presented and a decentralized reputation system can be created within the network. With this reputation system, users will earn reputation points based on certain parameters. Reputation in the system can be gained by evaluating a user's contributions to the system (commenting, voting, post sharing ...). A user must borrow some of his already existing reputations to be able to make a contribution. With the rule that a user's reputation score can only consist of numbers between -100 and 100, a solution to the disproportionate power problem within the community has been produced.

4.3.5 How Does Sapien Solve The Problems

Fake News: The reputation system in the system tries to prevent fake news sharing. With the little power of having a low reputation, it is ensured that the sharing is followed.

Unified Media Portal: Providing a blockchain-based system, they are able to access media content with crypto money.

Tokenizing Virtual Goods: With an environment where virtual products can be exchanged easily, people can easily exchange transactions without a third structure in between, and the sale of the desired product is allowed for the sale of any product.

4.3.6 Conclusion

On the Sapien Network, in order to be a more reputation user in the system, it is necessary to get contributions from reputable people so that the reputation score will increase. The proportionality of the token amount shared while posting, voting, or commenting with this reputation point creates the problem.

Below, the advantages and disadvantages of Sapien Network are listed.

Advantages

Data Transparency and Privacy
Token exchange (ETH, BTC, ...)

Disadvantages

Partial Decentralized Platform
Lots of verification for Bots(Sybill Attack)
Limited number of branches.

4.4 Minds

Minds is a social media platform that is open source and decentralized. For contributions to the project, users are compensated with Minds tokens. Minds seeks to create a new model for content creators to take back their rights, income and social influence from the internet. Today, Minds is a worldwide open source social network with around 1 million registered users. A utility token built with the Ethereum ERC-20 standard is the Minds token. The method of token distribution is ideally designed to grow autonomously with the creation and operation of the Minds network, ensuring that the ecosystem is equal and entirely dependent on user contribution. Minds tokens are not a currency or protection, but are a utility token used on the Minds social network to power services, including:

Boost: An advertisement network through which users trade tokens for content or channel views.

In the past few years, traditional social networks have come under media scrutiny with respect to advertisement fraud, manipulation of algorithms and disinformation. As fake news problems continue to make global headlines, it has become painfully clear that due to a number of factors - most notably, a lack of transparency - the traditional centralized social networking structure is being disrupted. To make the network as transparent as possible while preserving user privacy, Minds takes multiple measures. The code is hundred percent free and open source and accessible to the public, first and foremost. Secondly, with the introduction of smart contracts for key products such as Boost and Wire, Minds is shifting all of its advertising business onto the blockchain.

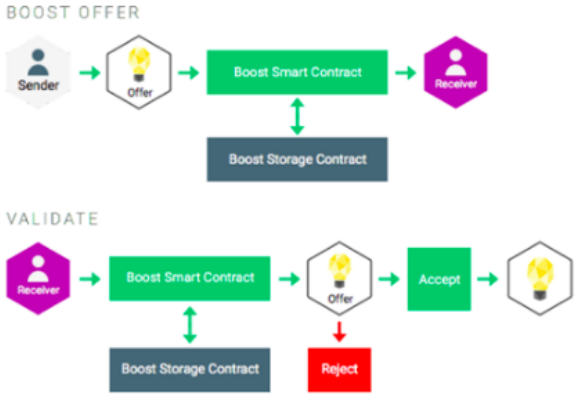


Fig. 5. Boost Context Diagram [7]

With a smart contract, each Minds token transaction will enable a direct, peer-to-peer relationship between advertis-

ers and content creators. This allows creators to own the relationship with their advertisers autonomously and removes any risk of interference or demonetization from third parties. The protection of a negotiated contract benefits both parties. Until the creator agrees to accept or deny, the advertiser will withdraw their bid. Upon accepting a bid, the creator would obtain their funds instantly. The advertiser will not be paid if the bid is refused.

Wire: A peer-to-peer payment system in which users exchange tips and content subscriptions with tokens.

Minds enables content creators to autonomously own the relationships with their donators and marketers without the chance of intervention by a centralized authority or service provider by using smart contracts for peer-to-peer payments. The possibility of demonetization is essentially eliminated because Minds tokens and the associated protocols are open source and platform agnostic.

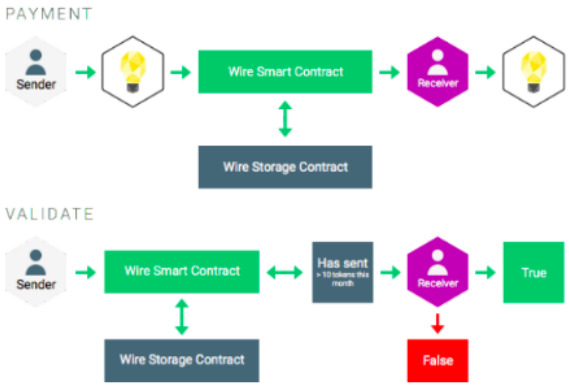


Fig. 6. Payment Context Diagram [7]

The related Wire smart contracts will store both the sender and receiver's wallet addresses, as well as the amount and timestamp for the particular transaction. In order for creators to monetize their content, wire can be leveraged in different ways.

Plus: A recurring monthly service that provides premium channel features, such as no ads.

Hosting: Build your own white-labeled social network using Minds source code

Affiliate Rewards: Third party affiliate program to enable distributed rewards for your business and customers.

Minds advantages can be listed as follows: ERC-20 ethereum based on token, it helps to exchange easily with other tokens. Open source improves the users reliability. Peer-to peer payment system without third participant. Tip, subscription systems. Premium to no ads. Enable users to build their own white- labeled social network. End-to-end encrypted messaging.User rewarding system. No filtering manipulation to content creator's posts reachs %100 followers. Ideologically neutral, as long as not illegal. Minds disadvantages can be listed as follows: Boot attacks can damage the reward system. Verifacation systems are not enough. For participants, they need to pay a fee to Mind to access reward system money the system depend on Minds Plus.

5 Compare State of Art

Günümüzde sosyal medya hayatımızın vazgeçilmez alanlarından biri.Hepimiz bu sosyal mecraya bir şekilde dahiliz.Ancak bu dahiliyet çeşitli problemleri de beraberinde getiriyor. Bunların en başında verilerimizin güvenliği yer alıyor.Kullanıcıların verileri sistemin kurucuları tarafından istenildiği şekilde kullanıyorlar.Biz de şöyle bir proje düşündük. Sosyal medyayı block zinciri teknolojisi ile birleştirerek dağıtık bir sistem üzerinde çalıştırmak. Bu sayede veri güvenliği sağlanmış olup,aynı zamanda da kullanıcıların ürettikleri içerikler sayesinde belirli bir reward alıp bundan içeriklerini paraya dönüştürme fırsatı elde ediyorlar.Biz de bu fikirden yola çıkarak merkezi olmayan bir blok zincir tabanlı bir proje geliştirmeye karar verdik. Burada ele aldığımız noktalar state of art modellerin iyi ve kötü yanlarını değerlendirip. İyi yanları alıp,kötü yanlarını gidererek bir model oluşturmaktan geçiyor.Bizde modeli oluşturmadan önce bu karşılaştırmaları yaparak çözüm üretmeye çalıştık.Ürettiğimiz çözümlerden proposed modelda bahsedeceğiz.Burada sadece problemler ve var olan modellerin birbiri ile kıyaslamasını yapacağız.

Sosyal Medya platformları monetizer olduğu için tokenlere ihtiyaç duyuyor,her sistemin kendi tokeni mevcut.

Örneğin en yaygın kullanılan Steemit platformunda kullanılan token yapısı Ethereum tabanlı değil,bu da exchange açısından daha yetersiz kalıyor.Diğer blok zincir tabanlı sosyal medya platformlarına baktığımızda(Sapien,Minds) exchange işleminin daha kolay olması için Ethereum tabanlı tokenlerin tercih edildiğini görüyoruz.

Bu tokenlerin oluşması tabii ki belirli kişilerin bu bilgileri bloklara işlemesi ile mümkün oluyor.Bu sistem içerisinde önemli olan bir noktada bu blokları üretecek olan kişilerin belirlenmesi ve blok üretim hızlarının tespiti.

Örneğin, Steemit platformu blokları üretecek kişilerin belirlenmesi için her kullanıcının istediği kişilere oy verebildiği Delegated Proof of State yapısını tercih etmiştir.Bu sistem herkesin oy kullanarak karara ortak olması bakımından güzel gibi gözükse de büyük bir problem barındırıyor.Bu problem verilen oyların eşit etkiye sahip olmamasından kaynaklanıyor.Büyük hisse sahiplerinin verdiği oylar daha değerli olduğu için bir tekelleşme mevcut. Bu tekelleşmeyi ve etkilerini güzel bir çalışma içerisinde toplamışlar.Orada da yapılan analizler gösteriyor ki,üstü kapalı bir şekilde büyük pay sahiplerinin zinciri üreten kişilerin seçiminde büyük bir etkisi var.Bu da ister istemez haksız kazanç sağlanmasına olanak sağlamış oluyor. Aslında benzer sistem diğer platformlarda da var,örneğin Sapien platformunda da itibar sistemi mevcut.Burada da kullanıcılar sistem üzerinde etkili olmak için belirli itibar seviyelerine erişmiş olması gerekiyor.Bu da itibarı yüksek kişilerin birleşerek merkezi bir yapı kurulabilmesine olanak sağlıyor.

Her ne kadar dağıtık ve tekbir merkezde toplanmayan bir sistem kurulmaya çalışılsa da sistemin efektif işlemesi

için bir şekilde kısmi merkezleşmeler ne yazıkki olmak zorunda kalıyor.

Zinciri üretecek olan kişiler kadar hangi grubun veya kişinin ne kadar zincir üreteceği de ayrı bir problem.Çünkü üretilen her bir blokta ,o sistemin sahip olduğu token ödül olarak verilirken işlenen her bir blok için fee alınmaktadır.Bu yüzden kimin ne kadar ürettiği önemli bir konu oluyor.

Her platform kendi sistemi için uygun bir model oluşturmak istemiş. Örneğin Foresting sisteminde load balancing yapısı mevcut,bu yapı blok üretim hızına göre üretebileceğiniz blok sayısını belirliyor.Bu sayede hem transactionların hızlı işlenmesi sağlanırken bir yandan da daha adaletli bir sistem oluşturmak hedeflenmiş.

Bu durum Steemit için ise daha farklı,blok üretimi round'lar üzerine kurulu.Seçilen tanıkların bu roundlar bitene kadar bloğu üretmesi gerekir.Bir load balance sistemi mevcut değildir.

Bir başka problem de Botlar.Blok zinciri tabanlı oluşturulan bu sosyal medya platformları kullanıcılarının para kazanmasını sağladığı için bir açıdan da gelir kaynağı.Bunu sömürmek isteyen kişiler de sisteme yüksek sayıda bot hesap ile dahil olarak kendi içeriklerinin öne çıkmasını sağlamaya çalışarak kazançlarını arttırmanın peşindeler.Bu bot saldırılarından tamamen sistemi kurtarmak mümkün olmasa da saldırıları en aza indirmek için çeşitli önlemler alınmaya çalışılmış.

Örneğin Minds platformu kullanıcının sisteme dahil olması için birden fazla kez authotentic olmasını sağlamaktadır.Sisteme aşamalı giriş ile bot hesapların işini zorlaştırmak istenmiştir.Steemit ve diğer sosyal medya platformları Recaptcha gibi sistemleri ile bu bot saldırılarını azaltmaya çalışmaktadır.Burada da en büyük zafiyet Steemit için oluşmaktadır çünkü yapılan çalışmada[[İncentivized]] curator reward larının yüzde 16 sı bot hesaplara gittiği görülmektedir. Bu da sistem için büyük bir zafiyet demektir.

6 Proposed Model Prudentia Decentralized Social Network

As a result of our state of art research and literature review, we determined the deficiencies of existing systems and put forward our own decentralized social media model. In this model, we decided to use the etherium-based blockchain system as seen in many models. With etherium business rules will be carried out with smart contracts.

The main source of motivation offered by our model to the users is the awarding system. All participants participating in the system have the right to produce content. This produced content is then submitted to the upvote and downvote of other users by entering certain contracts. As a result of the evaluations, it is presented to voters with the consensus algorithm, if 50% + 1 majority is provided, this post is written to the blockchain.

6.1 Lifecycle of a Post

As we mentioned before, every user has the right to produce content. Post is made available to all users. Users can access these posts by listing them in a certain order on the post listing screen divided into certain categories. The post created enters the appraisal contract. For 24 hours, users can rate the post and add comments with upvote and downvote. At the end of this 24 hours, the contract is voted on by the chosen voters according to the proof of stake consensus algorithm and the contract is terminated. As a result, the rewards are distributed and the block is added to the blockchain.

6.2 Reward Distribution

6.3 Consensus Algorithm

In our model, Delegated Proof of Stake method is used as the consensus algorithm in writing the blocks to the chain. According to this algorithm, the post after the evaluation is filtered by AI algorithms. 24 hours after the evaluation, these posts are sent to producers for the voting. Who want to be selected as producers apply to the system and investe a certain amount of money.This money can not be spent. The money given is deposited in the contract for the selection of the producer. In case of need, the producer is selected randomly, taking into some criteria. This criterias are listed as follows.

[

-] Producer candidate must have invested money in the system.The registration time of the producer candidate to the system. Size of the is time linearly proportional of the be chosen producer. The number of transactions carried out by the producer candidate in the system is linearly proportional of the be chosen producer. The number of a producer candidate being voter in the system is inversely proportional of the be chosen producer.

After being selected, producers who want to exit the system cannot take their deposited investment for 6 months. In this way, the producer, who will enter the system, is provided to take risks and it is ensured that the producer majority is kept above the required amount as much as possible. Producers who cause inappropriate content to be added to the chain are punished by seizing their deposits.

6.4 Prudent Token

In our system, the Prudent token, which we produce based on etherium, is used. This token, created with the ERC-20 protocol, keeps our own system's tokens in wallets thanks to the IDEX exchange (decentralized ethereum exchange) provided by the Etherium system. All monetary transactions on the system are transacted through Prudent.

6.5 Private Transactions

Instead of the lack of private transaction (private content sharing, private chatting etc.), which we have seen a lot of deficiencies in Proof of stake, we recommended a private conversation in our system. For private chat conversation, using the transaction manager as in Quorum, providing the

integrity of the data with encryption, decryption and hash with a symmetric key, it is ensured that two nodes communicate between themselves. The hash value of this data will be recorded in blocks. Thus, other users are prevented from reading this data, collision resistance with a hash algorithm. SHA 256 can be used.

6.6 Punishment of Harmful Content

6.7 Protection from Sybil Attack

7 Conclusion

This research study examines blockchain-based decentralized social networks. Compared to traditional social networks, analyzes and researches of non-centralized (distributed) applications were carried out. As a result of these analyzes, the main problems are that decentralized social media networks are open to monopolization, being partially centered, joining the system with too many authentication mechanisms against sybil attacks, and not having private chat environments in some networks. In this study, a decentralized social media platform model named Prudentia is presented to solve these problems. With this platform model, individual messaging is provided by cryptographic algorithms. Thus, personal data are protected in the chain. The most basic problems of traditional Social Media, data security, privacy and the like have been tried to be prevented.

References

[1]Facebook Cambridge Analytica data scandal. (2020). Retrieved 9 December 2020, from https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

[2]Steem price today, STEEM marketcap, chart, and info — CoinMarketCap. (2020). Retrieved 9 December 2020, from https://coinmarketcap.com/currencies/steem/markets

[3]Social Media and Fake News in the 2016 Election Web.Stanford.Edu, 2020, https://web.stanford.edu/ gentzkow/research/fakenews.pdf. Accessed 21 Dec 2020.

[4]"Sapien — Humans First". Sapien.Network, 2020, https://www.sapien.network/join.html. Accessed 21 Dec 2020.

[5]Google.Com,2020, https://www.google.com/imgres?imgurl=http://prod-upp-image-read.ft.com/42472134-2ea9-11e8-9b4b-bc4b9f08f381imgrefurl=https://www.ft.com/content/12fea2f2-2e87-11e8-9b4b-bc4b9f08f381tbnid=dBL1sK_EliO5RMvet=1docid=dJ1Ecnc4YgAk1Mw=2048h=1152source=sh/x/im. Accessed 21 Dec 2020.

[6]Arxiv.Org, 2020, https://arxiv.org/pdf/1904.07310.pdf. Accessed 21 Dec 2020.

[7]Minds.com White Paper. Available at: https://cdn-assets.minds.com/front/dist/en/assets/documents/Whitepaper-v0.5.pdf (Accessed: 21 December 2020).

[8]et al. (2020) Understanding Author Rewards Calculations — Steemit, Steemit.com. Available at: https://steemit.com/steemit/@gmichelbkk/understanding-author-rewards-calculations (Accessed: 9 December 2020).

A Resources

- Dergipark.Org.Tr,2020, https://dergipark.org.tr/en/download/article-file/1228631. Accessed 21 Dec 2020.
- "Understanding Author Rewards Calculations — Steemit". Steemit.Com, 2020, https://steemit.com/steemit/@gmichelbkk/understanding-author-rewards-calculations. Accessed 21 Dec 2020.
- "Steem Curator Reward System — Steemit". Steemit.Com, 2020, https://steemit.com/minnowsupportproject/@stephcurry/steem-curator-reward-system-2017625t214728825z. Accessed 21 Dec 2020.
- "Sapien-White-Paper".Github,2020, https://github.com/SapienNetwork/Sapien-White-Paper/blob/master/SPNv1$_2$.pdf.$Accessed$21Dec2020.
- WhitePaper.Minds.Com, 2020, https://cdn-assets.minds.com/front/dist/en/assets/documents/Whitepaper-v0.5.pdf. Accessed 21 Dec 2020.
- "When Blockchain meets Online Social Networks", www.sciencedirect.com/science/article/abs/pii/S1574119220300195, Accessed 21 Dec 2020
- "When blockchain meets social-media: Will the result benefit social media analytics for supply chain operations management?", www.sciencedirect.com/science/article/abs/pii/S1366554519315339, Accessed 21 Dec 2020