Web 3.0: The Decentralized Web Blockchain networks and Protocol Innovation

Conference Paper · April 2018

DOI: 10.1109/CAIS.2018.8441990

1 author:

Faten Alabdulwahhab
King Fahd University of Petroleum and Minerals
2 PUBLICATIONS **136** CITATIONS

SEE PROFILE

Web 3.0: The Decentralized Web

Blockchain networks and Protocol Innovation

Faten Adel Alabdulwahhab
Computer Science and Engineering department
Jubail University College JUC
Jubail, Kingdom of Saudi Arabia
Fatena42@gmail.com

Abstract— **The current web 2.0 is about connecting people. In which the social media platforms were invented, and the concentration of development was focused on the application layer. There are different approaches to think about web 3.0, some; would say the future is when we have a semantic web others would argue that the future is the virtual web. In this paper, we will talk about another direction to think about the future web called the decentralized web. To enhance the web, we should be concerned with solving the problems that we have and the problems that these platforms have created. The decentralized web is focused on developing protocols and the underlying technologies that are not noticed by end users. This paper gives an overview of the challenges in the current web 2.0. Describes the decentralized web, and what are the technologies that are in development now.**

Keywords-blockchain; decentralized; token model; protocol; web 3.0, data, internet

I. INTRODUCTION

The current web is typically called the social web. Because, it improved the web to a network in which people collaborate, communicate, and create content. This evolution in the web had significant advantages but initiated a lot of problems that need to be solved such as the loss of democracy because of the centralization of data. Internet censorship problems and also security threats since we are collecting vast amounts of data in one place. Before the blockchain networks, there were no protocols that support the decentralization of data Thus, causing all of our data to be collected by mega-platforms and owned by them. The decentralized web will solve this problem. And the token model will make sure that people invest in the development of protocols not only in the applications on top.

II. THE PROBLEMS IN THE CURRENT WEB

A. Loss of Democracy

Data are growing faster than ever before; Fig .1 shows that by the year 2020, our accumulated digital universe of data will grow to around 40,000 Exabyte [1]. All of the data that are being collected called big data. The meaning of big data is the large sets of information that are collected in every way possible and stored in databases. Big data are not limited to the information users enter when they log in to a website they include users location, their frequently visited restaurants and the calories they burned while running wearing fitness bracelets.

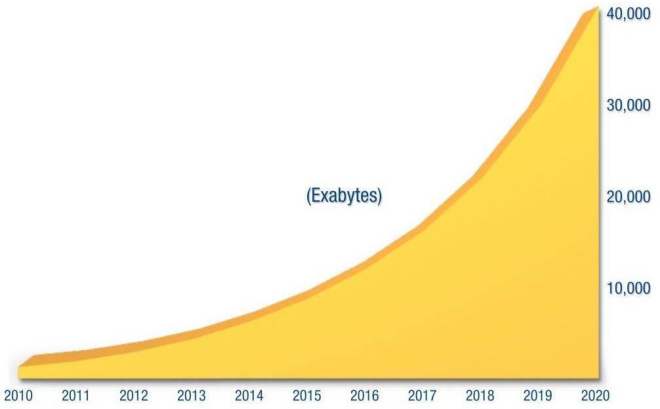

Figure 1. Expected data growth, 2010-2020

Big data are leading the way for future since they are needed for algorithm development and to improve artificial intelligence to provide better solutions, Big data are also sold to marketing companies, and they analyze the data the gain knowledge about how to present advertisements to the users and what ads are more profitable. The fact that data are collected from the end users without their knowledge or their ability to profit or have a choice about giving up their data is a loss of democracy. Moreover, Jaron Lanier has noted that "Big data and Artificial Intelligence are economic and political constructions that disenfranchise most people" [2, p. 34]. What is happening is mega-platform companies gave the allusion to the users that they have a great bargain since users think they are using these platforms for free. The reality is the users are losing the right to owning their data and their profit from what

978-1-5386-4427-0/18/$31.00 ©2018 IEEE

they generated since these platform owners are profiting without the users getting paid. Democracy is lost here not only the users are not benefiting but also if one of these platform shut-down the users' data will be lost since they do not own it in the first place. Not only the end users are harmed by this centralization of data, but also there is a lesser chance for competition since new upcoming business do not have access to the same data, and thus the mega-platforms have a head start on these new emerging companies since it is not an equal start from the beginning. This centralization of data has the net effect of centralizing wealth and power.

B. Censorship

OpenNet initiative in 2010 had documented Internet filtering by governments in over forty nations [3]. These countries filtering political, social, and security areas are limiting the freedom of speech. Censoring social media and limiting access to certain websites e.g., in 2010 China denied access to 1.3 million websites [4]. This limitation of access to some parts of the Internet in some countries is one of the major problems of the Internet today. Since countries can block websites by blocking the Internet Protocol IP address of the servers of these websites. The current web allows these countries to censor the access and limit the citizen's freedom.

C. Bandwidth

Centralizing our data into data centers and servers and addressing them using the location IP address is costly. Since if ten people are requesting the same file each one of them would require the same amount of bandwidth to retrieve the file which is slow, and it costs even if the file is available in the person's computer sitting next to you. This addressing using the server address to retrieve data consumes a massive amount of bandwidth, especially when requesting files over another content. This protocol that requires the location IP address is consuming the bandwidth which resulted in a slower connection.

D. Security

The web started decentralized, in which each person sets up their server and have the ownership of their data. But, this didn't last for long, and the internet shifted to a distributed centralized web in which vast amounts of data are stored in servers and data centers. This centralization provided a single or in the best case scenario multiple points of failure. Having all the data stored in when place increased the risk since hackers can attack a single entity and gain information about thousand other entities. Not only security threats are higher, but data corruption is also a problem if we are storing all of our data in one place if someone tries to corrupt the data or some system failure happened, and corruption occurred we would lose the integrity of large volumes of data.

III. The Decentralized Web

The inventor of the World Wide Web WWW Tim Berners-Lee said “The proposal is, then, to bring back the idea of a decentralized web. To bring back power to people” [5]. The solution to all these problems is the decentralized web. Blockchain networks are the technology that is leading us to the decentralized web and solving the current issues that are already available in the web 2.0. But, by just creating a blockchain we didn't create a new Internet. Blockchains by themselves have their limitations. A blockchain is the underlying technology that is implemented via different protocols such as Bitcoin, Neo, and Ethereum. Protocol innovation is booming in the decentralized web which is needed to solve the problems we have. The reason for the protocol innovation in the decentralized web is the shared data layer and the token model. First, we will explain the blockchain networks. Then, we will discuss what is leading the protocol innovation and how tokens incentivize protocol development and adoption.

E. Blockchain Networks

Blockchain network is a peer-to-peer P2P network that is built on trust-less transactions. In the blockchain, every computer (node) in the network has a copy of a shared ledger, and this copy is updated and maintained by all the nodes in the network. A transaction is not performed until it is added to a block that is linked to the blockchain. When a node requests a transaction, this request will be broadcasted on the network. And since the blockchain is built on trust-less transactions each node needs to verify that this request is from an authentic source. And to do so, a digital signature is produced using the message request and the private key of the requester. This digital signature is used by the nodes on the network with the public key of the source to verify that the message is from an authentic source. And since the signature depends on the message this means that the integrity of the message is ensured since no one can alter the message while passing it since any modifications to the message would invalidate the signature. Also, the dependency on the message not only assures that the message is not modified but also provides the benefit that the key cannot be known and used by someone else for a different transaction. Elliptic Curve Digital Signature Algorithm ECDSA is the algorithm used by Bitcoin for the verification of the authenticity without compromising the security [6].

This type of network is called a blockchain network because transactions are ordered into blocks that are linked to each other into a chain. After each transaction is verified using the public key, it is added with other similar transactions into a block. This block needs to be checked and confirmed so it can be linked to the previous block on the chain. The confirmation is done by using the collective computing power of the miners within the network to solve a mathematical problem that is irreversible by passing it through a hashing algorithm until a solution is found. Once the problem is solved the block is verified, and it is linked to the most recently verified block on the chain, creating a sequential ledger and then broadcasting the newly updated ledger to the whole network which is viewable by all the nodes. This method of grouping the transactions is done to avoid double spending problems, since the blockchain is built as a trust-less network you can’t trust that someone will not issue two transactions for the same resource. By grouping the transactions into blocks whatever transactions that are in the same block they are considered as if they occurred at the same time. Thus, when the next transaction to double spend is issued, and it is verified by another node that didn't receive the first transaction and

verified it this second transaction to double spend as an authentic transaction. It is still not executed since it is not yet added to the network, and when it is time for the confirmation of the block, it would be refused by the network since the resource has been used already. Thus, double spending is avoided using the idea of grouping.

This idea of solving mathematical problems to confirm the block and add it to the network could result in an end of chain ambiguity problem. If two blocks are confirmed at the same time, each node adopts the confirmed block it produced and broadcast it. And each node on the network builds on the block that it received first, and this will generate an ambiguity problem since there are different tails for the blockchain but this will be resolved quickly since the blockchain network requires that each node adopts the longest chain as the only option. In Fig .2 when three blocks are solved at the same time each one of them will use the block it generated and broadcast it. The node that will solve the next block first and link it to the network will result in the longest blockchain to be used, and the other two blocks are going to be dropped by the nodes using them and update their version of the blockchain to newest longest version. Therefore, the blockchain will be stabilized.

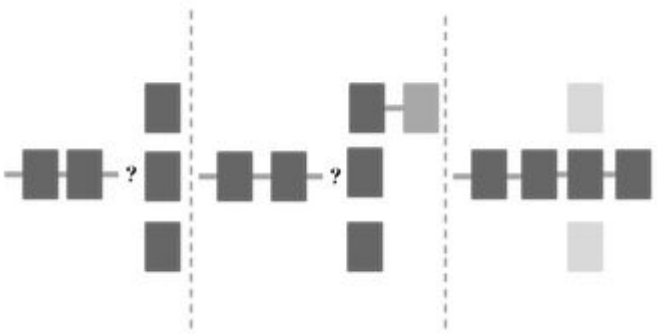

Figure 2. End of the chain Ambiguity problem

This race provides a great benefit for the network since solving the mathematical problem requires enormous computation power. The probability of solving blocks simultaneously is low; it's almost impossible that multiple blocks are solved at the same time over and over again [7]. And this race provides more security to the blockchain. If a hacker wanted to add an illegal transaction to a block, he needs to acquire 51% of the computing power of the network and would have to compete with the whole network to produce the longest blockchain so the corrupted block can be added. Which in theory can happen but in reality it is nearly impossible. Blockchains not only they provide more security since there is no single point of failure. But they also, solved the problem of democracy since every entity will remain the owner of its data and resources. The need for a middleman or a platform will be eliminated. In finances, this has already happened with Bitcoin and Litecoin. Blockchains are not only limited to the digital currency they can be used for social media and messaging systems and sharing economy just like Uber and Airbnb without third party involvement. The need for a platform will be eliminated, and the communication would be p2p. The idea of eliminating the middleman is useful since no one would be able to collect the data and thus, the users will remain the rightful owners of the information they produced in which they would be able to sell it if it is valuable for some company or decide what to do with it. But at the end, this is bringing the power back to the people to choose what they want.

F. Decentralized Protocols

The original Internet protocols such as HyperText Transfer Protocol HTTP that was developed by Tim Berners-Lee allowed for decentralized publishing. However, the Internet we have today is centralized even though HTTP allowed for decentralization. This is because HTTP is a stateless protocol, which implies that the state of the connection between the browser and the server is dropped once the transaction ends. This lead to the need for a data layer that will retain the state and this data layer was provided by platforms such as Google and Facebook. The centralization of the Internet happened because the original Internet protocols defined how data are delivered. However, not how they are stored, and this has lead to the centralization of data. In the decentralized web, blockchains provide the ability to build decentralized protocols with a built-in data. This means that blockchains provide a shared data layer that will eliminate the need for centralized data centers. The blockchain network is just like a blueprint that is implemented by different protocols that specify how the network should work and how the nodes can communicate and what are the rules for validation. Blockchain protocols examples are Bitcoin, Neo, and Ethereum. Each protocol has a shared data layer in which the data are stored in the users' computers and can be used between different decentralized application dApps that are built on top of these protocols. Resulting in a data layer that is used between different applications which is more efficient and the data would still be owned by the users, not on a server owned by the platforms.

G. Token model

Previous Internet Protocols such as HTTP, TCP/IP have produced a high amount of value. However, this value usually got captured in the application layer, and the people that implement and developed on top of those protocols are the ones that are receiving the high returns. This concentration of value in the application layer has lead to more developers focusing on the application layer since there is a low gain in developing protocols. However, this all changed after the blockchain networks. This change occurred because of the shared data layer and the token model. A token is just an abstraction. It represents owning an underlying tradable asset. Some example of assets in blockchains are the computing power in Ethereum, storage space in Storj, and transactions in Bitcoin. These tokens are called protocol tokens, and they incentivized protocol innovation. This is because tokens offer financial gain to the protocol inventors since they can monetize the protocol directly. This is done by creating a protocol and creating tokens that are native to that protocol and keeping some of these tokens for the developers to benefit

from them. If the protocol becomes popular, the value of the tokens will grow [8]. The creator's of the protocols will earn money based on the adoption and the use of their protocol and the amount of tokes they have retained. The higher demand for a token the higher it values goes. Token model is also helping in protocol adoption, since investors that bought their share of tokens would want benefit from their token and would want to raise its value. Hence they are more likely to use and develop on top of the protocols that they have invested on. Tokens align incentives between the developers, investors, and the users.

H. Overcoming Blockchain Limitation

Just implementing a blockchain protocol is not enough for a decentralized web. One of the limitations of blockchains is storage. To surpass this limitation we recommend using the InterPlanetary File System IPFS protocol. As described in the white paper "IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files" [9]. IPFS is a protocol that works by replacing the IP address that is dependent on the location of the document with a hash of the content to access it. IPFS solves the storage problem for blockchains by addressing large amounts of data with IPFS, and place the immutable, permanent IPFS links into a blockchain transaction. This timestamps and secures the content, without having to put the data on the chain itself [9]. Not only IPFS solves the storage problem, but also it saves bandwidth since it is a distributed content delivery in which it is a P2P delivery system. Thus, when trying to access a file using its content hash the nearest node with the file will respond and send the file to the requester. As demonstrated in [10] A p2p delivery system can result in bandwidth saving up to 60% over the traditional scheme. IPFS increases the security since the protocol against DDoS attacks and limits censorship since there is no specific address of a server to be blocked.

IV. Decentralized Applications Stack

Until now there is no specific defined stack to develop applications on the new web 3.0. But just like building a regular web application building a profitable decentralized application dApp requires computation, file storage, external data, monetization, and payments [11]. Table .1 summarizes some of the technologies that are being developed to replace the current centralized web 2.0. Not all of these technologies are perfect since we are still in the process of creating a new web. These technologies are still under development and experimentation. But it is feasible to build a profitable dApp using them.

TABLE I. Decentralized Applications Stack

	web 2.0	**web 3.0**
scalable computation	Amazon EC2	Ethereum, Truebit
file storage	Amazon S3	IPFS, Storj
external data	3rd party APIs	Oracles (Augur, Gonsis)
monetization	Ads, selling goods	Token model
payments	Credit Cards, Paypal	Ethereum, Bitcoin

V. Conclusion

Web 2.0 had its share of faults but, we have come a long way. Democracy was lost, and now we are on our way to restoring it with the help of blockchains. It was impossible to have a protocol with a shared data layer before the blockchain networks. And it was impossible to build a decentralized application. Still, there is a lot of work to be done before we reach a perfect state of decentralization. But now after the development of these technologies, we have protocols that provide value to their developers and protocols with a shared data layer. And most importantly, now it is feasible to build a dApp. More development is needed, and the community is working tirelessly to improve the state of the web and make it fully decentralized.

Acknowledgment

Thank you for the encouragement and support Dr. Ruchi Tuli, and Ms. Tabassum Sultana.

References

[1] "IDC Digital Universe Study: Big Data, Bigger Digital Shadows and Biggest Growth in the Far East Sponsored by EMC.", 2011.

[2] Lanier, *Who owns the future?*. London: Penguin Books, 2014, pp. 32-66.

[3] H. Noman and J. York, "West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011", OpenNet Initiative, 2011.

[4] Ghosh, "China Shut Down More Than 1M Web Sites Last Year", *International Business Times*, 2017. [Online]. Available: http://www.ibtimes.com/china-shut-down-more-1m-web-sites-last-year-298167.

[5] T. Berners-Lee, Tim Berners-Lee Keynote: "Re-decentralizing the web - some strategic questions". 2016.

[6] S. Driscoll, "How Bitcoin Works Under the Hood", *ImponderableThings*, 2013.

[7] M. D'Aliessi, "How Does the Blockchain Work?", *Medium*, 2016.

[8] A. Wenger, "Crypto Tokens and the Coming Age of Protocol Innovation", *Continuations*, 2016.

[9] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System (white paper)", 2014.

[10] K. Nguyen, T. Nguyen and Y. Kovchegov, "A P2P Video Delivery Network (P2P-VDN)", in *18th International Conference on Computer Communications and Networks*, San Francisco, CA, USA, 2009.

[11] F. Ehrsam, "The dApp Developer Stack: The Blockchain Industry Barometer", *Medium*, 2017. [Online]. Available: https://medium.com/@FEhrsam/the-dapp-developer-stack-the-blockchain-industry-barometer-8d55ec1c7d4. [Accessed: 12- Dec- 2017].