Netcash

Haroti Kotomana
12th December
Version 0.0.0 (draft)
(without citations)

Abstract: Current blockchain models are heavily restricted by their ability to scale effectively; Consequently, preventing them from ever achieving mass adoption and introducing a threshold on the amount of users that can use the network before it becomes ineffective. Furthermore, there is no cryptocurrency that is built on top of a blockchain with an effective protocol allowing for fully decentralised advertisement and monetisation. This paper will discuss both the technological and economical models behind netcash that allow it to effectively solve all three of these issues. Please note that the contents of this paper will get increasingly more advanced as it progresses. The first few chapters will try to help explain the basics and underlying aspects of netcash. If you wish to get a lighter understanding, it would be wise to visit "www.netcashio.com". If you are confident with the technology behind current cryptocurrencies then please read on.

1. Introduction

The increasing amount of attention and investment into cryptocurrencies has shown that there is a huge demand for decentralised technologies. In correlation with the further investments, an increasing amount of 'alt-coins' have been [and are currently being] developed and released. However, despite the increase in alternate cryptocurrencies, there has been very little development in regards to improving the underlying technology behind the protocols that allow for a decentralised system to work. For example, the issue of scalability; Bitcoin can currently do 3.88 transactions per second while Ethereum can do 15.2 transactions per second - a huge contrast in comparison to the 1388 transactions per second that VISA can achieve. If cryptocurrencies are going to be widely adopted as a medium of exchange then it is vital that the protocols for decentralisation are improved upon. Incorporating the minimal and few breakthroughs in decentralised technology that other cryptocurrencies have made in regards to this issue, the netcash protocol has a viable solution to the problem of scalability that renders the problem near, negligible. Solving the issue of scalability and increasing the speed of transaction times will allow for netcash to be widely adopted as a currency.

Currently, there are no cryptocurrencies that solve the issue of implementing a protocol that *fully* satisfy the requirements for advertising and monetising in a

decentralised way. Current issues of advertisement-based cryptocurrencies include; Implementing a protocol to securely ensure that the funds used to advertise are evenly distributed among the content creators, finding a way to allow for fair bidding to avoid centralised advertisement and implementing a way in which advertisements can be displayed on an app, site or dapp without the permissions of a third intermediary [the owner/admin]. Examples of content creators include; Artists, P2P file sharers, Spotify artists and many more.

Finally, most alt-coins in the industry of decentralisation fail due to the lack of a viable and practical economic model. For example, many cryptocurrencies that were intended to work with platforms such as, decentralised video sharing, decentralised file sharing, real estate tokenisation etc. reward average [consumer based] users with their currency. When looking at this from an economic standpoint, it becomes increasingly obvious that these economic models could *never* work in real life and were intended to 'look good' for investors. By rewarding average users with the currency, demand goes down significantly and devalues the currency from which the project is based. This is why it is important to maintain the scarcity of the token by making it difficult/impossible to earn and providing it with a substantial practical use in order to maintain its intrinsic* value. More alarmingly, a vast majority of cryptocurrencies never even mention or disclose their economic model. Netcash provides a model which helps to ensure, that as the project expands, each unit of netcash becomes increasingly rare and harder to acquire. Please note that, although it helps, deflation alone is not a good enough model to ensure scarcity. More information regarding the exact protocols will be discussed in further detail with each topic's corresponding chapter.

2. Hybrid Delegated Proof of Stake and Direct Acyclic Graphs

With scalability being, arguably, the most pressing issue of cryptocurrencies as of the current time period, it is important to address it first. Before beginning to solve the issue of scalability it is of utmost importance to understand what it means. By definition, scalability is; "The capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged to accommodate that growth". By this metric, we must look at the thresholds of current blockchain based systems that prevent it from being able to accommodate the potential growth with the required work. As a control variable (due to the fact that the majority of cryptocurrencies use a similar system) we will look at the blockchain based protocol that supports Bitcoin: The current thresholds or bottlenecks (whichever you prefer) that prevent Bitcoin from being scalable are: a) The fact that only one block can be confirmed at a time and that the blockchain is, by definition, in series. b) The fact that the amount of data that can go into each block is limited thereby, preventing a certain amount of transactions from being included in each block. Problem 'a' can be solved by either, increasing the speed at which each block can be confirmed to a degree where the confirmation time is negligible while still maintaining network security or, by changing the network protocol entirely so that block confirmations can occur in parallel. The latter solution is much more finite albeit, much harder to implement.

Proposed, are two protocols that can satisfy both solutions to a certain degree while interacting with each other and still being able to work on the same network. For bidding on the network, hybrid delegated proof of stake (HDPOS) is used. Hybrid delegated proof of stake is an entirely new system that aims to improve upon aspects of the original proof of stake system. It works by having a certain number of representatives of the network (nodes) being voted into power by the rest of the network. The number of representatives can be shown by x. The designated nodes that are voted into power then vote on the blocks to confirm. At regular time intervals of, let's say t, the network casts a new vote on who should be the next representatives of the network. The result, is a much faster and more secure protocol for consensus in comparison to regular proof of work or proof of stake. To help increase the incentives of the rest of the network to vote for the best possible representatives, the method for voting is divided into two sub-sections: Voting by proof of work and voting by proof of stake. Having a version of both allows for a much more distributed and fair voting model. Voters will also receive a percentage of the rewards that representatives receive through each block that the representative successfully votes for. By providing a monetary incentive, we can assume that there will be minimal bad actors on the network. In the event that a bad actor *is* found, the same logic will be applied *vice versa*. Voters who vote for a malicious representative will be punished by the network and have their funds locked. Malicious representatives will also have their funds locked and be removed from the list of representatives (x-1). HDPOS will not be a part of the main network but, will serve as part of the sub-section alongside a direct acyclic graph protocol (DAG). HDPOS will be used for the confirmation and filtering of bidders who wish to advertise through netcash. Further information regarding the use of HDPOS in the network and how it will be used in advertising and monetisation will be reviewed later in chapter 5.

For the main section of the network, a DAG protocol will be used. A DAG allows for the confirmation of transactions to be scalable to the degree where 1000's of transactions can be confirmed per second; A huge contrast to Bitcoin's mere 3.22 transactions per second. Using a DAG, users are incentivised to confirm a set amount of previous transactions by requiring that they perform a cryptographic proof in order to allow for their transaction to be eligible to be published to the network. To avoid confusion, it is important to note that, in the case of a DAG based protocol (specifically netcash), each transaction can also be referred to as a block. The optimal amount of Tx that each node should choose to confirm sits, rather comfortably, at the integer of two. Further information regarding the use of the DAG will be presented in chapter 4.

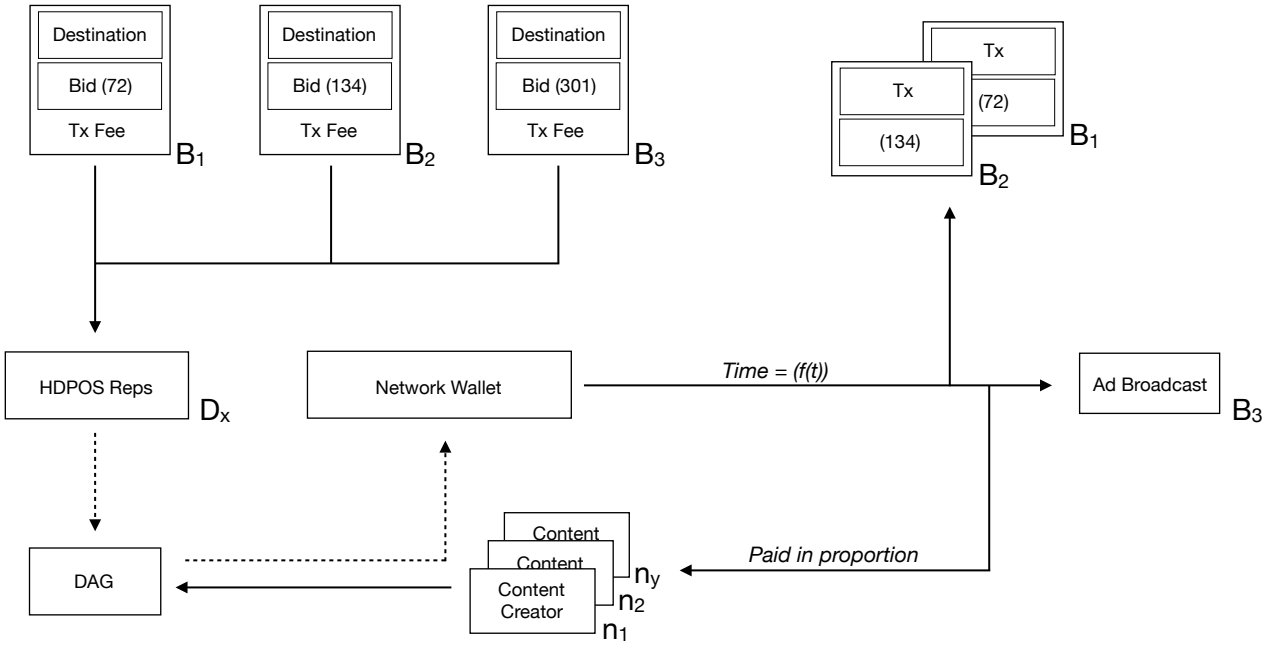
By incorporating the proposed systems, a generation three protocol is produced -generations one and two being the blockchain and smart contracts.

3. Feature: Decentralised Advertising and Monetisation

Current advertising and monetisation systems are heavily centralised - They favour the huge corporations that run them. Furthermore, the corporations that receive the necessary funds from advertising agencies, take a huge cut of the profits; Very rarely is it seen that these companies pay the producers (content

creators). For example, Spotify takes a huge cut off of the advertising funds it gets. It pays a small percentage of the money it receives from advertising towards the artists who make songs and drive traffic to the app. Netcash proposes a protocol whereby advertisers can bid on their place to have an ad displayed on a site, app or, dapp.

Advertisers place their bid and publish it to the public ledger of the network. For this, advertisers must pay a small fee. Once they have placed their bid, the funds in which they are bidding with are locked inside of a network wallet, from which nobody has access. After a set amount of time (f(*t*)) the network chooses the highest bidder's advertisement to be displayed on the given destination. The highest bidders funds (*i*) are sent and distributed accordingly among the content creators. The rest of the bidders funds, are returned to their wallets.



Once a highest bidder is determined (after f(t)) the advertisement is broadcast to the relevant destination. The process then restarts. Problems of this protocol arise from the fact that sending all of the advertisement data to the DPOS network would require a huge amount of bandwidth and would decrease the speed at which each block can be properly verified and confirmed. To counter this problem, advertisement data will only be sent to the DPOS network once the highest bidder is determined. This way, there is no need for all of the other bidders to submit the data and so the network can be as streamlined as possible. A DPOS network is necessary in order to ensure that the data of each advertisement is fundamentally correct and fulfils community [representative] standards. A DPOS system of verification for advertisements is much more robust and flexible when compared to a DAG based protocol. It also allows for the DAG to be as lightweight as

possible and prevents potential 'clogging' of the network from too much irrelevant data. All transactions will be confirmed and verified on the DAG model.

4. Further Details: Direct Acyclic Graph

The DAG will allow for the secure confirmation of transactions while still maintaining a high level of security. Currently, one could argue, that it is the best model for decentralisation thus far - It allows for a huge level of scalability while still maintaining the necessary features to prevent double spending and fraudulent transactions. To issue a transaction and spend a UTXO, users must first complete a cryptographic puzzle of [any] two previous transactions. The two previous transactions that are chosen are of a biased random - it favours the more recent transactions as oppose to older ones. The cryptographic puzzle must be of a relatively low difficulty in order to ensure that average nodes (smartphones, laptops, tablets) can issue transactions at an efficient and viable rate. With each new transaction, the network becomes faster and more secure. The chance of a double spend attack succeeding on a DAG based protocol is roughly, 0.0000114.

5. Economic Model

Finding a balance between the economic model and, the technological aspects of netcash was, by no means easy. However, while the technology behind netcash allows it to revolutionise the way in which currencies, advertising and, monetisation of current systems work, the economic model will ensure that a wide array of users can be reached and involved while still maintaining [increasing] the value of each unit of netcash.

By making a cryptocurrency that is finite in supply, netcash will ultimately increase with value as each new user is incorporated into the network (basic economics of deflation). In light of this, it is also important to note that netcash will only be long-lasting if specific use cases for it can arise. In the case of a currency, this means getting widespread adoption among merchants. Once this occurs, consumer adoption will naturally follow. In order to *maintain* and allow for successful *growth,* netcash must be scalable, fast and, secure - all of these issues are solved by the DAG protocol [see chapters 2 and 4]. Naturally, getting merchants to accept netcash as a medium of exchange is the hardest aspect. To help counter this, netcash already provides a secure utility use case for the currency; A tool for advertisements. As a niche in the, growing, decentralised industry, advertisement will not only propel adoption for netcash in its earliest days but, it will also serve as a long lasting purpose and use-case for the currency.

Furthermore, earning netcash is extremely difficult - it can only be earned in small amounts through the DPOS protocol. Because of the difficulty to earn netcash, the most practical way in which users can acquire it, is through buying it off of exchanges or selling items and merchandise for it. Again, this will help increase merchant adoption and help promote netcash as a *currency*. Overall, every aspect of netcash is ultimately there to solve the issue of user acceptance. By adhering to all of the issues, problems, and security issues that people may have when accepting a new currency, odds of survival and mass adoption can be dramatically increased.

6. Further Details: Hybrid Delegated Proof of Stake

In order to help maintain the security of the network while still keeping it as streamlined and practical as possible, a secondary protocol is introduced. The hybrid delegated proof of stake (HDPOS) chain is fully interoperable with the DAG chain. This means that two different use cases can be integrated into the system to split the necessary requirements of storage thereby reducing the required amount of necessary work by any amount in which advertising data is loaded; We can call this metric, (z).

Representative voters of the network are chosen through nodes voting by proof of stake *and* proof of work. In the case of proof of work based voting, nodes are required to solve a cryptographic puzzle and expend computing power and resources in order to cast a legitimate and accepted vote. In the case of proof of stake based voting, users stake a certain amount of netcash in order to cast a vote with the amount of netcash being staked resulting in a proportionate vote on the network. The amount of voting power in ratio of proof of stake to proof of work based votes will be 30:70. This ensures that the HDPOS protocol will be as fair as possible and helps to reduce the amount of centralisation of power on the network [like how we see on the majority of current blockchain based protocols].

Initially, the first use-case for HDPOS is to increase the speed and efficiency of an advertising-based feature. In order for a new feature to be added into the HDPOS system, such as, a social media based feature, >50% of the HDPOS nodes would have to update their software to accommodate. However, it is entirely possible for the network to adapt to other smaller use-cases. Small communities may even develop, and create nexuses for separate HDPOS protocols allowing for different features.

7. Conclusion

We have proposed a system that allows for much faster and more scalable transactions and blocks in comparison to current serial, blockchain based protocols. At first, we addressed the issue of scalability and speed by introducing a direct acyclic graph for proofs of UTXO and to prevent double spending. This allows for thousands of transactions to be accepted per second in comparison to the 3.22 tps of Bitcoin. Secondly, we were faced with the problem of integrating a work-efficient feature that didn't sacrifice any of the security or speed of the main network. The solution proposed was to incorporate two separate chains in unison [HDPOS and DAG] which dramatically reduced the stress on the DAG. Finally, we discovered a solution to the economic problem of cryptocurrency; Maintaining scarcity while still having an effective use-case and being adoptable by users in a scalable co-efficient manner.