THE UNIVERSITY OF WATERLOO

Faculty of Mathematics

Tokenomics

MealMe Inc.
San Francisco, California
Prepared By
Rohit Kaushik
4A Computer Science
ID: 20755173
March 15, 2022

Memorandum

To: Max Paulk

From: Rohit Kaushik

Date: March 15, 2022

Re: Work Report: Consensus Mechanisms in Blockchain Protocols

---

I have prepared the enclosed report on “Tokenomics”. This report, the fourth report that the Co-operative Education Program requires that I successfully complete as part of my BCS Co-op degree requirements, has not received academic credit yet. The world wide web is undergoing a paradigm shift today, with blockchain protocols growing in number and popularity. Tokenomics encompasses the supply and demand characteristics of cryptocurrency. A token is a digital unit of a cryptocurrency used as an asset or to represent utility on the blockchain. The most common types are security, utility, and governance tokens. We can predict how many coins will have been created in time due to their algorithmically pre-defined issuance schedule. Tokenomics introduces many game-theoretic ways to increase token value with time.

The Faculty of Mathematics requests that you evaluate this report for command of topic and technical content/analysis. Following your assessment, the report, together with your evaluation, will be submitted to the Math Undergrad Office for evaluation on campus by qualified work report markers. The combined marks determine whether the report will receive credit and whether it will be considered for an award.

Thank you for your assistance in preparing this report.

TABLE OF CONTENTS

Executive Summary		*... ii*
1.0 Introduction	*Intro to Tokenomics*	*… 1*
2.0 Analysis	*Characteristics of resource protocols*	*… 3*
2.1	*Resource-based participation*	*… 4*
2.2	*Tokenomics*	*… 5*
2.3	*Decentralized Service Provision*	*… 6*
2.4	*Blueprint for stake-based systems*	*… 7*
3.0 Conclusion		*… 10*
Acknowledgement		*… 11*
References		*… 12*

EXECUTIVE SUMMARY

This report on tokenization begins by introducing the notion of a token, and how it ties into a blockchain protocol. It describes the inherent value of these tokens and how they incentivize a community to maintain the protocol through rewards distribution among maintainers. It elaborates on the economic factors underlying a blockchain and how supply and demand of tokens can change the way users interact with the protocol.

There are four key characteristics of a resource-based service provider – resource-based participation, tokenomics, decentralized service providers and rewards distribution. Resource based participation involves sending tokens to a set of people, making them stakeholders in the protocol. Access to the protocol is granted by owning a resource, which can be proved in a plethora of ways like proof of work, stake, space, etc. The main characteristics are building systems with certain desired properties, using game-theory to encourage the system to hold desired properties in the future, and using cryptography to prove properties about the past, makes it tamper-proof. Decentralized service provision aims to ensure safety and liveness of the protocol, making sure the protocol behaves the same way for all users and that requests are handled in a timely manner. Finally, the report outlines, at a high level, the blueprint of a stake-based protocol.

The report concludes by summarizing the findings of the report.

1.0 Introduction

The blockchain movement has brought up several buzzwords like “cryptoeconomics” or “tokenomics,” but beneath all of this lie the human and artificial economic agents that must connect to produce, create, exchange, and communicate within a market (Lamberty et al., 2008). A token is a *thing* which serves as a visible, tangible, or intangible representation of a fact or a right. For example, a driving license card is a token which represents the fact that you are trained and allowed to drive a car (Lamberty et al., 2008). A cryptographic token is a secure, representation of a fact or right, which can be statistically proved and be processed in decentralized networks. They are multi-purpose instruments, ranging from simple-single to multi-complex designs. It could be value, stake, voting right, or anything. A token is not limited to one specific role or utility, it can fulfill a lot of roles in its ecosystem.

The combination of cryptography, game-theory, and market economics to create robust decentralized peer-to-peer networks is the foundational idea of tokenomics. Cryptography to prove events in the past, game-theory to design the interaction protocols that are interlinked with economic incentives to encourage desired properties to hold in the future.

The approach to achieve the tokenomics objective suggested by Nakamoto’s design is market based. The underlying digital asset of the system becomes a native digital currency that is required for accessing the service. The system also facilitates the exchange of the digital currency between parties and hence a market is created for the IT service. Moreover, its availability for public trading allows speculators to estimate the value of the service in the near

term and far future. At system launch, it is possible to have a pre-distribution of digital coins. For instance, digital coins can be “airdropped” to token holders of a pre-existing digital currency. In other cases, digital coins can be made available to investors in a “pre-sale” stage whereby software developers of the platform may use to fund the development of the software pre-launch (Kiayias, 2021). After system launch, additional coins can become available and distributed following a certain ruleset to the system maintainers. Such ruleset is public knowledge and algorithmically enforced during system maintenance. Depending on the system, the rate of new coin availability can be constant per unit of time, as in Ethereum originally, or follow some function per unit of time, as in the case of Bitcoin, which has a finite total supply and hence relies on a geometric series to distribute coins to maintainers. In some cases, the number of new coins that become added to the circulating supply depend on the behavior of the maintainers - in the case of Cardano, higher coin “pledges” by the participants increase the rate that coins become available. While the ruleset is algorithmic, enforced in the system “ledger rules”, it can be changed by modifying the software that supports the system, assuming there is wide consensus between the system maintainers to adopt the update (Ciampi et al, 2020). For instance the “London update” of Ethereum made the total supply of coins a variable function that depends on the transactions processed by the system.

2.0 Analysis

Consider a service which translates to a program ß that captures all the operations that users wish to perform. A resource-based realization of ß is a system that exhibits the following four fundamental characteristics (Kiayias, 2021):

- *Resource-based participation*: There must be a fungible resource that can be acquired by participants, possibly at a cost. Those in possession of this can exercise it to participate in the maintenance of the service.
- *Tokenomics*: A digital asset is used to tokenize the collective efforts of the maintainers and reward them. Such digital *coins* are maintained in cryptographic wallets and should be argued to be of sufficient utility to make system maintenance an attractive endeavor.
- *Decentralized service provision*: A user interacts with the service by submitting a transaction which is openly circulated in the network of maintainers provided it is well formed. Such well formedness may require the commitment of a sufficient amount of digital currency or other user expenditure to prevent spamming. The maintainers collectively take the required actions of ß needed for the submitted transactions in a consistent and expedient fashion while the system records their efforts.
- *Rewards Sharing*: The digital assets that the system makes available to maintainers are distributed to the active maintainers in a regular and fair manner so that the system's safety and liveness properties emanate from their incentive driven participation. Any property violation should be a deviation from an equilibrium state that incurs costs to the perpetrators, hence ensuring the stable operation of the system.

2.1 Resource-based participation

In classic distributed systems, system maintenance is offered by nodes that are authorized by common agreement (e.g., via public-keys that identify them) or by the network connections that are assumed to exist between them (Garav et al, 2020). Such configurations are commonly referred to in cryptographic modeling as setup assumptions. In decentralized networks, participation to contribute to the protocol execution is earned by possessing a certain resource. This is proof of resource, commonly referred to as *proof-of-X (PoX)*, where X signifies the resource. The two most widely cited such schemes are proof-of-work (PoW) and proof-of-stake (PoS). The case of PoW is exemplified in the Bitcoin blockchain protocol and is essentially a proof of possession of computational power (Nakamoto, 2008). Given the characteristics of the PoW algorithm, a specific logic or architecture may be more advantageous and as a result, maintainers may benefit from special purpose implementations. In such case, the PoW algorithm will not be a proof of general computational power, but rather a proof of ability to execute the algorithm utilized in the PoW scheme (Wood, 2014).

Contrary to PoW, a PoS scheme proves possession of a virtual resource (or currency). A significant distinction in this class of algorithms is that issuing a PoS has cost independent of the amount of "stake" in possession of the prover, while PoW typically incurs a linear cost in terms of computational power. Beyond stake and work, other types of resources, both virtual and physical, have been proposed and utilized. These include "proof of space", whereby the prover

demonstrates possession of storage capacity (Faust et al, 2015) and “proof of elapsed time”, supported by Intel SGX, whereby the prover demonstrates that certain wait time has elapsed, just to name two examples.

2.2 Tokenomics

Tokenomics applies game theoretic mechanism design in combination with cryptography to create robust decentralized P2P protocols. The main characteristics are the following:

- Building systems (networks) that have certain desired properties.
- Using game-theory and economic incentives to encourage the system to hold desired properties in the future.
- Using cryptography to prove properties about the past, makes it tamper-proof (Lambert et al, 2008).

Tokenomics requires a deep understanding of cryptography as well as game-theory. The cryptography underlying these systems is what makes the P2P communication within the networks secure, and the game-theory is what incentivizes all actors to contribute to the network so that it continues to develop over time. The incentive mechanism is designed to make the network fault tolerant and attack-resistant. This allows entities who do not know one another to reliably reach consensus about the right state (Buterin, 2017).

Tokenomics can now be used to properly design efficient markets. This means, protocol and incentive mechanism design aligns stakeholder interests to create more efficient markets. Each participant acts "selfish", that means, from his or her local point of view profit maximisation.

Game theoretical mechanism design ensures that the system properties result and that the individual players do not benefit disproportionately (Poddey et al., 2019). Cryptography is a linear component in the equation, whereas game theory forms a more complex exponential component.

2.3 Decentralized Service Provision

Decentralized implementations of services should provide both *safety and liveness*. For safety, the system should be consistent in the way it processes requests. In other words, despite being realized by a variable number of system maintainers, the effect of a certain valid input should never be incongruous to the effect that the same input would have if it was applied to ß. A safety violation for instance, would be that a user submits two mutually exclusive inputs, i.e., inputs that cannot be both applied to the state of ß and subsequently some users observe the first input as being actioned upon by the system while others observe similarly the second input (Kiayias, 2021).

Liveness refers to the ability of the system to react in a timely manner to users' input. Liveness may be impacted by congestion and denial of service (DoS) attacks, where the system's capacity gets depleted as well as by censorship attacks where system maintainers choose to ignore the user's input. The expected responsiveness of the system may be affected by demand, but ideally, the system should have the capability to scale up with increasing demand so that quality of service is maintained.

It is sought is to argue that under reasonable resource restrictions the properties hold in the

Byzantine sense – i.e., an adversary cannot violate them unless it controls a significant number of resources. It is worth pointing out that while this is necessary, it is not sufficient; we would also want that given a reasonable modeling of the participants' utility functions, the desired system behavior is an equilibrium or even a dominant strategy, given a plausible class of demand curves for service provision (Kiayias, 2021).

2.4 Blueprint for stake-based systems

We assume that the developer has already a classical distributed protocol implementation of the service ß for k parties and understands the service maintenance costs and user demand. Adopting a stake-based approach, the resource will be digital coins. The developer mints an initial supply of such coins and disperses them over an existing population of recipients. This can be achieved by e.g., "airdropping" such digital coins to cryptocurrency holders of an existing blockchain platform. Due to this distribution event, the recipients become the stakeholders of the system (Kiayias, 2021).

A tokenomics schedule that considers the expected demand is determined and programmed into a smart contract. This contract will acknowledge the initial supply of coins as well as the schedule under which any new coins will be made available to the maintainers – the entities running the k-party protocol. Following market-based tokenomics the contract will also manage incoming transaction fees. Decentralized service provision is comprised of four parts. One is the k-party protocol that implements ß; the second is a proof-of-stake blockchain protocol that offers "dynamic availability," i.e., a protocol that can handle a wide array of participation

patterns without the requirement to be able to predict closely the active participation level (Badertscher et al., 2018). Inputs to the protocol will be recorded on chain, an action that will incur transaction costs to be withheld by the contract. The third part is a “proof-of-service” sub-system that should enable any system maintainer running the k-party protocol to demonstrate their efforts in a robust way. The verifier of such proofs will be the smart contract which will determine a performance factor for each maintainer. Finally, the fourth part is an algorithm that will parse the blockchain at regular intervals and determine the k parties to run the k-party protocol for ß. This can be done by weighted sampling (Spirakis et al., 2016), considering the stake supporting each operator. For rewards sharing, we need a mechanism to incentivize the stakeholders to organize themselves into at least k well-functioning nodes that will execute the multiparty protocol for ß when selected. To achieve this, we can deploy the reward sharing scheme over the underlying PoS blockchain; for that scheme it is shown how incentive driven engagement by the stakeholders can determine a set of k nodes at equilibrium (Brünjes et al., 2020). The reward scheme will be coded into the contract and will reward the stakeholders at regular intervals using the available supply from the tokenomics schedule and the transaction fees collected. The performance factor of each operator will influence the rewards, adjusting them in proportion to the operator’s efforts. The developer will produce an implementation of the above system and will make it available for download. A launch date for the system will be set as well as an explanation for its purpose. At this point, the developer’s engagement can stop. The stakeholders —the recipients of the newly minted digital coin— can examine the proposition that the system offers and choose whether to engage or not. If a non-negligible

number of them chooses to engage out of their own self-interest (which will happen if the developer's predictions regarding the long-term utility of ß are correct) the system will come to life bootstrapping itself (Kiayias et al., 2021).

3.0 Conclusion

This report begins by introducing the concept of a token, and how tokens play an important role in blockchain protocols. The combination of cryptography, game-theory, and market economics create robust decentralized peer-to-peer networks. It also introduces, at a high level, how tokens are created and how they accrue value over time.

Next, the report goes into the analysis of the characteristics of blockchain services - Resource-based participation, tokenomics and decentralized service provisioning. Participation talks about how to incentivize people to maintain the protocol, since it is running on decentralized machines. This is done by rewarding maintainers with tokens and can be implemented using many different schemes like proof of work or proof of stake.

Decentralized service provisioning involves ensuring both safety and liveness of the protocol, which means that the protocol must process requests in a consistent way for all users, and liveness ensures that requests are processes in a timely manner. Bottlenecks, congestion of requests, DoS attacks and censorship can affect the liveness of the protocol. These are enforced in a Byzantine sense, where no adversary can violate the rules of the protocol unless they own most of the computational power.

The report finally covers a blueprint model for a proof of stake protocol, outlining the division of resources among k members who will maintain the protocol. A smart contract acknowledges the initial supply along with scheduling further minting of tokens and specifies how rewards will be distributed based on available supply and transaction fees that are collected.

Acknowledgement

This report was created in an effort towards understanding the economics of blockchain protocols, since I am interested in creating one myself. Since the protocol will be handling large amounts of money, and will only come to life if there are enough incentives for all parties, I wanted to understand all considerations of tokenomics before creating an initial whitepaper for the protocol. This report was created using a plethora of research papers from the IEEE International Congress and arxiv collections, among other sources like the ETH Whitepaper.

References

1. *Lamberty, R., de Waard, D. and Poddey, A. "Leading Digital Socio-Economy to Efiiciency," 2008.*

   Source: https://arxiv.org/pdf/2008.02538.pdf

2. *Kiayias, A. "Decentralizing Information Technology," 2021.*

   Source: https://arxiv.org/pdf/2112.09941.pdf

3. *Michele Ciampi, Nikos Karayannidis, Aggelos Kiayias, and Dionysis Zindros. "Updatable blockchains," 2020.*

   Source: https://arxiv.org/pdf/2112.09941.pdf

4. *Juan A. Garay and Aggelos Kiayias. "Sok: A consensus taxonomy in the blockchain era.," 2020.*

   Source: https://arxiv.org/pdf/2112.09941.pdf

5. *Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system," 2008*

   Source: http://bitcoin.org/bitcoin.pdf

6. *Gavin Wood. "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, 2014.*

Source: https://ethereum.github.io/yellowpaper/paper.pdf

7. *Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. "Proofs of space," 2015.*

   Source: https://www.iacr.org/archive/crypto2015/92160192/92160192.pdf

8. *V. Buterin. "Introduction to cryptoeconomics," 2017*

   Source: https://2017.edcon.io/ppt/one/Vitalik%20Buterin_Introduction%20to%20Cryptoeconomics_EDCON.pdf

9. *A. Poddey and N. Scharmann. "On the importance of system-view centric validation for the design and operation of a crypto-based digital economy," 2019.*

   Source: https://arxiv.org/abs/1908.08675

10. *Christian Badertscher, Peter Gazi, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. "Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability," 2018, pages 913–930. ACM.*

    Source: https://eprint.iacr.org/2018/378.pdf

11. *Pavlos S. Efraimidis and Paul (Pavlos) Spirakis. "Weighted random sampling," In Encyclopedia of Algorithms, pages 2365–2367. 2016*

Source:

https://www.researchgate.net/publication/200026664_Encyclopedia_of_Algorithms

12. Lars Brünjes, Aggelos Kiayias, Elias Koutsoupias, and Aikaterini-Panagiota Stouka. "Reward sharing schemes for stake pools," In IEEE European Symposium on Security and Privacy, EuroS&P 2020, Genoa, Italy, September 7-11, 2020, pages 256–275. IEEE, 2020. Source: https://arxiv.org/abs/1807.11218