Financial Incentives in Crowdsourced Content Curation

Andrés Monteoliva Mosteiro

Master of Science
Computer Science
School of Informatics
University of Edinburgh

2018

Abstract

The amount of available content on the Internet vastly outweighs the attention span of online users. In the last few years, crowdsourced content curation has emerged as a novel approach to the aggregation and filtering of content in social media platforms. As opposed to traditional curation techniques, it avoids the reliance on a central party to curate content, allowing online communities to self-regulate. The advent of blockchains and cryptocurrencies has created new ways for the distribution and ownership of financial value over the Internet. Steemit is a social media platform which establishes financial rewards for the crowdsourced curation of content using the cryptocurrencies of the Steem blockchain.

In this work we present an analysis of the Steem blockchain, focusing on the economic and incentives model of the platform. Then we identify and evaluate the main issues of the incentives model of Steemit. Namely, we analyze the self-voting pattern and voting rings, moderation and censorship abuse in Steemit, and the types of voting bots in the platform. To better understand how self-voting can affect financially incentivized crowdsourced curation, we construct a formal model inspired by Steemit. Our model provides a formal framework which may be used in the evaluation of the incentive compatibility of Steemit or other decentralized content curation systems with monetary rewards. To conclude, we design and implement a solution for the moderation and censorship issues of Steemit in the form of a smart contract.

Acknowledgements

I would like to greatly thank my industrial supervisor Dr. Ben Livshits, Chief Scientist at Brave Inc. and Reader at the Imperial College of London, and my academic supervisor Professor Aggelos Kiayias. Their guidance, patience and insightful comments have been essential for the development of this project. I want also to express my sincere gratitude to Orfeas Stefanos Thyfronitis Litos, Ph.D. student at the Blockchain Lab, for his invaluable advice and discussions. Last but not least, I would like to thank my parents, Alejandra and Eduardo, for their endless support and for providing me the opportunity to study this Masters.

Declaration

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

(*Andrés Monteoliva Mosteiro*)

Contents

Chapter 1

Introduction

We live in the Information Age. The Internet has enabled an explosion in the amount of information available to us. In the past decade, the amount of accessible data has grown exponentially. However, we humans have only a limited amount of time and attention span. The challenge of our generation is not in the possibility to consume content, but what content to consume. How do we decide what to read or which movie to watch? And most importantly, who is the one deciding?

Content curation is the process of ranking, filtering and aggregating information. Recently, social media aggregation sites like Reddit or Digg have popularized the use of the wisdom of the crowds to better curate content. As opposed to more traditional curation techniques such as experts or algorithmic-based content curation, crowdsourced content curation lets users distributedly review and value a product or a piece of information. In particular, the case of Reddit is the epitome of crowdsourced content curation. All the content in the site is generated and curated by the users of the platform, with the need for minimal external intervention. Ironically, all the financial value created in the platform goes to the owners of the site.

The advent of blockchains and cryptocurrencies has given new means for a fairer distribution of value among online communities, transforming networks into markets. Their convergence with social media creates new possibilities for the sharing of value and ownership in online platforms. The addition of financial incentives in the generation and curation of content establishes a new paradigm that must be studied in detail.

1.1 Motivation and Objectives

Several projects have explored using financial rewards as a more effective approach to content curation and value distribution among social networks. Among them, Steemit[1] has the longest track record, having been in operation since 2016 and attaining a considerable user base of more than 1.08 M registered accounts[2]. Our hypothesis is that the analysis of the inner workings of Steem, framing it as a live experiment, can provide us with new and valuable insights into the role of financial rewards on crowd-sourced content curation. Although content curation has already been studied from a game-theoretic and economic mindset, we recognize these past efforts as mostly theoretical exercises. We attempt to fill this gap with the present work. The analysis of Steemit and how financial rewards affect users behavior in the platform will enable us to contribute to the field with a completely original approach.

1.2 Contributions

Steemit is an open-source project which accounts for more than 200K lines of code. The official documentation is very sparse and lacks a detailed description of the functionality of the Steem blockchain [6]. Taking into account that the current market capitalization of the Steem project surpasses the $300M[3], a clearer description seems essential for the better understanding of the project for researchers, users and prospective investors. In particular, our core contributions are:

- **Analysis and evaluation of the Steem blockchain.** Description and evaluation of the main properties and components of the Steem blockchain. Analysis of the cryptocurrencies of the blockchain, its consensus algorithm and the role of block producers in the blockchain. See Chapter 3.
- **A mathematical model of the rewards and curation system extracted from the source code.** We have developed a mapping between the source code of the current implementation of the blockchain and a mathematical model which describes the financial rewards and curation system in the platform. Based on previous research work from users of Steemit [5, 32, 58], we provide a complete

[1] Steemit is the social media platform and Steem the blockchain behind it.
[2] https://steemdb.com/accounts.
[3] https://coinmarketcap.com/currencies/steem/. Accessed: 2018-08-06.

and grounded mathematical analysis of the rewards mechanics of Steem. See Section 3.4.

- **Identification and evaluation of the main issues and potential attacks of the rewards and curation system of Steem.** In particular, we have identified three major problems: abusive self-voting behavior and the creation of voting rings, lack of a solid moderation protocol and possibility of censorship abuses, and the noticeable influence of voting bots on the platform. See Chapter 4.

- **Steemit as a game.** Development of a formal model of crowdsourced curation with financial incentives in social media. Abstracting from the particularities of the Steem blockchain, we have aimed to model financial rewards for crowdsourced curation in a more general framework. See Chapter 5.

- **Moderation protocol.** Design and implementation of a solution proposal in the form of a smart contract to the moderation and censorship issues of Steemit, based on the work of Buterin [15]. Our proposal should be framed as a potentially implementable Proof of Concept for the Steem blockchain, not as ready-to-use moderation protocol. See Chapter 6.

1.3 Outline

Our MSc Thesis is divided into 7 chapters. The *Introduction* describes the motivation of our research problem, objectives and the main contributions of this Thesis. The *Background* provides both a technical and a historical review of the state of the art of the field. *Analysis of Steem Rewards and Curation System* starts with a high-level overview of the Steemit project, describing its native cryptocurrencies or consensus algorithm. Then, it provides an in-depth analysis of the rewards and curation system of the Steem blockchain. *Issues and Potential Attacks on the Rewards System of Steem* identifies and evaluates the main issues of the voting, rewards and curation system of the Steem blockchain. *Modeling Steemit as a Game* proposes a formal model of how self-voting patterns can affect the quality of curation in social media platforms. Then, *Moderation Protocol Proposal* develops a solution to the moderation and censorship issues in Steemit. In *Conclusion* we present interesting further related work and provide our concluding remarks.

Chapter 2

Background

2.1 From Usenet to the Blockchain

Social media and the Web 2.0

The importance of social media has been growing increasingly since Usenet was created in 1980 as the first discussion platform over the Internet [43]. As of 2018, social networks such as Facebook have more than 2 billion active monthly users[1], 500 million tweets are created on Twitter each day[2] and Instagram users like more than 4 billion posts every 24 hours[3]. In consequence, social media and its effects on the evolution of the Internet have been extensively researched in academia. Kaplan and Haenlein [36] highlight the importance of two terms deeply connected with social media: the Web 2.0, as the new patterns of collaboration and sharing of content on the World Wide Web and User-Generated Content (UGC), taking into account how online users evolved from sole consumers to creators and curators of the content of the Web. From the already mentioned social networks to collaborative wiki projects as Wikipedia or user distribution platforms like Youtube, social media platforms have been built in many different shapes, but all share an emphasis on the content generated by the users on the platforms.

[1] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. Accessed: 2018-07-22.

[2] http://www.internetlivestats.com/twitter-statistics/. Accessed: 2018-07-22.

[3] https://blog.hootsuite.com/instagram-statistics/. Accessed: 2018-07-22.

Decentralizing the Internet, again

As social media grew in importance, the economic value created in these sites also escalated with the boom of the so-called "attention economy" [24]. However, even though the users were generating most of the value, creating and curating content, the economic gains mostly remained within the companies which owned the platforms. As a consequence, these companies have become effective data silos, profiting from the data and the content of their users through advertisement-based business models [47]. At the same time, an opposing force was growing on the Internet with the advent of peer-to-peer file-sharing systems, which became mainstream when Bram Cohen created the BitTorrent file distribution system [22]. Yeung et al. [64] analyzed how the convergence of social media and P2P decentralized architectures could lead to a fairer distribution of the ownership of data and content in social networks. These advances have created new possibilities in the sharing and distribution of user-generated content, but effective mechanisms to distribute the economic value created by online users was still lacking. When Satoshi Nakamoto published the Bitcoin White Paper in 2009 [48], a new paradigm emerged, enabling digital users to exchange and store value without relying on a central entity. The financial applications of Bitcoin were just the beginning, as other projects started envisioning blockchain architectures as a new means to decentralize the ownership and exchange of value over the Internet.

2.2 Blockchain and Cryptocurrencies

Bitcoin, a New Form of Money

Prior to Bitcoin, there were some attempts to create a digital version of money, like the e-cash proposed by Chaum et al. [20] or Nick Szabo's "BitGold" [56]. However, these projects had to rely upon centralized services in various degrees. Satoshi Nakamoto created the first peer-to-peer financial system which also solved the "double-spending" attack[4] using an innovative data structure: the blockchain. Also known as a distributed ledger, a blockchain can be understood as a cryptographically-signed shared record of all the transactions that happen in the network. Transactions are stored in blocks by "miners", and new blocks are sequentially appended to the chain including the hash

[4]Double-spending occurs when a user spends more than once the same coin.

of the previous one, forming an immutable and tamper-resistant ledger shared by all the peers of the system. Miners, also known as block producers, run a distributed consensus algorithm known as Proof of Work to determine who appends the next valid block in exchange for cryptocurrency rewards. Essentially, the Nakamoto Consensus solved the double spending attack by creating a public cryptographically signed database which was shared and extended by the users of the system over a P2P network [48].

Beyond the Financial Applications of Bitcoin

In spite of the narrow financial purposes of Bitcoin, using blockchains as a public trusted ledger have the potential of tackling a wider spectrum of problems. In 2014, the Ethereum blockchain was created as a general-purposed transaction based state machine, aiming to overcome the constraints of Bitcoin [61]. Also known as a "world-computer" given its Turing completeness, Ethereum enabled the creation of programs, also known as smart contracts, which are stored and executed redundantly in all the nodes of the network [61]. Consequently, the tech community started exploring the usage of decentralized architectures for different use cases beyond financial applications. These projects are building protocols and applications over Ethereum, using token-based models such as the popular ERC20 standard [1]. An orthogonal approach to extending the functionalities of Bitcoin is to create single-purposed blockchains. These distributed platforms, also known as "app-chains", attach a blockchain to a specific use case. Examples of this design pattern are NameCoin[5], which aimed to create a decentralized domain name system or Steemit [6], which uses a distributed database as the backend of a social media platform. Both approaches used distributed ledgers to create a shared "source of truth" but also to deploy new economic ecosystems. The cryptocurrencies pegged to each blockchain enable the monetization and exchange of value between the different agents of these systems.

A Technical Taxonomy of Blockchains

To better understand the differences between blockchain-based systems, Xu et al. [62] proposed a taxonomy to classify existing solutions. Although the categorization of

[5] https://namecoin.org/.

their work is more extensive, we highlight what we consider the main design decisions of blockchain system: their openness and the consensus protocol used.

In terms of their openness, these systems can be defined as:

- **Public blockchains[6].** Any new user can create an account or an address (i.e. a pair of a private key and its public key) at minimum or no cost. Any address running a node on the network has read and write permissions on the ledger. Examples of public blockchains are Bitcoin or Ethereum.
- **Private blockchains.** There are restrictions on joining the system, based on an initial setup or decided by current members. The read and write permissions of the ledger may also be restricted for some users. Private blockchains also tend to be employed by a federation or a consortium of different business entities, as the Hyperledger Project[7], led by the Linux Foundation.

In both public and private blockchains, miners or block producers must agree on the validity and the state of the ledger, which is known as the consensus protocol. There are many proposed solutions to address consensus in distributed ledgers, but the most popular ones are:

- **Proof of Work (PoW).** Miners try to solve a computationally hard mathematical problem. The user who first finds a valid solution is elected as the "leader" and appends a new block of transactions to the ledger. Nakamoto Consensus PoW or its variants (e.g. Litecoin's Scrypt [50]) have been the most popular consensus protocols for permissionless blockchains [62].
- **Proof of Stake (PoS).** PoS substitutes the need for consuming computational power and block producers are chosen probabilistically in proportion to the amount of cryptocurrency they hold or have staked in network. Staking refers to the process of locking a determined amount of tokens in a vesting plan, so the owner cannot exchange them, becoming illiquid. Different projects like Cardano's Ouroboros [38] or Ethereum's Casper [16] are exploring PoS as a more scalable and energy efficient alternative to Proof of Work.
- **Byzantine-Fault-Tolerance (BFT).** This is a branch of consensus protocols widely studied in the distributed systems literature, and refer to algorithms re-

[6] In the rest of this writing, when the term "blockchain" is used we will be referring to permissionless or public blockchains. Otherwise, we may precise "private blockchain".

[7] https://www.hyperledger.org/projects/fabric.

sistant to Byzantine Attacks [17]. In BFT protocols, the block producers are determined prior to the protocol execution. A consortium of block producers is selected randomly in BFT-based public blockchains and deterministically for the permissioned setting. An example of the usage of Byzantine Agreements in a public blockchain is the Algorand protocol [30].

Economic Analysis of a Blockchain

Along with the high levels of innovation in the blockchain ecosystem, the market capitalization of the main cryptocurrencies has drastically increased in the past several years. At the time of writing, the cryptocurrencies total market capitalization was situated above $280B, with Bitcoin accounting for more than the 45% of the market, $128B[8].

The high valuations of blockchain based networks have triggered a desire in the research community to understand the economic implications of these systems. Catalini and Gans have identified the costs attached to blockchain networks: the cost of verification and the cost of networking [18]. The cost of verification tends towards zero in the permissionless setting, but it may increase in more permissioned systems due to Know-Your-Customer (KYC) and related verification processes. The networking costs can be divided into the bootstrapping of the network and the operational costs. The bootstrapping of the network has been accomplished via funding models like the popular Initial Coin Offerings (ICOs) [19] and with more organic growth inflation models like the case of Bitcoin. Sockin and Xiong argued that cryptocurrencies establish membership to owners in the blockchain, facilitating transactions and exchange of value within the platform [54]. Therefore, since investors in a cryptocurrency are at the same time users of the blockchain, a successful bootstrapping of the network is essential to the correct functioning of a cryptocurrency. It should be noted that blockchains are decentralized P2P systems, so the operation of the network must align the incentives of all the agents in the network. This equilibrium is usually achieved by including financial rewards in the form of tokens to the validators and maintainers of the ledger (i.e. the miners).

[8]https://coinmarketcap.com/. Accessed: 2018-07-22.

Forking a Blockchain

However, there are certain events which can disrupt the balance of incentives in blockchain systems. Apart from targeted attacks on the platform or edge cases such as the 51 % attack [48], Abadi and Brunnermeier have researched the incentives and competition between rival forked ledgers [7]. Blockchains are open source collaborative projects, so a subset of the users of the network may change the protocol and "fork" the ledger, starting an independent blockchain while sharing the whole previous history with the original ledger. Forks can be divided into hard forks and soft forks, meaning that hard forks make an upgrade compulsory from the nodes of the network. Forks may destabilize the dynamics of these networks, forcing the users and miners to choose one of the opposing factions.

Price and Valuation of Cryptocurrencies

Besides the internal economic dynamics of blockchain networks, researchers such as Abadi and Brunnermeier [7] or Burniske and Tatar [14] have developed economic frameworks to better understand the key drivers of price and valuation of cryptocurrency projects. Following economic fundamental standards, price can be derived from the tension between supply and demand. The supply of cryptocurrency is tied to the bootstrapping and operation mechanics of a blockchain. The monetary policy of the system will define the initial supply of the cryptocurrency, the amount of tokens minted per block and if the the total supply of is capped (i.e. has a limit, as the 21 millions limit of Bitcoin) or not. The demand for cryptocurrency can be conditioned by its current applications or driven by purely speculative motives. Cong et al. [23] propose a dynamic asset-pricing model for the evaluation of user adoption in cryptocurrencies. The model shows how crypto-tokens derive their value as assets with limited supply that users may hold to gain availability of a particular set of utilities in the blockchain. They argue that embedding tokens in a platform can accelerate user adoption, but also may lead to a faster abandonment of a non-successful project. Consequently, they highlight the importance of the feedback loop between utility, user adoption and price of cryptocurrencies. The utility of a blockchain increases user adoption, consequently raising the expectation of growth and demand for cryptocurrency, which leads to an increase in its price. However, it should be noted that as cryptocurrency markets are still in a immature phase, the price fluctuation may be more influenced by price speculation than actually adoption and user base growth [14].

The next figure presents the evolution of the price of the cryptocurrencies of Steem, showing the speculation bubble in the price of STEEM in 2016 described by Burniske and Tatar [14]:

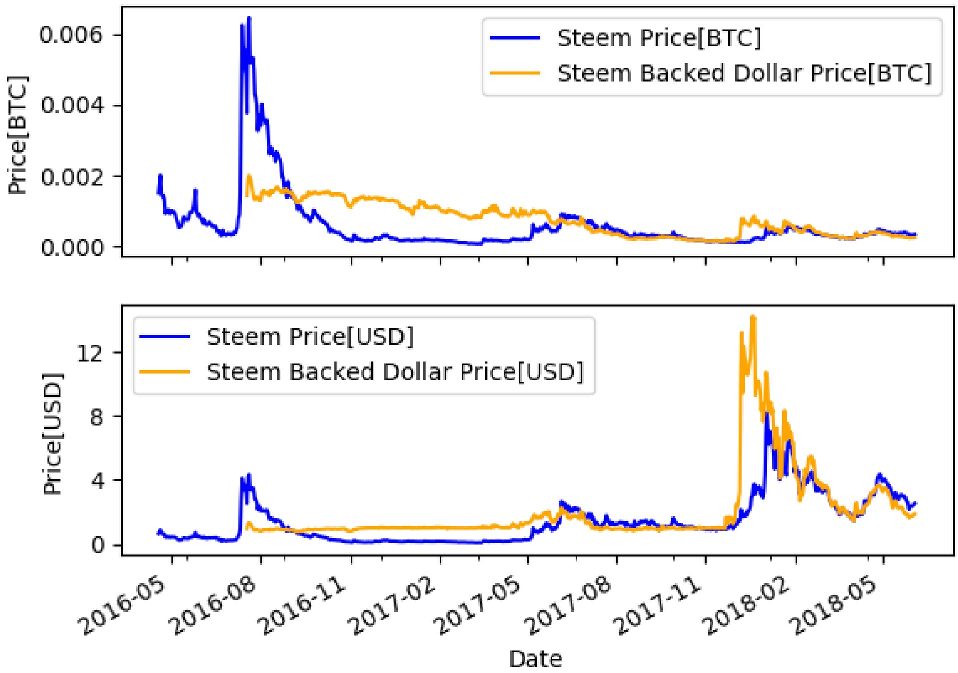

Figure 2.1: Evolution of the prices of the main cryptocurrencies of the Steem blockchain in terms of BTC and USD. Data extracted from the cryptocurrency market tracker Coingecko. Accessed: 2018-07-25.

Cryptocurrencies and Social Media

One of the use cases which have converged with cryptocurrencies is social media. The decentralization and censorship resistance of public blockchains have emerged as desired properties for a new generation of social media platforms. Apart from that, the ownership and exchange of value in the form of cryptocurrencies provide new means for fairer distribution of the value generated in these platforms. The main projects which aim to integrate social platforms and blockchains and cryptocurrencies are:

- **Steemit.** It is a social platform tied to the Steem blockchain, where users can create and curate content. Part of the new Steem tokens created with each block is distributed between the author and curators of popular content, thus establishing incentives for the creation of quality content in the platform [6].

- **Synereo.** The Synereo platform also aims to incentivize the curation of news and user generated content. For that purpose, it uses two cryptographic tokens, REO and AMP, which let users invest in articles to help them become popular and measure the different reputation levels among different users. The core idea is that posts with big amounts of cryptocurrency will be leveraged on the Synereo's ranking algorithm [40].
- **Akasha**[9]**.** Built over Ethereum and IPFS[10], the Akasha project is building a censorship resistant social network where users create and vote for content, with the possibility to be rewarded with the token AETH if their content becomes popular.
- **Yours.org**[11]**.** It lets users post and vote for content on the site. Authors can create free or "Pay-per-View" content, so the rest of the users need to pay a determined fee to the author to visualize the "paid content". Users are also able to tip an author for a post when they vote for it. The monetary exchanges of the platform are performed with the cryptocurrency Bitcoin Cash (BCH).
- **Peepeth**[12]**.** Built as an Ethereum's smart contract, it is an uncensored Twitter-like platform, where users can donate and tip creator of good content. Unlike the rest of the projects presented in this section, Peepeth does not have a built-in incentives infrastructure for voting and content curation, and it is solely based on tipping and donations.

2.3 Crowdsourced Content Curation

While the blockchain-based projects mentioned in the previous section establish financial incentives for distributed content curation and aggregation of quality content, curation of content in online communities is a well-researched topic in academia.

[9] https://akasha.world/.
[10] https://ipfs.io/.
[11] https://www.yours.org/.
[12] https://peepeth.com/.

Content Curation Patterns

Askalidis and Stoddard defined crowdsourced content curation as a recent alternative to more classical approaches such as expert-based curation or algorithmic-based curation [9]. Crowdsourced curation has become popular in the last decade with news aggregation sites like Reddit or Digg. These platforms rely mostly on their users to weight and curate news and posts through upvotes and comments.

They studied both sites and parametrized the effectiveness of crowdsourced content curation with two metrics: curation quality and discovery efficiency. The outcomes of their study reflected that while crowdsourced curation effectively discovered and promoted high quality content, the ordering of the posts in terms of their objective quality was not so accurate. Along these lines, Zhong et al. performed an empirical study on the crowdsourced content curation dynamics of the photo-sharing site Pinterest and the radio-streams community Last.fm [65]. They differentiate two distinct types of curation: structured and unstructured content curation. Unstructured curation refers to users who just highlight content (e.g. an upvote or a retweet) and structured curation includes more participatory mechanisms such as custom-tagging and user-defined rankings. This study reflected that a higher prevalence of structured curation in a particular post was highly correlated with its popularity.

Besides the categorization of different approaches to content curation, it is interesting to understand the dynamics of individual users when they upvote or share content in social media platforms. Glenski et al. studied the browsing and upvoting patterns on Reddit [31]. Reddit follows the so-called “Wikipedia Law”[13], where 90% of the users are just information consumers, 9% are editors or moderators, and only about 1% of the users are content creators. Studying a subset of the browsing behavior of Reddit users, they found out that 73% of the votes are made without actually reading the article and that users are more likely to vote and comment in “subreddits” rather than in the home page. It should be noted that another common behavior is users trying to maximize their reputation on the platform, or “karma” in Reddit jargon [9]. These observed patterns have led other research groups to model users in social media platforms as strategic rational agents.

[13] https://www.theguardian.com/technology/2006/jul/20/guardianweeklytechnologysection2.

Strategic Behaviors in Social Media

Several studies have modeled users in social media as strategic agents, supported by the development of game-theoretic frameworks to understand users' incentives and objectives.

May et al. describe the dynamic between bloggers and readers as a "Blog-positioning game", to empirically study crowdsourced curation [45]. The proposed game consists of two sets of players: the bloggers deciding what and when to post, and the users, who decide who to follow or upvote. The authors of the study highlight that users and bloggers follow two observable dynamics: a) users who receive less content read more popular content and b) popular but less active bloggers usually post more successful posts on average. Along these lines, Abbassi et al. proposed a game-theoretic model between publishers and readers to find out the optimal content selection to achieve the most efficiency on the curation of content [8]. They showed that optimal content curation under a Centralized Curator, which has complete information on the system and optimizes, respect to the social welfare, the set of items each publisher must post is a NP-complete problem.

The propagation of high quality information in social media has also been framed as a game-theoretic challenge. Gupte et al. modeled content creators as rational agents who try to maximize the diffusion of their content [35]. For that matter, they differentiate between greedy and courteous authors. The main difference between the two strategy profiles is that courteous authors care if they spam their followers with information that they already have received. Supported by their theoretical model, they proved that high-quality information successfully spreads over the network if the content producers are greedy. Another approach to understanding the diffusion of content is to model news and user-generated content as public perishable goods. Ramachandran and Chaintreau showed the impact of time in the diffusion of content and proved that short-lived information has simpler and more predictable diffusion patterns than long-lived content [52].

The previously mentioned research efforts aim to better understand the incentives behind content diffusion and crowdsourced curation in social media platforms. It can be argued that their objectives are based on economic goals such as advertisement partnerships or fees for content creators. Nevertheless, the economic rewards for authors and curators in traditional systems are not always so evident, as rewards can be also in the form of reputation or social badges [42]. Blockchain-based social networks like Steemit establish a precise translation between user activity and economic rewards. Therefore, the modeling of users as strategic agents proposed by these authors seems more appropriate in platforms like Steemit than in traditional platforms. The explicit financial rewards present in Steemit or Synereo create a more accurate scenario for game-theoretic frameworks.

Crowding-Effect

As a side note, a behavioral economics theory called "Crowding Effect" studies the effect of economic rewards in the motivation of users to perform an action [29]. Liu et al. have studied the crowding effect on online communities [42]. The existence of monetary rewards motivates users to share knowledge or curate content. However, at the same time, they decrease their intrinsic motivation (e.g. personal fulfillment, pro-social behavior or genuine interest). Therefore, we can expect that while financial rewards will motivate users to create and curate content, their behavior will be driven mostly by economic factors, resembling more to strategic players.

2.4 Attacks and Decentralized Governance

Social media platforms are a target of different kinds of attacks vectors, from external agents, users themselves or the owners of the platform. The governance of online communities is of vital importance. Through the creation of rules and policies, the governance mechanisms of social media platforms ensure their resilience and protection against attacks and failures.

A Classification of Attacks

Kayes and Iamnitchi proposed a taxonomy of attacks on social networks [37]. They define two broad categories: attacks against a subset of users of the platform and attacks targeting the platform itself. Three types of attacks against social media platforms that are relevant to our study are Sybil attacks, Social Spam and Distributed Denial-of-Service(DDoS). In a Sybil attack, a malicious user creates multiple fake identities to alter a particular outcome of the system. If the sign-up barrier to the platform is low (i.e. users can create accounts fast and at a low price) an attacker can create Sybil accounts at a low financial risk. The solutions against Sybil attacks can be divided between Sybil detection and Sybil resistance techniques. Sybil detection mechanisms aim to identify and block accounts from fake identities. Examples of Sybil detection techniques are IP and device detectors. In contrast, Sybil resistance techniques leverage the social graph of the platform to create structures resilient to the effect of these fake accounts. Examples of Sybil resistance mechanisms are online auctions or reputation systems. On the other hand, social spam (or just spam) can be defined as unwanted content spread through the network. When the cost of sending a message tends to zero, social spam can be pervasive in social networks and in other communication channels such as e-mail. Back in 1988, Dwork and Naor, proposed a spam resistance mechanism over e-mail, which is considered to be the precursor of the PoW protocol used in Bitcoin [26].

Another type of attack on a social media platform is censorship abuse. It refers to the suppression or extreme moderation by power users or the owners of the social network, censoring the freedom of speech of a determined subset of users. Bamman et al. have analyzed censoring practices in Chinese social media [11]. They describe different censorship mechanism in the blogging website Sina Weibo[14], such as network filtering and chat and messages deletion. However, these practices also occur in the major Western sites such as Facebook or Twitter, as reported in the "Community Guidelines"[15] of these sites. When the community rules of an online platform are too stringent, censorship abuse can become more prevalent, as reported in the Q&A site StackOverflow[16].

Governance in Online Communities

Governance in social media platforms can be understood as the mechanisms to deliberate and enforce the rules and policies of the system [41]. In the centralized setting, the owners of the platform can arbitrarily set and change its rules. However, in decentralized system, there has to be a set of mechanisms which enable the distributed self-regulation of the platform. The most popular and well-researched example of

[14] https://www.weibo.com.
[15] https://www.facebook.com/communitystandards/.
[16] https://stackoverflow.blog/2018/04/26/stack-overflow-isnt-very-welcoming-its-time-for-that-to-change/.

decentralized governance is Wikipedia. Governance can be divided in two separate mechanisms: deliberation and enforcement.

Leskovec et al. analyzed the deliberation mechanisms of Wikipedia governance. They describe the voting and election processes for administrators, and how casting public votes may influence the voting behavior of users [41]. Forte and Bruckman describe a complete taxonomy of the different roles of users in the Wikipedia community, explaining the role of editors, administrators and committees in the platform [28]. They also include a description of how these hierarchies and processes have become more decentralized over time. Voting behavior and online elections have also been researched by Kling et al., when they studied the election process of the German Pirate Party. The German Pirate Party is arguably the greatest organization in the world which permits vote delegation among its user base [39]. Consequently, they studied the dynamics of the creation of super-users (i.e. users who have been delegated large amounts of votes) and how this pattern affects the governance deliberation process. They found out that super-users does not have a disruptive effect on the outcomes of election but, rather, they become stabilizer agents in voting results.

When there is an established set of rules, there must be mechanism to enforce these policies. Taraborelli and Ciampaglia extensively researched the practices of deletion and inclusion of articles in Wikipedia [57]. In particular, they analyzed the logs of the so-called “Article of Deletion”, the main channel to asses the suitability of content in the platform. They detected a long-tailed distribution in terms of user-participation, with a small subset of editors participating in most of the discussions. Along these lines, Yasseri et al. investigated the effect of editorial wars in Wikipedia [63]. They measured the activity peaks of editing logs when conflicts between different subgroups of the platform appeared.

Taking Decisions with Prediction Markets

To achieve a decentralized governance infrastructure, a system must aggregate the opinions and decisions of its users in the fairest and most effective manner. Prediction or information markets have emerged as an effective approach to aggregate the wisdom of the crowd. Wolfers and Zitzewitz define prediction markets as markets where participants bet in contracts and conditions whose payoff depends on a future unknown event [60]. They claim that if the “Efficiency of markets theory” is assumed as valid (i.e. the price of an asset reflects all the available information) [44], the market price will be the best predictor of an outcome. The most popular example of a prediction market in practice is the Iowa Electronic Market on the American Presidential elections. Berg and Rietz describe how prediction markets can be effectively used as tools to take better and more informed decisions [12]. They argue that decision support systems are better suited to conditional prediction markets, where predictions are made about future events conditioned by other future events. To better understand the influence of money in prediction markets, Servan-Schreiber et al. analyzed the differences between real and play-money prediction markets [53]. The authors did not find major differences between the two settings, and their hypothesis is that while real-money markets have stronger incentives for betting and information discovery, the flatter distribution of wealth in play-money market equilibrated their results.

Markets as Decentralized Governance

Merkle describes how prediction markets can enhance democracies in the decision making process, with a governance model called “futarchy”. He claims that the aggregation of knowledge extracted in the markets can help maximize the Democratic Collective Welfare, a key parameter to describe the welfare of a population [46]. Merkle also describes how this paradigm could be implemented in the form of a Decentralized Autonomous Organization (DAO), a distributed entity whose rules are hard-coded and its governance decisions in the system are extracted from voting and betting markets mechanisms. Influenced by these ideas, Buterin proposed the application of prediction markets and DAOs to enhance the properties of crowdsourced content curation [15]. He argued that the existence of markets would incentivize the participation of the crowd, thus achieving a decentralized and effective self-governance in social media platforms.

Chapter 3

Analysis of Steem Rewards and Curation System

Steemit is a social media platform which relies on the information stored in a distributed ledger, Steem[1]. The Steem blockchain is an open-source project and our aim in this chapter is to better understand its inner workings in detail. For this purpose, we analyze the main properties of Steem such as its reputation system or consensus algorithm, preceded by an exposition of previous related work and background. Then, we focus in more depth on the economic and incentives model of Steem, analyzing its rewards and curation system. This analysis will provide us a better understanding of the financial incentives in the crowdsourced curation of the platform. We aim to develop an explanatory mathematical model based on our investigation of the source code of the current implementation of the blockchain.

3.1 Related Work

Thelwall published the only journal paper focusing on the Steemit platform to our knowledge [59]. He analyzed the first and subsequent posts of all the users in Steemit, correlating the content of the posts and the rewards earned. The research effort of Thelwall is mostly empirical, as it just focuses on analyzing the outcomes of Steemit but does not attempt to evaluate the mechanics of the platform. Chohan authored a high-level explanation of Steemit, as part of a discussion series on cryptocurrencies [21].

[1] We will refer to Steem as the blockchain or ledger and to Steemit as the platform.

This paper briefly describes the history and evolution of Steemit, the dynamics of the platform and its main related issues. Moreover, in the Steemit platform itself, many users aim to research and explain the inner workings of the platform. Although most of this information is mainly opinionated, there are posts which complement the official documentation of Steem. As an example, González analyzed the author and curation rewards in Steemit from a mathematical perspective [32]. Along these lines, core contributors to the Steemit project like "Theoretical"[2] have also published explanatory posts on the reward mechanics of Steem [5]. We aim to aggregate the knowledge of these different sources and provide a more scientific and grounded approach to the analysis of Steem.

3.2 Methodology and Objectives

Objectives

We analyze the mechanics of the Steem blockchain and how financial rewards are created and distributed among its users. The official documentation, in the form of the Steemit Whitepaper [2, 3, 6] provides only a high level description of the inner workings of the Steem blockchain. Past research on Steemit has focused either on the content created in the platform [59] or just provided a more descriptive perspective on the system [21]. We aim to fill the gap between the official documentation and past research efforts, to actually understand the voting and rewards systems in Steem and identify potential issues on the platform. The lack of an extensive documentation of the process has lead us to analyze the actual implementation of the blockchain, available in the Steemit's Github account[3].

Research Methods

The official documentation of the Steemit project is sparse. In order to achieve a detailed understanding of the system, we will combine several exploratory approaches. The research methods to develop an accurate model of the inner workings of the Steem blockchain will be:

[2] https://steemit.com/@theoretical.

[3] https://github.com/steemit/steem.

1. **Documentation.** Study and research on the available sources of information which describe the operations of the Steem blockchain. Namely, our sources of information will be:

   (a) **Steemit White papers.** The Steemit project have published a White paper. The White paper has undergone important modifications across the 3 main published versions [2, 3, 6].

   (b) **Posts on Steemit.** The description of the functioning of Steem is a popular topic on the content created in Steemit. We analyzed explanatory posts from different sources, including Steemit project core contributors [5] and the material created by independent researchers [32, 58].

2. **Steemit GitHub Repository.** The analysis of the main repository of source code of the project will allow us to extend our understanding of Steem and compare it with the existing documentation. The Steem blockchain currently accounts for more than 200K lines of code, most of them written in the C++ programming language. To explore the considerable sized code base, we will use:

   (a) **Sourcetrail[4].** A C++ source code explorer which uses static analysis and a graphical interface to help developers become familiar with existing large code bases. This will correspond to a first stage of the code exploration, to better understand the call-graph of the project, dependencies and relevant files for our research.

   (b) **Source code[5].** After building a certain familiarity with the code base, we will manually analyze the code files relevant to our analysis. This will also encompass the exploration of important commits and issues on the repository by Steem core contributors.

3. **Blockchain analysis.** To retrieve relevant data from the blockchain, like the number of users or the token supply, we will employ:

   (a) **Steem-Python library[6].** It is the official library of Steem for Python developers. It provides an easy way to interact with the blockchain and retrieve relevant data without running a full Steem node.

[4] https://www.sourcetrail.com/.
[5] https://github.com/steemit/steem.
[6] http://steem.readthedocs.io/en/latest/index.html.

(b) **Steemdb**[7]**.** It is the most popular blockchain explorer for the Steem blockchain. Historical data from the blockchain can be obtained without the need for developing customized complex queries to the blockchain.

3.3 Steem Blockchain

3.3.1 Introduction

Steemit is a social media platform which lets users earn money when creating and curating content in the network. Steemit is the front-end of the social network, a graphical web interface which allows users to see the content of the platform, owned by Steemit Inc. However, all the backend information is retrieved from a distributed ledger, the Steem blockchain. Steem can be understood as an "app-chain", a blockchain with an specific application purpose: serving as a distributed database for social media applications [6]. It should be noted that although Steemit Inc. leads the Steem blockchain project, other independent social media platforms are based on the Steem blockchain, such as SteemKr[8] or D.tube[9].

The Steem blockchain was launched in March 2016, and the first payout distribution among its user base was performed in July 2016. Steemit can be thought of as the the first blockchain-based social media project, with a stable functioning track record and a considerable user base, with more than 1.08M registered accounts[10]. It should be noted that one user can create several accounts, so the actual amount of active users should be a portion of this number. An account in Steem is defined as a string "@accountName", mapped to a key-pair which uniquely identifies a user.

3.3.2 Cryptocurrencies in Steem

The Steem blockchain has 3 currencies or units of account in their system:

- **STEEM**[11]**.** It is the main native cryptocurrency of the Steem blockchain and the

[7] https://steemdb.com/.
[8] https://steemkr.com/
[9] https://d.tube/.
[10] https://steemdb.com/accounts. Accessed: 2018-07-27.
[11] STEEM refers to the cryptocurrency and Steem to the blockchain.

other cryptographic tokens derive their value from it. It is a liquid asset, so it is tradable without restrictions both in Steem internal exchange and in external exchanges.

- **SBD.** Steem Backed Dollar. It is the secondary cryptocurrency of the blockchain. It aims to be pegged to the price of the dollar, converting it into a stable token. It is also a liquid asset, tradable in both internal and external exchanges.

- **SP.** Steem Power. It corresponds to the amount of STEEM a user has staked in the system. The process of staking STEEM, also known as Power Up, corresponds to adding STEEM to a vesting plan where the funds are temporarily locked in the system. The Steem Power is illiquid and can only be exchanged by STEEM following a percentage withdrawal plan of 13 weeks. SP is not tradable with other currencies in external exchanges.

The next figure shows the evolution of the market capitalization of STEEM and SBD in terms of BTC and USD:

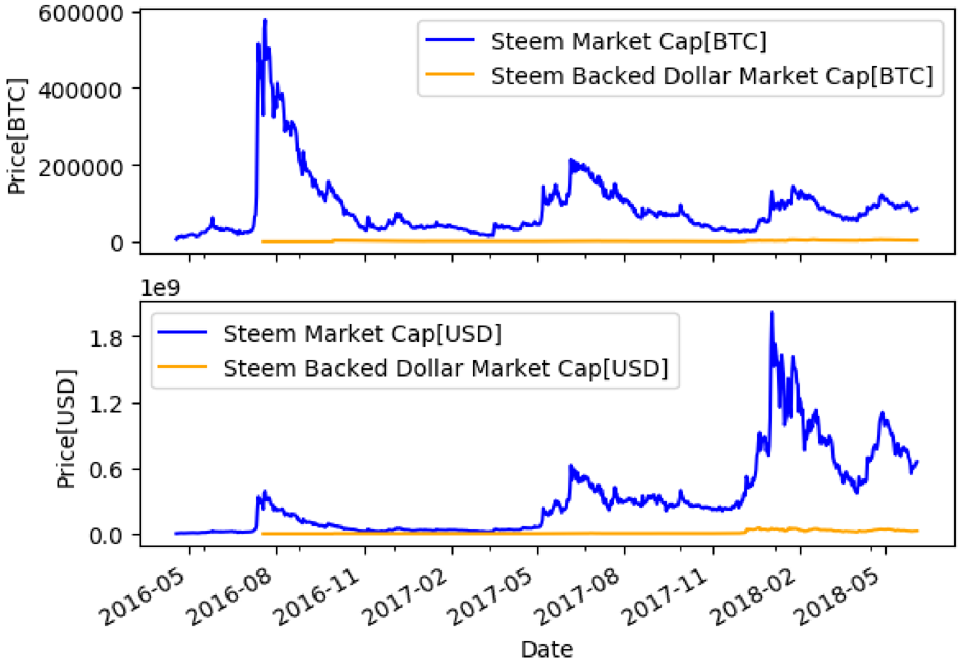

Figure 3.1: Evolution of the market capitalization of STEEM and SBD in terms of BTC and USD. The figure shows the differences of scale between the two main currencies of Steem. Data extracted from the cryptocurrency market tracker Coingecko. Accessed: 2018-07-25.

3.3.3 Consensus Algorithm

The Steem blockchain reaches consensus with a protocol called Delegated Proof of Stake (DPoS). DPoS is framed by the official documentation as “a variant of Proof of Stake” [6], where a fixed amount of block producers are elected via a polling scheme. In each round slot, one of the block producers (also known as witnesses) group a set of transaction into a block and append it to the ledger [4]. A transaction in Steem has a broader meaning than a Bitcoin transaction, as it can contain any update to the global state of the chain. Examples of transactions in Steem are creating a post or a comment, upvoting content or converting STEEM to SP.

Election of Witnesses

In Steem, 21 witnesses are selected through a voting scheme, where each Steem account can vote for other users to become witnesses. The worth of each vote is proportional to the amount of Steem Power the voting account holds. To be eligible as a witness, the user must operate a full Steem node and set the “Witness parameter” as True. From the 21 elected witnesses, the first 20 are the accounts who have received the greatest amount of votes. The last witness is selected at random among the rest of eligible accounts, where the probability of being elected is equal to the SP-weighted votes it has over the total amount of votes casted towards all non-elected eligible nodes. The list of active witnesses is updated once every 24 hours, when the votes of Steem users are tallied.

Extending the Ledger

In the Steem blockchain, one block is appended every 3 seconds. Rounds are assembled in groups of 21 slots, so each witness appends one block per round. Before each round, the list of active witnesses is known and the order of participation is randomized. If a witness fails to append their block in time, the turn jumps to the next witness. The official documentation claims that if 2/3 of the witnesses are honest, the chain will ensure its validity. In the White Paper it is also argued that if 2/3 + 1 of the witnesses have appended their block, the chain can be considered irreversible [6].

It should be noted that the properties of the chain (e.g. validity or finality) are not supported by any kind of formal description or proof. Moreover, the DPoS title might be misleading, as the operation of the consensus protocol is not related to other Proof of Stake algorithms such as Ouroboros [38] or Casper [16]. In fact, its operation resembles to a classic BFT consensus algorithm, used more in permissioned blockchains. However, it is out of the scope of this work to analyze the formal properties of Steem consensus protocol and this section only has descriptive aims.

3.3.4 Is Steem a Permissionless Blockchain?

Public or permissionless blockchains allow users to create an account (i.e. public and private key-pair) freely and without any kind of verification process. In public blockchains, the address or identifier of an account will be its public key (or a hash of it). However, the account identifier in Steem would be a handle of the form "@username", which is linked to the account key-pair. To create an account in the Steem blockchain you need to be delegated Steem Power. Therefore, Steem is effectively a member-invite distributed ledger, as only Steem accounts can hold Steem Power to delegate it to the newly created account. To create a new Steem account, an already existing Steem user has to pay a flat fee[12] of 0.1 STEEM[13] and delegate (i.e. lend) Steem Power to the new account. Therefore, we can categorize the Steem blockchain as a permissioned blockchain.

In practice, Steemit Inc. offers to pay the fees of account creation as long as the user goes through a verification process or KYC. We must acknowledge the weight of Steemit as centralizer entity in the Steem blockchain, as they can afford the allocation of funds to create accounts in exchange for users' data. On the other hand, there are other 3rd party services which let users pay the upfront fee to create an account without the need for personal verification.

3.3.5 Voting and Rewards

Voting Power

To prevent abusive voting bots and incentivize users to select their favorite content, each user has a limited influence in the system. The parameter to measure the influence

[12] The amount of the fee will be subsequently destroyed or "burned".
[13] https://steemdb.com/. Accessed: 2018-08-01.

of a vote is called voting power. We can think of voting power as a bar of influence, which can range from 0% to 100%. Each time a user executes a vote, her voting power will be reduced. The voting power bar is regenerated by the system in a predefined time interval. For a more detailed description, see Subsection 3.4.1.

Author and Curation Rewards

A fraction of the STEEM minted when a new block is produced is allocated to the so-called “Reward fund”. The Reward fund is distributed among the users of Steem to incentivize the creation and discovery of quality content. The rewards in Steem are split between:

- **Author rewards.** Allocated to the authors of posts and comments. They are proportional to the amount of votes received by a post[14].
- **Curation rewards.** Distributed to users who discover high quality content in the platform. Users will earn curation rewards if they are early voters of a post which later becomes popular in Steem (i.e. receive a lot of votes).

Reputation

Each account in Steem is linked to one reputation score. This score is defined in a log10 scale and can range from -25 to 75. Newly created accounts are set with a default reputation of 25. Users can earn or lose reputation according to the following rules[15]:

- **Increase of reputation.** Users earn reputation when they receive an upvote from another user. The increased amount will depend on the reputation and the Steem Power of the voter.
- **Decrease of reputation.** Users can lose reputation when they are downvoted by another users with a higher reputation score. Even if the downvoter has more SP than the author of the post, the loss of reputation will only become effective if they also have more reputation than the author of the post.

[14] Posts and comments are equally treated in Steem. We will use “post” for clarity purposes.

[15] https://steemit.com/steemit/@digitalnotvir/how-reputation-scores-are-calculated-the-details-explained-with-simple-math.

In practice, content produced by authors with negative reputation scores will be hidden in Steemit website. However, it should be noted that since Steem is an immutable ledger, posts from negative reputation authors will remain in the chain.

3.4 Financial Rewards on Steem

In Subsection 3.3.2 we provided a high-level and general overview of the Steem blockchain. This section aims to develop an in-depth analysis of the voting system and financial rewards in the platform. Consequently, based on our analysis from the last section, we will construct a mathematical model of the system, mapped in detail with the source code of the Steem blockchain implementation[16].

3.4.1 Economic Analysis

Inflation Model

The inflation model of currency describes the rate in which new currency is created over time. The Steem blockchain inflation model has undergone important modifications over time. From March to December 2016, Steem used PoW as consensus protocol and it minted cryptocurrency at a rate of 800 STEEM/minute [6].

In December 2016, Steem performed its 16th hard-fork (see Appendix A) updating its monetary creation rate. In the Hard fork 16, it was set that at block 7,000,000 the inflation rate of STEEM would be of 9.5% per year. The inflation rate decreases 0.01% every 250,000 blocks. When the inflation rate decreases, the amount of coins produced per block will decrease respect to previous blocks. The current value of the inflation rate is 9%. When the inflation rate reaches 0.95% it will be maintained at this value. This point of inflation will be reached on block 220,750,000 and it will approximately occur in year 2034 #L109.

The new STEEM created in each block is defined by #L1981:

$$newSteem = \frac{currentSupply \cdot inflationRate}{blocksPerYear} \tag{3.1}$$

[16]Steemit is a live project. We provide links to the file versions at the time of the writing. The actual implementation may be different at the time of the reading.

where $blocksPerYear$ and $inflationRate$ are estimated taking into account that one block is produced every 3 seconds. In Figure 3.2 we can see the evolution of the STEEM supply over the last year:

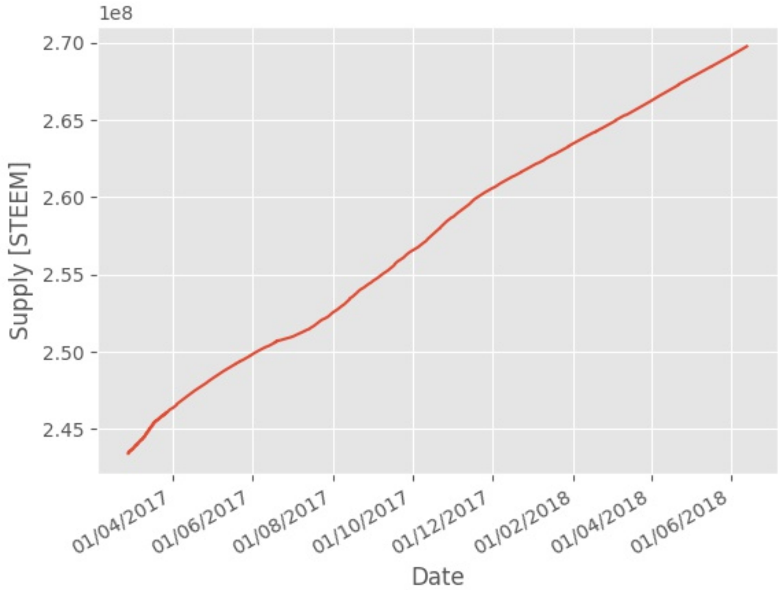

Figure 3.2: Evolution of STEEM supply (March 2017 - June 2018). Data extracted from Steem using Steem-Python library.

Allocation of New Coins

In Bitcoin, all the tokens created with each block are given to a miner. However, the Steem blockchain follows a more complex model of inflation allocation #L1982-1986. The allocation of coins for the ith block are added to the following STEEM funds:

- **Rewards fund.** $F_{R,i+1} = F_{R,i} + 0.75 \cdot newSteem$. Pool of coins to be distributed to authors and curators of content in the various platforms.
- **Vesting fund.** $F_{V,i+1} = F_{V,i} + 0.15 \cdot newSteem$. Funds allocated to the holders of Steem Power. It can be understood as a mechanism to incentivize users to hold Steem Power and reward users with large amounts of STEEM vested in the system.
- **Witness fund.** $F_{W,i+1} = F_{W,i} + 0.1 \cdot newSteem$. Funds to be split between the 21 elected witnesses of Steem.

An excerpt from the inflation model source code is shown below:

```
auto new_steem = ( props.virtual_supply.amount *
    current_inflation_rate ) / ( int64_t( STEEM_100_PERCENT ) * int64_t(
    STEEM_BLOCKS_PER_YEAR ) );
auto content_reward = ( new_steem * STEEM_CONTENT_REWARD_PERCENT ) /
    STEEM_100_PERCENT;
if( has_hardfork( STEEM_HARDFORK_0_17__774 ) )
  content_reward = pay_reward_funds( content_reward ); /// 75% to content
      creator
auto vesting_reward = ( new_steem * STEEM_VESTING_FUND_PERCENT ) /
    STEEM_100_PERCENT; /// 15% to vesting fund
auto witness_reward = new_steem - content_reward - vesting_reward; ///
    Remaining 10% to witness pay
```

Code 3.1: Inflation allocation in Steem.

Steem Currency System

STEEM is the main cryptocurrency of the platform[17]. In order to increase their influence in Steem, users must submit their STEEM to a vesting schedule mechanism, converting it to Steem Power (SP). When a user stakes 1 STEEM, it receives 1 SP. However, in the blockchain SP is reconverted into another unit of account, the Vest.

In the last section, we described how part of the newly created STEEM is allocated for the holders of SP into the Vesting fund F_V. To measure how much SP a user holds, each account is linked to an amount of "Vesting shares". The unit of account of the Vesting Shares is the Vest. The sum of the Vesting Shares of all the users determine a global variable of the blockchain, the "Total Vesting Shares" VS_{tot}. The amount of STEEM that a user has vested in the system (i.e. her SP) is calculated from her Vesting Shares VS with the following formula #L1141:

$$SP = VS \cdot \frac{F_V}{VS_{tot}} \tag{3.2}$$

[17] As described in Subsection 3.3.2, the Steem blockchain has 3 currencies: STEEM, SBD and SP. For the rest of this thesis, we will actively abstract from the use of SBD in our analysis. We have identified that Steem Backed Dollars add too much complexity and this abstraction does not harm the fundamentals of our research.

The 15% of interest created by F_V appreciates the value of SP against STEEM over time. This is an incentive for the users to have their holdings in a longer term commitment scheme in the form of SP. In the next figure we can see the evolution of the value of 10^6 vests (i.e. MVests) in STEEM (i.e. $\frac{F_V}{10^6 \cdot VS_{tot}}$), demonstrating how SP appreciates over time against STEEM due to the allocation of new coins into F_V:

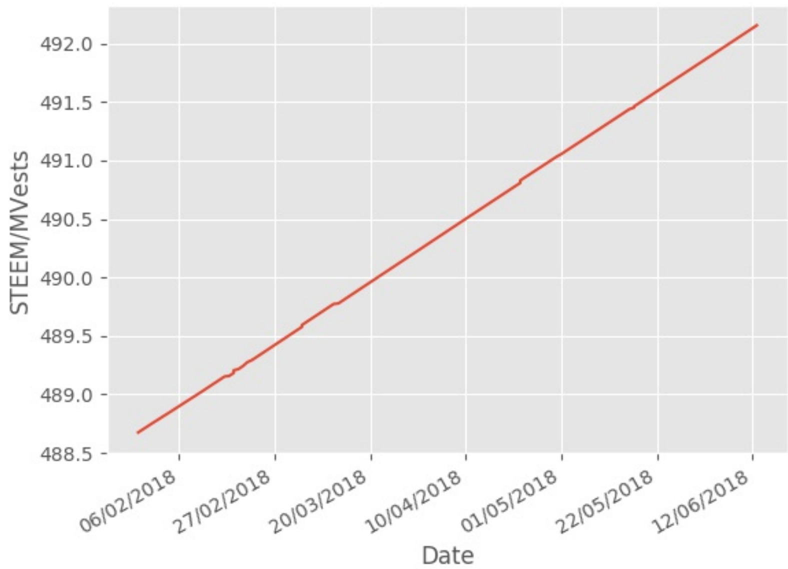

Figure 3.3: STEEM vs MVests (Feb 2018 - June 2018). Queried from Steem using Steem-Python library.

Conversions between STEEM and SP

The process of converting STEEM to SP is instantaneous, called "Power up". The inverse exchange, the "Power Down", is subject to interval withdrawals, to enforce the vesting mechanism. When a user wants to convert any fraction of their SP to STEEM (i.e. cashing out from the platform) the exchange process is segmented in 13 weeks[18]. Each week, the user can convert $1/13$ of their initial amount of SP to STEEM and the user can decide to halt the process at any time. Moreover, SP is illiquid, so it cannot be transfered between different accounts. However, users can delegate SP to other users, lending their influence for a limited amount of time. SP delegation can be understood as lending part of the SP to another user for a limited amount of time.

[18]It should be noted that before HF16, the vesting schedule extended for 2 years.

3.4.2 Voting System

Steemit uses a voting system to discern the quality of the content and distribute the platform rewards accordingly. The naive solution for a crowdsourced curation scheme would be allocating a predefined number of votes per user (e.g. 5 or unlimited) and establishing that all votes are worth the same. However, as votes in Steem have intrinsic financial value, the mentioned strategy would be vulnerable to vote spam and bots.

In Steem, each user is provided with a limited temporal amount of influence called voting power. Thus, users can perform an unlimited amount of votes, but their voting power decreases each time a vote is cast. If the voting power of a user reaches 0, her votes become worthless (see Equation 3.6). The contribution of a vote to a post is measured in r-shares. R-shares are proportional to the Steem Power of the user. Therefore, users with more cryptocurrency vested into the platform will have a greater voting influence, creating an effective Sybil resistant mechanism. [37].

Voting Power

The voting power $VP \in \{0, 1, ..., 100\}$ should be understood as a percentage bar of temporary influence of each user. When a user casts a vote at time t_{now}, the protocol verifies when was the last time she voted $t_{lastVoted}$, and calculates the elapsed time Δt #L1245:

$$\Delta t = t_{now} - t_{lastVoted} \tag{3.3}$$

After that, and prior to the vote execution[19], the voting power regeneration during Δt is calculated. The voting power is fully regenerated (i.e. from 0 to 100) in the regeneration interval $\Delta r = 5days$[20]. The regenerated power RP would be #L1251:

$$RP = \frac{\Delta t}{\Delta r} \cdot 100 \tag{3.4}$$

To calculate the current voting power (after regeneration) VP, the regenerated power

[19] There is a minimal interval between vote execution of 3 seconds.

[20] We may refer to time intervals in days for readability purposes, but all calculations are made with seconds precision.

RP is added to the original voting power (prior to regeneration) VP' #L1252:

$$VP = min(VP' + RP, 100) \tag{3.5}$$

An extract of the Steem source code which shows how the influence of a vote is calculated is shown below:

```
int64_t elapsed_seconds = (db.head_block_time() - last_vote_time).
    to_seconds();

int64_t regenerated_power = (STEEM_100_PERCENT * elapsed_seconds) /
    voting_helper->get_vote_regeneration_period();

info->current_power = std::min( int64_t(voting_power + regenerated_power),
     int64_t(STEEM_100_PERCENT) );

int64_t abs_weight = abs( vote_weight );
```

Code 3.2: Voting mechanics of Steem.

Casting a Vote

When casting a vote, a user can determine its weight $w \in \{-100, -99, .. -1, 1, ...99, 100\}$. The weight of the vote can be understood as an intensity parameter, where $w = -100$ means a full downvote and $w = 100$ a full upvote. The weighted voting power used in a vote WP is calculated as #L1258:

$$WP = \frac{VP \cdot abs(w)}{100} \cdot 1day \tag{3.6}$$

However, the effective power P deposited in the post or comment is further weighted by a constant called "Vote Denominator" V_{den} #L1261-1271 and #L261:

$$V_{den} = 10 \cdot \Delta r = 50days \tag{3.7}$$

$$P = \frac{100 \cdot WP + V_{den} - 1}{100 \cdot V_{den}} \approx \frac{WP}{V_{den}} + 0.01 = \frac{VP \cdot abs(w)}{5000} + 0.01 \tag{3.8}$$

After a user casts the ith vote, her current voting power after the vote execution is defined as the subtraction of the effective power used to its original voting power #L1575:

$$VP = VP^{'} - P \tag{3.9}$$

As an example, if a user casts a vote with full voting power $VP = 100$ and full weight $w = 100$, the power used will be $P = 2.01$.

Influence of a Vote

The influence of a vote in the platform is proportional to the effective power of the vote P and the Steem Power the user holds, which is proportional to her vested shares VS as shown in Equation 3.2. Users who have vested larger amounts in the system will cast more influential votes. The influence of a vote is measured in r-shares or rewards shares[21] RS #L1274:

$$RS = \frac{P \cdot VS}{100} \tag{3.10}$$

The calculation of the reward shares deposited by a vote is implemented as follows:

```
info->used_power = ((info->current_power * abs_weight) /
    STEEM_100_PERCENT) * (60*60*24);

info->used_power = (info->used_power + max_vote_denom - 1) /
    max_vote_denom;

info->abs_rshares = ((uint128_t(voter_effective_vesting_shares) * info->
    used_power) / (STEEM_100_PERCENT)).to_uint64();
```

Code 3.3: Calculation of the influence of a vote.

[21] It should be noted that the rewards generated by a post are only the r-shares accumulated in its first week of existence.

3.4.3 Rewards and Distribution of Payouts

Payout of a Post

Calculating the payout of a post or comment in Steem can be translated as determining which fraction of the reward fund balance F_R it attained. The reward fund is going to be split among all the posts that have been upvoted over the last week, known as the recent claims RC. RC is defined as the sum of the reward shares from all the posts submitted to the ledger in the last 7 days:

$$RC = \sum_{i \in \mathcal{P}} RS_i \tag{3.11}$$

Therefore, the payout of the ith post will be defined as #L53:

$$P_{tot} = F_R \cdot \frac{RS_i}{RC} \tag{3.12}$$

The total payout of a post P_{tot} is further distributed between the author and its curators. Authors and curators can claim their rewards when the voting period has finished (i.e. after one week of the creation of the post).

Author Rewards

The payout for the author is going to be at least $3/4$ of the payout of the post. Thus the assured author payout $P_a^{'}$ will be:

$$P_a^{'} = \frac{3}{4} \cdot P_{tot} \tag{3.13}$$

Curation Rewards

The remaining $1/4$ of the post payout is allocated to the curators. However, a fraction of the curators payout may be paid back to the author of the post. If the vote happens in the first 30 minutes of the existence of the post, the curator rewards are scaled by an auction curation window $w(t)$. To better explain the curation payout mechanics lets define the following variables:

- $RS_i \equiv$ total amount of reward shares attained by the post prior to the vote of the ith curator.
- $RS_{i+1} \equiv$ total amount of reward shares attained by the post after the vote of the curator. See equation 3.10.
- $RS_{tot} = \sum_i RS_i \equiv$ total amount of reward shares attained by the post in the voting reward interval (i.e. 1 week).

The auction curation window $w(t)$ is defined as follows #L1366-1369:

$$w(t) = \begin{cases} \frac{1}{30} \cdot t & if \quad 0 < t \leq 30 \\ 1 & if \quad t > 30 \end{cases}$$

The curation mechanics of Steem incentivize early voting in posts, as the curation rewards of a vote are weighted with the votes that the post already has. However, the auction curation window $w(t)$ is included to avoid bots upvoting content before other users have time to read it. The reward shares awarded to a curator when she votes a post, will be defined as R_c #L68 and #L51:

$$R_c^{'} = \frac{\sqrt{RS_{i+1}} - \sqrt{RS_i}}{\sqrt{RS_{tot}}} \tag{3.14}$$

This quantity is weighted by the auction curation window, to get the final curation rewards #L1371:

$$R_c = w(t) \cdot R_c^{'} \tag{3.15}$$

Recalling that curators are entitled to $1/4$ of the payout of a post, the payout of a curator will be defined as:

$$P_c = \frac{P_{tot}}{4} \cdot R_c \tag{3.16}$$

As noted before, the rest of the curation rewards, lost by the votes cast within the curation window are paid back to the author. Therefore, the final rewards attained by the author of the post, where $P_c^{'}$ is the payout of the curator before the weighting of the auction curation window, will be #L1722:

$$P_a = P_a^{'} + \sum_i (P_c^{'} - P_c) \tag{3.17}$$

3.5 Summary

In this chapter, we have performed a thorough analysis of the Steem blockchain, with a particular focus on its economic model. We have identified the Steem blockchain as not fully permissionless, which questions the degree of decentralization of the system. We have also described the consensus protocol of Steem, aiming to categorize it within the taxonomy of blockchains of Xu et al. [62].

However, we acknowledge that we have made some simplifications to develop a more meaningful analysis. The role of the SBD currency has been neglected. Although we think that the fundamentals of our research would not change with its inclusion, we cannot guarantee it with certainty. Another caveat in our analysis is that we have mainly focused on the current implementation of the Steem blockchain. In Appendix A we have gathered relevant changes of the project in a table with the most important hard forks of the blockchain history. To provide a more accurate picture of the system, an in-depth analysis of older states of the platform could be performed (e.g. the effects of the modification of the inflation model). We regard this as interesting related work for the future.

The mathematical analysis of the rewards and curation system based on the source code of the project has provided us with some valuable insights. The rewards system is based in two core ideas: the Voting Power and the Steem Power. The main purpose of these concepts is to resist the effects of Sybil accounts and to provide a fair distribution of rewards proportional to the vested amount of the player in the platform. Along these lines, the incentives of early voting in Steem (see Equation 3.14) are also essential to promote the discovery of valuable posts and an overall curation quality. In the next chapter, we will identify some potential issues with the rewards system of Steem.

Chapter 4

Issues and Potential Attacks on the Rewards System of Steem

The main objectives of the curation and rewards system of Steem blockchain are: a) guaranteeing the quality of the curation and the discovery of high-quality content in the platform and b) enforcing a fair distribution of rewards among the users of the system. We are going to frame as a potential attack any behavior that deviates from the protocol which can harm any of these properties. The protocol of Steem can be understood as the process of voters rewarding the content they regard as more valuable. First, we provide a background on relevant social media attacks and point out the differences with Steemit. Then, we identify and evaluate the main issues with the reward system of Steem, and propose and implement a solution for the moderation in Steemit in chapter 6.

4.1 Introduction

4.1.1 Security Issues of Social Media Platforms

Social media platforms have emerged as a critical infrastructure in our society and online lives. At their core, they are built on trust, and the social graphs and user-generated content produced within their systems are their most valuable assets. Kayes and Iamnitchi analyzed the security and privacy aspects of traditional social networks [37]. They characterized attacks on social networks in two main categories: attacks on the users and attacks on the platforms. The potential attacks on the platforms are further segmented as:

- **Sybil attacks.** Creation of multiple fake identities to disrupt the functioning of the platform.
- **Crawling attacks.** Distributed aggregation of personal information from the users of the platform.
- **Social spam.** Propagation of content of low quality or that users do not want to see. It can hurt the resources of the platform.
- **Distributed Denial-of-Service attacks (DDoS).** Overloading the service of the platform with a massive amount of distributed requests.

4.1.2 Steemit, a Different Security Paradigm

Steemit, as a social media platform, is subject to some of the attacks described above. For example, crawling attack do not apply to the Steemit case, as all the information is already publicly available in the Steem blockchain. Moreover, Steem establishes a threshold on the maximum number of posts a user can publish to avoid a subset of denial-of-service issues. On the other hand, the decentralized architecture of Steem creates a new security paradigm for the platform. In traditional social networks, the owners of the platform can actively implement measures to avoid the effects of spam or detect if they are being subject to a DDoS attack. In Steem, the design of its protocol must predefine a set of rules to align the incentives of its users and ensure the stability of the platform.

The element which provides the set of rules and incentives to Steem users is its rewards and voting system. At a high level, these are the main design decisions of the rewards and voting system in order to prevent the potential attacks described in the last section:

Sybil Attacks

- Flat fee of 0.1 STEEM to create an account in Steem.
- Minimum amount of Steem Power required to create posts and comments.
- Voting influence and rewards proportional to the Steem Power of the user.

- Reputation score linked to each account.

Social Spam

- Curation rewards for high-quality content.
- Social graph: Users can follow other users.
- Flagging system to punish inappropriate content.

New Set of Vulnerabilities

However, apart from the vulnerabilities of traditional social networks, the financial incentives in Steem create a new spectrum of possible attack vectors. Steem relies on the correct functioning of its curation system to provide a platform with valuable content and where rewards are distributed in proportion to the value created. Based on our analysis of the rewards system in Chapter 3, we have looked for potential vulnerabilities in the system, which can disrupt its correct functioning. We have identified 3 main issues: self-voting, voting bots and censorship abuse. In the following sections, we will describe each issue in more depth and propose a solution to the censorship and moderation problem of Steem in Chapter 6.

4.2 Self-Voting

Self-voting occurs when a user upvotes their own content. Steem allows its users to self-vote. While this cannot be regarded as an intrinsic flaw in the protocol, if self-voting abusively is profitable, there are no incentives for rational players to follow the curation system and look for high-quality content. We will describe the potential issues linked to abusive and systematic self-voting patterns, not to eventual upvotes of a user valuing its own content.

4.2.1 Economic Analysis of Self-Voting

In Steem, users can only deposit one vote per post/comment. However, a malicious user can create dummy content with the only purpose of upvoting himself. González demonstrated how self-voting can be profitable in Steem [33]. Based on these insights, we show analytically the profits of the abusive self-voting pattern using our analysis of Section 3.4.

In Equation 3.10, we determined that the reward shares corresponding to one vote are:

$$RS = \frac{P \cdot VS}{100} \tag{4.1}$$

Let the attacker always vote with $w = 100\%$ in her posts. Also, let the attacker optimize her voting power VP, voting at $VP = 100\%$ in intervals of $\Delta t_v = 144min$. Using the results of Equation 3.12 from Chapter 3, the payout of a self-vote can be defined as P_{sv}:

$$P_{sv} = VS \cdot \frac{P}{100} \cdot \frac{F_R}{RC} \tag{4.2}$$

where VS are the Vesting shares the player has vested in the platform. The VS can be converted to SP using Equation 3.2. Therefore, the rewards from a vote can be rewritten as:

$$P_{sv} = SP \cdot \frac{P}{100} \cdot \frac{F_R \cdot VS_{tot}}{RC \cdot F_V} = SP \cdot \frac{P \cdot D}{100} \tag{4.3}$$

where $D = \frac{F_R \cdot VS_{tot}}{RC \cdot F_V}$ only depends on global variables of the blockchain such as the number of Vesting shares the users hold or the size of the Reward Fund F_R.

Taking in account that the user performs all her votes with full weight and full Voting Power, the power used will be $P = 2.01$ (see Equation 3.8). Then, Equation 4.3 can be rewritten as:

$$P_{sv} \approx SP \cdot \frac{D}{50} \tag{4.4}$$

To measure the profitability of self-voting over a year, we calculate the number of 100% weighted votes a user can do in a year:

$$n = \frac{Year(mins)}{\Delta t_v} = \frac{365 \cdot 24 \cdot 60}{144} = 3650 \tag{4.5}$$

Therefore, we can calculate the yearly compound interest of SP using Equation 4.4:

$$SP_{year1} = SP \cdot (1 + \frac{D}{50})^{3650} \tag{4.6}$$

We have queried the Steem blockchain using the Steem-Python library to see how profitable would be abusively self-voting at the time of this writing using the strategy described above:

Dates	**D**	SP_{year1}
2018/07/21-25	0.0032	1.19

Table 4.1: Analysis of the profitability of self-voting. Data extracted from the Steem blockchain using Steem-Python library

Assuming that D is remains stable, the gains of SP over a year would be 19% of the initial SP. The profitability of the self-voting strategy depends of the global variables of Steem grouped in D, but it will be always positive in terms of SP. However, if the majority of the users followed this strategy the curation protocol of Steem would be damaged, decreasing the added value of the platform. If this resulted in a decrease of demand, the price of STEEM would decrease against other currencies [14]. Self-voting leads to a gain in rewards but can harm the overall quality of the platform. The dynamics and equilibriums between these strategies will be further developed in Chapter 5.

4.2.2 Voting Rings

Rings are voting structures where different users of a social media platform cooperate and deliberately exchange votes among themselves. This type of attack on the reward and reputation system of a social network is more easily implementable in platforms like Twitter or Reddit, where there is a a one-to-one mapping between users and votes.

The next figure shows a diagram of the structure of a voting ring:

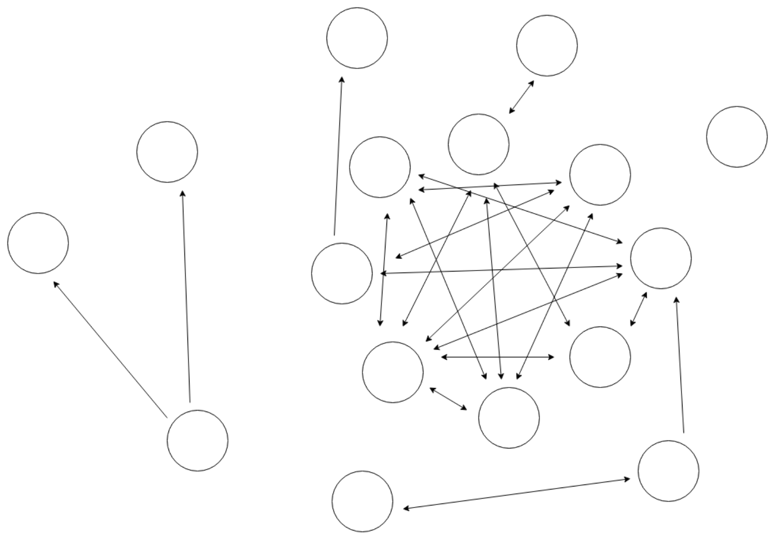

Figure 4.1: Graph diagram of a voting ring.

The worth of a vote in Steem is weighted with the Steem Power of the user. This design decision makes the system more resistant against the effect of Sybil accounts which could potentially participate in voting rings. In this scenario, a rogue user can create several accounts and then delegate SP among them, distributing the influence of each account and obfuscating his activity. This network of Sybil accounts could be constructed as a voting ring. However, the financial rewards on the platform may be sufficient motivation to create voting rings between legitimate users. The curation protocol does not enforce any type of prevention to decrease the impact of these voting structures. One of the solutions proposed by members of the Steemit community is to apply an extra weight voting parameter, so when a user repeatedly votes for the same account its votes have less influence [34].

4.3 Censorship and Moderation

Steemit aims to be a decentralized social media platform and lets the users alone regulate the content which appears in the network. The inclusion of content in the blockchain is censorship resistant, as users can include arbitrary posts in the transactions they submit to the ledger. However, the main graphical user interface for the ledger (i.e. Steemit) orders the visibility of the posts according to the worth of the votes deposited on them. Posts with low or negative reward shares will be effectively hidden from the front pages of the site.

4.3.1 Moderation in Steemit

If content curation aims to discover and order content in terms of value, moderation can be understood as a binary choice: whether the content is legitimate or not. Steem does not have any specific protocol for self-moderation besides legitimate users downvoting inappropriate content. As an example, if big stakeholders detect an abusive use of self-voting, they may target the self-voter with flags and downvotes, nullifying their rewards in the platform and punishing their reputation. We regard this more as a patch than as an actual solution to the moderation problem of the platform. Steemit relies on the intrinsic motivation of big stakeholders to act as moderators [6]. It should be noted that from a strategic perspective, downvoting is the worst economical decision. Using Voting Power as a downvote decreases the potential curation rewards, so when a user executes a downvote, the user is actually losing the opportunity to earn rewards from their Voting Power.

A parallel and more refined approach to the moderation problem has been the creation of moderation bots[1]. Altruistic users can delegate SP to moderation bots, which will search programmatically for unsuitable content in the platform. Although moderation bots represent a more sophisticated approach to moderation, it relies again in users acting against their economic incentives and behaving altruistically. Moreover, moderation bots may be closed-source and possibly centralized, so their moderation policies are subject to the interests of the owners of the bots and may contain implementation errors.

4.3.2 Downvoting Wars

The payout and the visibility of the post is determined by the amount of r-shares deposited on it. A downvote deposits a negative amount of r-shares. Large stakeholder can arbitrary mute and nullify users with less stake in the system, regardless of whether their content is legitimate or not. There is no mechanism in Steem to prevent this kind

[1] https://steemit.com/steemcleaners/@steemcleaners/announcing-steemcleaners-the-steemit-abuse-fighting-team.

of abusive behavior from large stakeholders. Moreover, any user can pay a bid bot (see Section 4.4) to effectively censor the activity of any user. This behavior is called a "downvoting war" and resembles the editing wars described by Yasseri et al. in Wikipedia [63].

4.4 A Survey of Voting Bots in Steemit

A bot is a software application which automates tasks and behaves according to a set of programmed rules. The influence of voting bots in Steem is considerable. As an example, from the top-10 accounts in terms of curation rewards earnings during the period 2018-07-01 and 2018-08-01, 8 of them are voting bots[2]. We have identified 4 types of bots in Steemit:

- **Curation bots.** Bots which automatically vote for posts or comments which are likely to be successful based on predefined parameters. Thelwall showed that posts which contain keywords like "steem" or pictures are more likely to achieve greater rewards [59]. Therefore, a curation bot could be adjusted to selectively vote for posts which fulfill these metrics. Curation bots are mostly run by individuals aiming to optimize their voting power. Although they may harm the overall quality of curation, the presence of curation bots is impossible to avoid.
- **Delegation bots.** These bots tend to accumulate great amounts of SP through the influence delegation of one or more stakeholders. Then, users can send STEEM to this bot to choose a target post to be voted. This effectively creates a secondary marketplace where users can rent SP in the platform. As previously mentioned, the existence of these bots may alter the curation quality and generate downvoting wars.
- **Bid bots.** A particular type of delegation bots are Bid bots. Between each vote execution of the bot, the bid bot accepts SBD/STEEM from any amount of users. When its voting power is fully regenerated, it splits a 100% vote between all of the bidders based on the fraction of the total bids they sent. This is by far the most common type of bot in Steemit. Users can choose which bid bot is more suitable for them in bid bots marketplaces such as Steem Bot Tracker.

[2] https://steemdb.com/labs/curation?grouping=monthly.

- **Moderation bots.** As already described in Subsection 4.3.1, moderation bots are a particular kind of delegation bots. Users altruistically delegate SP to these bots (i.e. no financial returns expected). The objective of moderation bots is to detect inappropriate posts in the platform and downvote them to punish their authors in rewards and popularity. An example of a popular moderation bot is Steem Cleaners.

4.5 Conclusion

In this chapter we have analyzed the main potential attacks and deficiencies of the rewards and curation system of the Steem blockchain. We have showed that the abuse of self-voting can be profitable and how this behavior can be hidden behind voting structures such as voting rings. Even though self-voting can lead to better rewards, we have not demonstrated that this strategy is in any way *optimal* for long-term financial rewards on the platform.

After that, we evaluated the moderation and censorship issue in Steemit. At the end of the chapter, we have developed a taxonomy of the voting bots present in the social media platform, pointing out the noticeable influence they have in the curation of posts. Based on these insights, in Chapter 5 we aim to develop a formal model to better understand the impact of the described issues on the quality of curation in Steemit.

Chapter 5

Modeling Steemit as a Game

In this chapter we model Steemit as a strategy game where users create and vote for posts. Steemit can be modeled as a game[1], where there is a finite pool of rewards to be split among the users of the system. For this purpose, our model inherits important concepts of the Steem blockchain such as Voting Power or Steem Power, but abstracting other components of the system like the currencies STEEM or SBD. Our aim is to create a game based on Steem, which also describes more general voting dynamics of financially incentivized crowdsourced curation systems.

5.1 Game Description

The game is constituted of N players, and each player creates exactly one post, as a simplification of our model. The players cast votes in rounds following a defined strategy. There is a predefined number of voting rounds. After each player casts their votes, the list of posts is ordered by votes received. Honest players vote for posts they like and greedy players form voting rings and aim to maximize the position of the posts from their ring. After all the rounds have been executed, a payout is distributed among players based on the position of their post in the list of posts.

[1] We use the terms "game" and "model" interchangeably. The term "game" does not refer to the game-theoretic definition.

5.2 Properties of the Game

5.2.1 Players

The are $N \in \mathbb{N}^*$ players in the model. A player u is defined by its Steem Power SP, its Voting Power VP, its Likability Distribution L and its Strategy S. Let the ith player be characterized by the following tuple

$$u_i = (SP_i, VP_i, L_i, S_i),$$

where $SP \in \mathbb{N}$, $VP \in [0,100]$, $L \in \mathcal{D}\left([0,1]^N\right)$ and $S \in \{H,G\} \times [100] \times 2^{[N]}$[2]. The tuple of players is defined as $\mathcal{U} = (u_1, ..., u_i, ..., u_N)$ and each player is identified by their initial index in $\mathcal{U}$.

To summarize each player u_i, where $i \in [N]$ can be described as follows:

- **Steem Power.** The Steem Power funds of player u_i are defined as $SP_i \in \mathbb{N}$ and represented the influence of the player in the platform. The vector of Steem Power funds for the N players is defined as $\mathcal{SP} = (SP_1, ..., SP_i, ...SP_N)$.
- **Voting Power.** The Voting Power of a player u_i is defined as $VP_i \in [0,100]$ and it can be understood as a temporal bar of voting influence of the player in Steem. The vector of Voting Power for the N players is defined as $\mathcal{VP} = (VP_1, ..., VP_i, ...VP_N)$.
- **Likability Distribution.** The "Likability Distribution" L_i of player u_i determines how likely is the jth player to like a post created by u_i. Defined as $L_i \in \mathcal{D}\left([0,1]^N\right)$, it determines a distribution on how likable is the content produced by u_i to the rest of the players. The Likability Distribution for the whole system is $\mathcal{L} = (L_1, ..., L_i, ..., L_N)$.
- **Strategy.** The strategy of player u_i is defined as $s_i \in (\{H,G\}, MinVP, R)$, where $\{H,G\}$ is the core strategy of the player, $MinVP$ is their VP threshold and R their voting ring.
  - **Honest/Greedy.** The tuple $\{H,G\}$ characterizes the core strategy of a player, where $H \equiv$ *honest* and $G \equiv$ *greedy*. An *honest* player votes according to the Likability Distribution $\mathcal{L}$, that is to say she votes to the

[2] We denote the powerset of a set A with 2^A.

posts she likes. For *Honest* players, the value of the vote is computed as $v_{H,i} = VP \cdot l \cdot SP$, where l is defined by the Likability distribution. In Steem terms, l can be understood as the weight of a vote. A *Greedy* player casts votes to posts produced by users of its Voting Ring. The value of vote for a player if u_i is *Greedy* is defined as $v_{G,i} = VP \cdot SP$, as all the votes are executed with full weight.

- **Ring.** If player u_i is *Honest*, her Voting Ring is $R_i = \emptyset$. If player u_i is *Greedy*, her Voting Ring is $R_i \in 2^{[N]}$. A voting ring is defined as $R_i = \{g_i, ..., g_j, ..., g_n\}$, where$g_j \in \mathcal{U}$ is the jth member of the voting ring and n is the size of the ring.

- **MinVP.** Minimum Voting Power a user allows herself to reach, defined as $MinVP \in [0, 100]$. When a user cast a vote, its Voting Power decreases. A player u_i casts votes in a round as long as $VP_i > MinVP_i$.

Ultimately, the tuple of the strategies for the N players is defined as $\mathcal{S} = (S_1, ..., S_i, ...S_N)$.

5.2.2 Posts

A post is defined as $p = (i \in [N], l_i \sim L_i, votes \in \mathbb{N})$:

- **Author.** Each player can create one post. The post created by u_i is defined as p_i.
- **Likability.** The likability of a post is defined as $l_i \in [0, 1]^N$, where $l_i \sim L_i$ is retrieved at random following the "Likability Distribution" of player u_i.
- **Votes received.** It refers to the total value of the votes received by the jth post. The amount of votes received by post j is defined by $V_j = \sum_i v_i$, where V_i is the value of the ith vote.

The set of all posts created in the system will be then[3] $\mathcal{P} = ||_{i=1}^{N} p_i$.

[3] $a \, || \, b$ denotes the concatenation of a and b.

5.3 Game Execution

5.3.1 Description

In this model there exists a set of N players. Each of the players has an initial amount of Steem Power (SP) and Likability distribution in [0,1] for each of the N players of the game. The Likability distribution can be understood as how probabilistically likable is going to be a post created by the player for each of players in this setting.

Players have associated balances of Voting Power (VP)[4] and Steem Power (SP), emulating the voting mechanics of Steem described in Chapter 3. However, our model operates in only one currency, SP, avoiding the use of STEEM and SBD for simplicity. Each player is further characterized by their strategy, either "honest" or "greedy". Honest players vote according to the Likability distribution, voting for the posts they like until they reach a minimum level of VP. Greedy players only vote for the posts created by the players who are part of their voting ring (see Subsection 4.2.1), and also keep casting votes until they reach their minimum VP threshold.

At the beginning of the execution of the game, each player creates exactly one post, with a Likability drawn from the Likability distribution. Prior to the execution, posts are shuffled, so the initial ordering of the posts is randomized. Then, players vote for posts following their strategies for a number of predetermined rounds (i.e. in Steem the voting round interval is 3 seconds). When a player votes, it processes the list of posts from the first to the last, and votes the ones that match their strategy while she has enough Voting Power. Moreover, it is not allowed to vote twice for the same post. After a player completes her voting slot, the votes are tallied and the list of posts is reordered according to the value of the votes received. The game ends when all the rounds in the game (i.e. in one week) have been executed.

At the end of the execution, the outcome is a list of posts ordered by the value of votes received. The designer of the game wins if the order of the posts is similar to the best order, as given by the average Likability of each post. If greedy players can place low-quality posts of their voting ring in high positions of the final order, they take points from the designer.

[4] We do not take voting power regeneration into account.

5.3.2 Algorithms

The game is formalized in 4 algorithms:

Algorithm 1 Each player creates a post according to their Likability Distribution

function GENERATEPOSTS($N, \mathcal{L}$)
  $\mathcal{P} = []$ ▷ List of posts
  for $i \in N$ **do**
    $l_i \xleftarrow{R} \mathcal{L}_i$ ▷ Get likability of posts
    $p \leftarrow (i, l_i, 0)$
    $\mathcal{P} \leftarrow \mathcal{P} \| p$ ▷ Add post to list of Posts
  end for
  $\mathcal{P} \leftarrow$ SHUFFLE($\mathcal{P}$) ▷ Shuffle the order of Posts
  return $\mathcal{P}$
end function

Algorithm 2 Player casts votes according to her strategy and until she reaches her Min Voting Power

```
function VOTE(i, 𝒫)
    switch s do
        case Honest
            for (author, l, V) ∈ 𝒫 do                       ▷ Iterate over all the posts
                if VP_i > MinVP_i then                      ▷ User votes if has enough VP
                    vote ← VP_i · l_{i,p} · SP_i            ▷ Calculate value of the vote
                    V_p ← V_p + vote                        ▷ Add vote to votes received.
                    VP_i ← VP_i − (VP_i · l_{i,p})/100      ▷ Recalculate VP
                end if
            end for
        case Greedy
            for (author, l, V) ∈ 𝒫 do                       ▷ Iterate over all the posts
                if author ∈ R_i ∧ VP_i > MinVP_i then       ▷ If post belongs to voting ring and not reached MinVP
                    vote ← VP_i · SP_i
                    V_p ← V_p + vote                        ▷ Add vote to votes received
                    VP_i ← VP_i − VP_i/100                  ▷ Recalculate VP
                end if
            end for
    return 𝒫
end function
```

Algorithm 3 Execution of votes by the players over the number of predefined rounds

function CURATE($N, \mathcal{SP}, \mathcal{S}, \mathcal{P}, rounds$)
    $\mathcal{N} \leftarrow [1, ..., N]$
    for $round \in rounds$ **do** ▷ Vote while there are rounds left
        $\mathcal{N} \leftarrow$ SHUFFLE($\mathcal{N}$) ▷ Randomize order of player participation
        for $i \in \mathcal{N}$ **do**
            $\mathcal{P} \leftarrow$ VOTE($i, \mathcal{P}, s, sp$) ▷ Player i votes for posts
            $\mathcal{P} \leftarrow$ ORDER($\mathcal{P}$) ▷ Order posts by value of votes received
        end for
    end for
    return $\mathcal{P}$
end function

Algorithm 4 Main protocol for the curation of posts in Steem. It represents one week of voting and each player creates only one post. At the end of the week, a payout is distributed according to the final ordering of posts by value of votes received

function PROTOCOL($N, \mathcal{SP}, \mathcal{L}, \mathcal{S}, rounds$)
    $\mathcal{P} \leftarrow$ GENERATEPOSTS($N, \mathcal{L}$)
    $\mathcal{P} \leftarrow$ CURATE($N, \mathcal{SP}, \mathcal{S}, \mathcal{P}, rounds$)
    $SP \leftarrow$ PAYOUT($\mathcal{P}$) ▷ Distribute payouts based on the final ordering of posts
end function

5.4 Discussion

In this chapter, we have modeled Steemit as a strategy game. This formal model may be used in the future to analyze whether the content curation of posts in Steemit is incentive-compatible. In particular, it provides an appropriate infrastructure to argue whether the posts of the highest quality would rise to the top of the list of all posts when players vote strategically in order to maximize their expected revenue. Based on the mechanics of Steemit, our game provides a general framework to better understand the dynamics of crowdsourced content curation when monetary rewards are present.

Chapter 6

Moderation Protocol Proposal

6.1 Introduction

In this section we propose a solution for the moderation and downvoting wars issues of Steemit. In short, the idea is to create a prediction market for the moderation of content in Steem. Using prediction markets as a mechanism for content curation was first proposed by Buterin and our moderation protocol is heavily inspired by its core ideas [15].

Based on that, we have designed and implemented a moderation protocol potentially compatible with the Steem blockchain. Although the design properties of our proposal followed the functioning patterns of other components of the Steem rewards system (see Subsection 3.4.1), we have implemented our design as an Ethereum smart contract. We have preferred to highlight the properties and implementability of our design providing a working Proof of Concept than actually building on top of the Steem blockchain source code. We have identified the latter as far beyond the scope of this work, but we want to reaffirm that a similar mechanism could be implemented as a Steem hard fork.

6.2 Background and Related Work

6.2.1 A Primer in Smart Contracts

First proposed by Szabo [55], a smart contract is a set of rules and premises executed by code. Effectively, they are just computer programs which computationally enforce a set of hard-coded rules, allowing users to programmatically handle monetary value. In the case of Ethereum, contracts are programs linked to an Ethereum address. Once the smart contract is deployed in Ethereum's network, any user can interact with it and when procedures of the contract are called, the execution is performed redundantly in every node of the network [61]. A deeper introduction to smart contracts on Ethereum and their main caveats was published by Delmolino et al. [25].

As an example of a simple smart contract, the next code snippet shows a simple implementation of a domain name system in Ethereum as in [51]. It is written in Solidity, the most widespread contracts-programming language in Ethereum:

Code 6.1: Domain name registry in Solidity as in [51]

```
contract DomainRegistry {

 mapping (string => string) domains;

 function registerDomain (string name,string value) returns boolean {
  if (domains[name] == 0) {
   domains[name] = value;
   return true;
  }return false;
 }

 function getDomain (string name) returns string {
  return domains[name];
 }
}
```

As noted in Chapter 2, Ethereum is "Turing complete", so it has support for loops and recursive functions. To overcome the obvious denial-of-service vulnerability, the concept of gas was introduced. Ethereum's gas can be understood as the costs of executing an operation in the Ethereum network. For each transaction, there is a gas price specified by the user, which is paid upfront in Ethereum's native cryptocurrency, Ether [61].

6.2.2 Related Work

Prediction markets can be an effective tool as decision support systems [12]. As previously mentioned, Buterin proposed how markets could be used to improve crowd-sourced content curation [15]. Motivated by the widespread presence of Sybils, scams and spam content in Twitter and Reddit, he argued that content curation markets would establish economic incentives for regular users to help with the moderation of these sites. Our moderation proposed design is inspired by Buterin's work, but applies these ideas for the particular case of the Steem blockchain.

Along these lines, there are other projects which are exploring different governance models in blockchain networks. For a deeper exposition of this subject, see [27] and [13].

6.3 Design of the Scheme

6.3.1 The Problem

Steem uses financial incentives both for rewarding content creators and curators. The curation mechanics of Steem are combined with a reputation system to ensure the following, as described in our IPP [47][1]:

1. Discover and reward high-quality content.
2. Avoid spam content.
3. Detect impersonation and malicious uses.
4. Penalize illegitimate content (e.g. illegal, hateful or harmful content).

However, in the curation system of Steem, rewards are only given to users who up-vote other content. The platform relies in the intrinsic motivation of large stakeholders to detect and downvote spam or inappropriate posts [6]. We have observed that this

[1] The four protocol requirements have been exactly replicated from our IPP.

asymmetry of extrinsic incentives can be harmful to the overall quality of the platform. Therefore, a mechanism to enforce points 2-4 is necessary. The lack of central administrators in a decentralized platform needs to be overcome by incentives for the community to self-regulate itself [47].

At the same time, a self-moderated community must avoid potential arbitrary censorship between peers with different influence on the platform. The current curation system of Steem does not protect average users from large stakeholders on the system. Through downvotes, the so-called "whales" can effectively nullify the influence of weaker users. Moreover, voting bots enable average users to execute more powerful votes, creating the possibility of widespread downvoting wars (see Subsection 4.3.2).

6.3.2 Proposed Solution

Our proposed solution lies in the creation of a hybrid curation system, separating the curation of the quality of the content and the curation of the suitability of the content or moderation. Designing a solution as a betting market seems intuitive for Steem, as its curation system behaves already effectively as a prediction market, since users do not upvote or downvote content reflecting their opinions on the quality of the content, but they try to predict which posts are going to be popular in Steemit and upvote in consequence.

We propose the creation of virtual markets linked to content, which are triggered when a flag is "raised" against the post [15]. Users can earn rewards betting in the markets and behaving as moderators of the platform. A small fraction of the Reward Fund of Steem can be allocated to prefund these markets. To avoid abuse from big stakeholders and to enforce the honest behavior of the participants in the market, the Moderators of Steem[2] (see Subsection 3.3.3) will make the final decision on a small subset of the moderation markets. These mechanics are already observable on Steemit. The race between users to predict which posts are going to be upvoted resembles this market approach. The moderation parties on the Steemit platform are effectively the biggest stakeholders of Steem Power, as they account for a big percentage of the prospective voting power on a post.

[2]In our solution, the Witnesses of Steem could represent the moderation parties and both terms will be used interchangeably.

6.3.3 Design of the Protocol

The mechanics of such a system were outlined in our IPP [47][3]:

1. User makes a post/comment.
2. If the post receives a downvote (or flag), a virtual market associated with the event is created.
3. Users can bet for or against the flag (against meaning that they think the post is appropriate/legitimate).
4. If the post has a determined ratio of downvotes, it is filtered out of the front-end of the platform (e.g. Steemit).
5. A moderation party decides about the outcome (which users win the betting process) in a small percentage of virtual markets. There is also a betting threshold where the moderation party always participates, to avoid abusive betting behaviors from big stakeholders.
6. After the betting and the (possible) moderation party decision, bets are redistributed according to the results of the decision of the Moderation party or the results of the market. See Figure 6.1.

[3] The mechanics of the protocol were outlined in our IPP. However, the details of the protocol have been slightly modified.

The next figure shows a flow-diagram describing the mechanics of the moderation protocol scheme, providing a mapping to the relevant functions in our implementation:

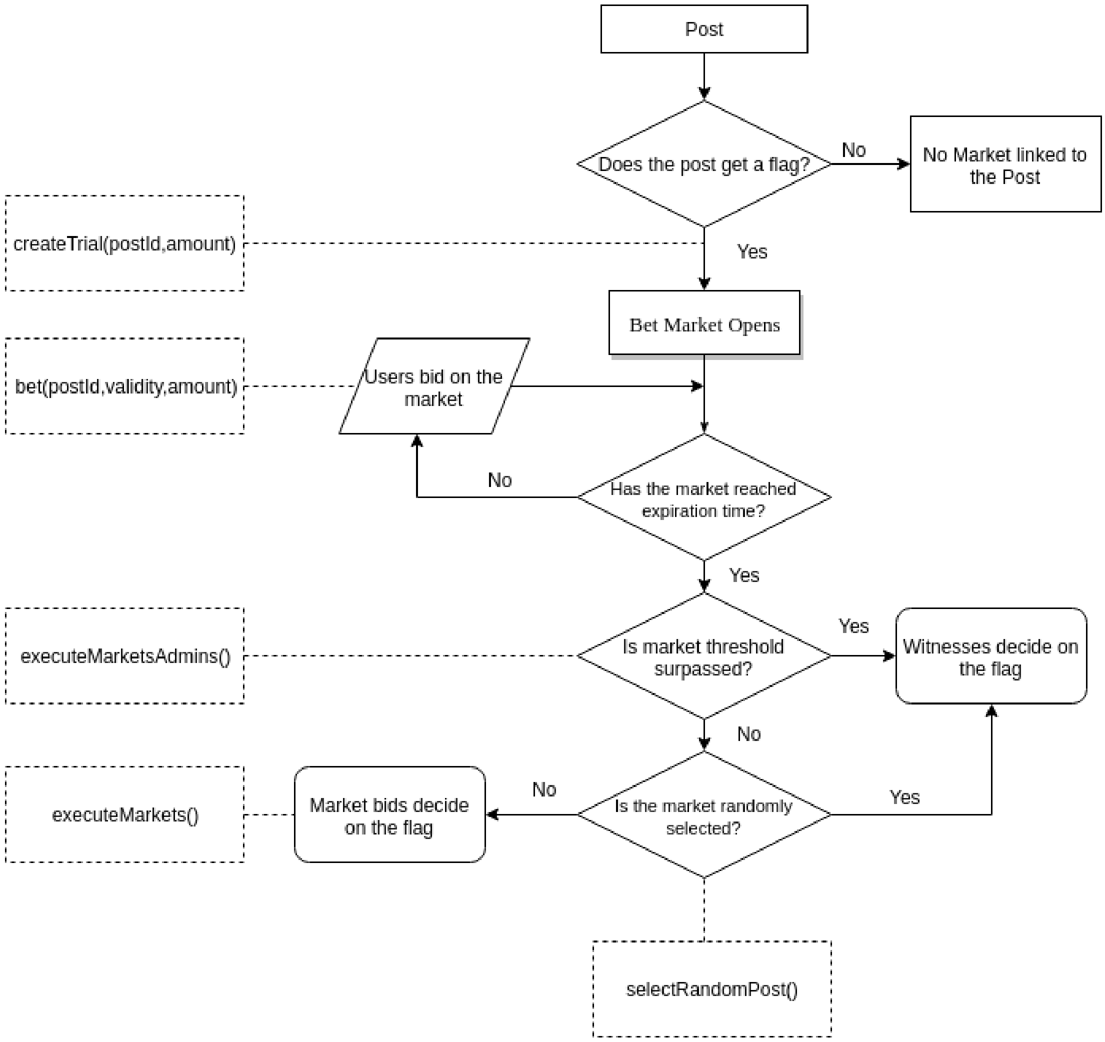

Figure 6.1: Flow chart moderation protocol. The dotted figures map the diagram with the relevant functions of our implementation.

Our solution enforces the self-regulation and curation of the content in a social media platform. Users are incentivized to actively report and detect illegitimate behavior, producing a powerful tool to detect Sybils and inappropriate content. Moreover, users who lose bets or have produced posts which are filtered out would have their reputation damaged, as already performed in the current implementation of the Steem protocol.

6.4 Construction

Implementation as a Smart Contract

The implementation of the moderation protocol can be found in the following GitHub repository Moderat.sol. The smart contract implementation can be found in Appendix B, where we have omitted comments and documentation for conciseness. It is written in Solidity, with a length of 400 lines of code including comments and documentation.

6.4.1 High-level Description

The smart contract core component is a mapping of *Post IDs* and *Markets*. The main parameter of a Market is its State. Markets can be Open, Closed and Resolved.

- **Open.** Time interval within which users can submit their bets. Default initial state when post is flagged.
- **Closed.** No more bets are accepted and the market awaits for resolution. The state of the Market changes from Open to Closed when the betting time is surpassed or the maximum bet pot is reached.
- **Resolved.** The payouts are distributed according to the outcomes and the market is archived. The state of the Market changes from Closed to Resolved when the market or the moderators decide the outcome of the flag.

As described above, the set of moderators (i.e. the Witnesses of Steem) will decide the outcome of a market if it surpasses a certain pot threshold. Moreover, Witnesses will decide in a random subset of small-pots markets, which will be selected at random. Only one market per post can be created. For a more detailed description of the contract, see the comments on the file Moderat.sol.

6.4.2 Key Points of the Contract

- The bets on the smart contract are performed in *Ether*. We could think analogously in terms of Steem's r-shares.
- To incentivize early participation in its curation system, the Steem blockchain weights the curation rewards with the votes that a post already had (see Equa-

tion 3.14). To emulate this behavior, the Moderat contract weights the value of bets with the time elapsed since the market creation #L380.

- The contract compensates the gas costs of the creator of the market (i.e. the user who executed the flag) with an allocation of rewards. We have assumed that the contract was prefunded, as an analogy to Steem's Reward Fund, to cover these expenses (see #69).

6.5 Assumptions and Limitations

Our moderation protocol proposal for Steem is a Proof of Concept. We have focused on developing a working implementation of the protocol, but there are several details which would require extensive further study prior to a real world deployment. We are going to divide our evaluation in two parts: protocol-level analysis and implementation-level issues.

6.5.1 Protocol-level Issues

Mechanism design is a complex science, and we have not aimed to develop proofs and a formal framework of the incentives compatibility of the scheme. This analysis is out of the scope of this work, but stands out as interesting related future work. However, it is noteworthy to collect open questions and the main caveats in our design:

- The optimal time length of the betting and voting intervals. An equilibrium must be found where the protocol can moderate content effectively while allowing the participation of a meaningful amount of people.
- The definition of the fraction of the markets which are randomly selected for the moderators to decide on them. It should be big enough to incentivize users to vote according to the rules of the platform. At the same time, if we expect the majority of Witnesses to participate in the decision, it cannot be too big. Along the same lines, a reward must be allocated for moderators with high participatory levels without creating incentives for the Moderators to compromise the moderation quality.
- As we have already seen, creating incentives for early voting in the markets is

key to having economic liquidity and meaningful market outcomes. The function which determines the weighting on bets is a key design aspect. Another exploration path to improve liquidity in the markets would be the inclusion of automated market-makers, such as the prediction markets platform Augur [49].

- In our scheme, we are making the assumption that the Witnesses are a reliable "source of truth" for the markets. The Steem blockchain accepts this for parts of its operation (i.e. price feed of the USD) [6], so it can be seen as a valid assumption. However, details on the minimum quorum for a valid decision and on the minimal participatory Witnesses must be further studied.

6.5.2 Implementation-Level Issues

To develop the smart contract we have followed best practices for developing smart contracts in Solidity[4]. To detect any possible logic error or security vulnerabilities we have taken advantage of the Solidity static analysis tool in Remix[5] and used its online IDE as testing environment. The following issues are specific to Ethereum, for a deeper understanding refer to research from Atzei et al. [10]:

- The time intervals of the markets (e.g. betting time) are defined by the timestamps of the last blocks of the chain. This timestamp is subject to the manipulation by the miners #L103.
- Creating randomness in a deterministic environment like the Ethereum blockchain is an open challenge. We have used the hash of the last block of the chain as source of randomness. This value is also subject to the manipulation of the miners #L353.
- The distribution probability when calculating a random post is affected by the modulo bias #L356.

Moreover, we have included the whole logic of the protocol "on-chain", so the operational gas costs of our smart contract may be expensive in terms of Ether. However, parts of the smart contract's logic could be moved "off-chain" to optimize the costs of execution of the protocol in Ethereum.

[4] https://consensys.github.io/smart-contract-best-practices/.
[5] https://remix.ethereum.org/.

Chapter 7

Conclusions

7.1 Discussion

The crowdsourced curation of content in Steemit enables the aggregation and filtering of information solely relying on the feedback of the users of the platform. In this dissertation, we have analyzed which are the consequences of establishing financial rewards on the curation of content in social media platforms. Steem relies on cryptocurrencies to distribute the value and the rewards among the users of the system.

In Chapter 2 we provided the relevant technical background on social media platforms, blockchain and cryptocurrencies and content curation so as the reader is equipped to follow the rest of our work.

Then, in Chapter 3, we analyzed the Steem blockchain. We described the main components of the ledger such as its consensus protocol and identified Steem as a permissioned blockchain. After that, we developed an in-depth analysis on the economic and incentives model of Steem, providing a mathematical model supported by the relevant references in the actual implementation of the blockchain. This research granted us with valuable insights of the weaknesses and potential attacks of the curation and reward systems of Steem.

In Chapter 4, we identify and evaluate the three weaknesses of the incentives model of Steem: abusive self-voting and voting rings, moderation and censorship abuse issues and the prevalence of voting bots in the platform. To extend our understanding of the self-voting problem in financially incentivized crowdsourced systems, we developed a formal model of Steemit as a game in chapter 5. This model aims to provide a formal framework which may be used to prove (or disprove) the incentive-compatibility of the curation protocol of Steemit. In particular, it provides a suitable infrastructure to determine whether the posts of the highest quality would rise to the top of the list of all posts when players vote strategically in order to maximize their expected revenue.

In Chapter 6 we propose a solution to the moderation and censorship abuse problem in Steemit. We implemented our proposal as a smart contract written in Solidity. We acknowledge our implementation as a Proof of Concept which may be potentially implementable on top of the curation rewards system of Steem.

To summarize, our research work of Steem is divided in four main stages: research and analysis of Steem, evaluation of potential attacks on its incentive model, the construction of a formal model to better understand the role of self-voting in financially incentivized curation, and the development of a solution which enhances the moderation properties of Steemit.

7.2 Future Related Work

We acknowledge that the understanding of financial incentives in content curation is in an early stage, so there are substantial further research paths which can complement and expand our work.

Our analysis of Steem in Chapter 3 has focused on the economic model of Steem. However, an in-depth study of the consensus protocol of Steem (i.e. DPoS) is yet to be made. In our analysis of the financial rewards in Steem, we have neglected the influence of the secondary currency of the ledger, SBD. Although we identify this abstraction to not affect the fundamental concepts of our work, it may change some of the economic properties of the system. Another issue that we have not covered in great detail is the evolution of the voting and curation rewards system of Steem (see Appendix A). The understanding of the effects of the different updates of the protocol could provide valuable insights of the incentives model of the platform.

In Chapter 4, we gave a high-level description of the voting bots of Steemit. To quantitatively measure the impact of voting bots in the platform, a blockchain analysis in form of the data mining of the transactions in the ledger could provide a better understanding of this issue.

We have showed the economic profitability of self-voting. However, if this is the best economic strategy in terms of long-term rewards remains as an interesting open question. Our formal model of Chapter 5 performs the first step in this research direction and may provide an useful framework to prove the incentive compatibility of Steemit. The development of a computer simulation based on our formal model also seems a logical next step to be performed in future work.

In the evaluation of our moderation protocol proposal in Chapter 6, we have included some possible improvements for our solution (see Section 6.5). Apart from that, it would be interesting to perform a migration of our implementation to a version built on top of the Steem blockchain.

7.3 Concluding Remarks

Crowdsourced curation is a powerful approach to the aggregation of content, as it does not depend on a central entity and can establish powerful decentralized architectures for self-regulation of online communities. The financial rewards in the crowdsourced curation of posts in Steem represent a live experiment, which provide novel research opportunities. The convergence of cryptocurrencies as decentralizing agents in the distribution of economic value and the essential role of social media in our online society establish a new paradigm for further study.

Our work here aims to provide a better understanding of the influence of financial rewards in the curation of content. We hope that our findings can be useful for further research and help moving a bit forward the state of the art in this rapidly evolving field. Some of the lessons on how to both detect and avoid potential attacks can be applied both to Steem as well as other emerging social blogging platforms based on blockchains, such as Ono[1] and Mithril[2].

[1] https://ono.chat
[2] https://mith.io

Appendix A

Hard Forks on the Steem blockchain

Since its deployment in March 2016, the Steem blockchain has been subject to many modifications and upgrades. Hard forks in Steem must be understood as updates and notable changes in the protocol, not as split-offs from parts of the network. The Steem blockchain has performed 19 hard forks. We gathered the hard forks of the chain with relevant modifications to our study[1]:

HF	Date	Rewards	Other
19	20/06/17	· Linear Rewards · Square Root Curation · Increase vote influence by 4	
18	30/06/17	· Comment reward pool removed	
17	21/06/17	· Comment reward pool added · Calculate recent claims over last 30 days of payouts	· PoW Witness Removed · 7 days Comment Payout · Removed posting limit rate
16	06/12/16		· Change inflation model · Power Down 13 weeks · SBD conversion 3.5 days
13	15/08/16	·Set Minimum R-shares per vote	
12	26/07/16	· Disable Liquidity Rewards	·Penalize more than 4 post/day
10	16/07/16	· Create Liquidity Rewards	

Table A.1: Relevant Hard Forks of the Steem Blockchain.

[1] https://github.com/steemit/steem/releases

Appendix B

Moderation protocol proposal

This appendix includes the implementation of our proposed moderation protocol as a smart contract written in Solidity. We have removed the comments and the documentation for conciseness. See the smart contract Moderat.sol in the GitHub repository of this thesis for the full version of the program. See Chapter 6 for a description of the main design decisions and the evaluation of the contract.

Code B.1: Implementation of the moderation protocol as a Solidity smart contract.

```
pragma solidity ^0.4.23;

contract Moderat{

    address owner;
    mapping(bytes32 => Market) public markets;
    mapping(address => uint256) public adminsId;
    mapping(address => uint256) public rewards;
    bytes32[] aliveMarkets; //Markets that are either open or to be executed
    bytes32[] adminsMarkets; //Markets to be judged by the administrators/Witnesses
    address[] admins; //Moderators of the platform
    uint numberAdmins; //Number of admins
    uint256 constant votingTime = 120; // (in seconds)
    uint256 constant judgingTime = 120; //(in seconds)
    uint256 constant judgeThreshold = 100 szabo; //Threshold above the admins
    uint256 constant potThreshold = 500 szabo; //Maximum allowed pot on a market
    uint256 constant numberMaxAdmins = 21; //Maximum number of admins/Witnesses
    enum States {open, closed, resolved}

```

```
    struct Market{
        States state;
        uint256 timeOfCreation;
        address[] bettors;
        bool decision;
        uint256 total;
        int256 adminVoteCount;
        mapping(address => mapping(bool => uint256)) betAmounts;
        mapping (bool => uint256) totalOutcome;
        mapping(address => bool) adminVoted;
    }

    modifier onlyAdmin{
        require (adminsId[msg.sender] != 0);
        _;
    }

    modifier onlyOwner{
        require(msg.sender == owner);
        _;
    }

    constructor(uint256 prefundAmount) public payable {

        require(msg.value == prefundAmount);
        require(msg.value >= 1000);
        owner = msg.sender;
        addAdmin(0);
        numberAdmins--;
        addAdmin(owner);
    }

    //++++++++++++++++++++++++MARKETS++++++++++++++++++++++++++++
    function createTrial(bytes32 postId, uint256 amount) payable public{

        require(msg.value == amount);
        require(amount > 0);
        require(msg.value <= potThreshold);
        Market storage trial = markets[postId];
        require(trial.total == 0); //Check that the market has never been created
        trial.timeOfCreation = now;
        trial.state = States.open;
```

```
            trial.decision = false;
            trial.betAmounts[msg.sender][false] = amount;
            trial.bettors.push(msg.sender);
            trial.totalOutcome[false] = amount;
            trial.total = amount;
            aliveMarkets.push(postId);
            rewards[msg.sender] += 250;
        }

        function bet(bytes32 postId, bool valid, uint256 amount) payable public{

            Market storage trial = markets[postId];
            require(now < trial.timeOfCreation + votingTime);
            require(msg.value == amount);
            require(msg.value > 0);
            require(amount <= potThreshold);

            if(trial.betAmounts[msg.sender][false] == 0 && trial.betAmounts[msg.
                sender][true] == 0){
                trial.bettors.push(msg.sender);
            }

            trial.betAmounts[msg.sender][valid] += betWeight(now - trial.
                timeOfCreation,msg.value);
            trial.totalOutcome[valid] += betWeight(now - trial.timeOfCreation,
                msg.value);
            trial.total += msg.value;

            if (trial.decision != valid && trial.totalOutcome[valid] > trial.
                totalOutcome[!valid])
                trial.decision = valid;

            if(judgeThreshold <= trial.total + amount){
                adminsMarkets.push(postId);
                trial.state = States.closed;
            }

            if(potThreshold <= trial.total + amount){
                uint256 refund = trial.total + amount - potThreshold;
                trial.total = potThreshold;
                rewards[msg.sender] += refund;
            }
```

```
    }

    function executeMarkets() onlyOwner public{

        for(uint i = 0; i < aliveMarkets.length; i++){
            bytes32 postId = aliveMarkets[i];
            Market storage post = markets[postId];
            if(now > post.timeOfCreation + votingTime + judgingTime && post.
                state == States.open){
                post.state = States.resolved;
                remove(i,aliveMarkets);
                aliveMarkets.length--;
                for (uint j = 0; j < post.bettors.length; j++){

                    bool winnerDecision = post.decision;
                    address bettor = post.bettors[j];
                    uint betAmount = post.betAmounts[bettor][winnerDecision];
                    uint amountRewarded = calcFractionPot(betAmount,post.total,
                        post.totalOutcome[winnerDecision]);

                    post.betAmounts[bettor][winnerDecision] = 0; //Avoid reentrancy
                    rewards[bettor] += amountRewarded;
                }
            }
        }
    }

    //++++++++++++++++++++ADMINS/WITNESSES++++++++++++++++++++++
    function executeMarketsAdmins() onlyAdmin public {

        for(uint i; i < adminsMarkets.length; i++){
            bytes32 marketId = adminsMarkets[i];
            Market storage post = markets[marketId];
            if(now > post.timeOfCreation + votingTime + judgingTime){

                post.state = States.resolved;

                remove(i,adminsMarkets);
                adminsMarkets.length--;
                for (uint j; j < post.bettors.length; j++){

                    if(post.adminVoteCount > 0){winnerDecision = true;}
```

```
                    else{winnerDecision = false;}
                    bool winnerDecision = post.decision;
                    address bettor = post.bettors[j];
                    uint betAmount = post.betAmounts[bettor][winnerDecision];
                    uint amountRewarded = calcFractionPot(betAmount,post.total,
                        post.totalOutcome[winnerDecision]);

                    post.betAmounts[bettor][winnerDecision] = 0; //Avoid reentrancy
                    rewards[bettor] += amountRewarded;
                }
            }
        }
    }

    function selectRandomPost() onlyOwner public returns(bool){

        require(msg.sender == owner);
        uint256 numberMarkets = aliveMarkets.length;
        require(numberMarkets > 0);
        uint256 targetTrialIndex = calculateRandom(numberMarkets);
        bytes32 targetTrial = aliveMarkets[targetTrialIndex];

        if (markets[targetTrial].timeOfCreation + votingTime >= now){
            adminsMarkets.push(targetTrial);
            remove(targetTrialIndex,aliveMarkets);
            aliveMarkets.length--;
            Market storage post = markets[targetTrial];
            post.state = States.closed;
            return true;
        }
        return false;
    }

    function voteAdmin(bytes32 postId, bool support) onlyAdmin public {

        Market storage trial = markets[postId];
        require(!trial.adminVoted[msg.sender]);
        require(now < trial.timeOfCreation + votingTime + judgingTime);
        require(trial.state == States.closed);

        if (support){trial.adminVoteCount++;}
        else{trial.adminVoteCount--;}
```

```
            trial.adminVoted[msg.sender] = true;
        }

        function addAdmin(address newAdmin) onlyOwner public {
            require(admins.length <= numberMaxAdmins);
            uint id = adminsId[newAdmin];
            if (id == 0) {
                adminsId[newAdmin] = admins.length;
                id = admins.length++;
                numberAdmins++;
            }
        }

        function removeAdmin(address targetAdmin) onlyOwner public {
            require(adminsId[targetAdmin] != 0);

            for (uint i = adminsId[targetAdmin]; i<admins.length−1; i++){
                admins[i] = admins[i+1];
            }
            delete admins[admins.length−1];
            admins.length−−;
            numberAdmins−−;
        }

    //++++++++++++++++++++++++++GETTERS++++++++++++++++++++++++++++
        function getMarket(bytes32 postId) public view returns (
            uint createdAt,
            bool decision,
            States state,
            uint betTrue,
            uint betFalse,
            uint totalTrue,
            uint totalFalse,
            uint total,
            bool voted
        ) {
            Market storage post = markets[postId];
            createdAt = post.timeOfCreation;
            decision = post.decision;
            state = post.state;
            betTrue = post.betAmounts[msg.sender][true];
            betFalse = post.betAmounts[msg.sender][false];
```

```
        totalTrue = post.totalOutcome[true];
        totalFalse = post.totalOutcome[false];
        total = post.total;
        voted = post.adminVoted[msg.sender];
    }

    function isBettable(bytes32 postId) public view returns(
        bool bettable,
        bool executable,
        uint createdAt,
        uint bettingTimeLeft
    ){
        Market storage post = markets[postId];
        createdAt = post.timeOfCreation;
        require(createdAt != 0);
        bettable = now < createdAt + votingTime;
        executable = now > createdAt + votingTime + judgingTime;

        if(now < createdAt + votingTime){bettingTimeLeft = createdAt +
            votingTime - now;}
        else{bettingTimeLeft = 0;}
    }

    function marketInfo() public view returns(
        uint256 numberMarketsAlive,
        uint256 numberMarketsAdmins,
        uint256 numberOfAdmins
    ) {
        numberMarketsAlive = aliveMarkets.length;
        numberMarketsAdmins = adminsMarkets.length;
        numberOfAdmins = numberAdmins;
    }

    function balanceOf() public view returns(uint256 balance){
        return address(this).balance;
    }

//++++++++++++++++++++++++++OTHER++++++++++++++++++++++++++++++++++++
    function untrusted_withdrawRefund() external {
        uint256 refund = rewards[msg.sender];
        rewards[msg.sender] = 0;
        msg.sender.transfer(refund);
```

```
    }

    function calculateRandom(uint256 noTrials) internal view returns(uint) {

        uint256 blockNumber = block.number - 1;
        uint256 blockHash = uint(blockhash(blockNumber));
        uint256 targetTrial = (blockHash % noTrials);
        return targetTrial;
    }

    function calcFractionPot(uint256 betAmount, uint256 pot, uint256 betWinners)
        pure public returns(uint){

        uint fraction = (betAmount*pot)/betWinners;
        return fraction;
    }

    function betWeight(uint256 timeElapsed, uint256 amount) pure public returns(uint256
        weightedAmount){

        require(timeElapsed > 0);
        require(timeElapsed < votingTime);
        weightedAmount = amount - (timeElapsed * amount / (4*votingTime));
        return weightedAmount;
    }

    function remove(uint index,bytes32[] array) pure internal {
        if (index >= array.length) return;
        for (uint i = index; i<array.length-1; i++){
            array[i] = array[i+1];
        }
        delete array[array.length-1];
    }

    function () public payable{
        //do-nothing
    }
}
```

Bibliography

[1] ERC: Token standard #20. https://github.com/ethereum/eips/issues/20, 2015. Accessed: 2018-07-15.

[2] Steem whitepaper, version 1. *Version 1* (2016). https://github.com/aesmonty/MSc-Thesis/blob/master/bib/steemit/steem_whitepaperV1.pdf. Accessed: 2018-08-05.

[3] Steem whitepaper, version 2. https://github.com/aesmonty/MSc-Thesis/blob/master/bib/steemit/SteemWhitePaperV2.pdf. Accessed: 2018-08-05.

[4] Delegated proof of stake consensus. bitshares. https://bitshares.org/technology/delegated-proof-of-stake-consensus/., note = Accessed: 2018-07-22, 2018.

[5] The steem reward system. https://steemit.com/theoretical/@theoretical/the-steem-reward-system-part-1-v-shares. Accessed: 2018-07-01.

[6] Steem whitepaper. https://github.com/aesmonty/MSc-Thesis/blob/master/bib/steemit/SteemWhitePaperV3.pdf. Accessed: 2018-08-05.

[7] ABADI, J., AND BRUNNERMEIER, M. Blockchain economics. Tech. rep., Princeton University, 2018. https://scholar.princeton.edu/sites/default/files/markus/files/blockchain_paper_v3g.pdf. Accessed: 2018-07-28.

[8] ABBASSI, Z., HEGDE, N., AND MASSOULIÉ, L. Distributed content curation on the web. *ACM Transactions on Internet Technology (TOIT) 14*, 2-3 (2014), 9.

[9] ASKALIDIS, G., AND STODDARD, G. A theoretical analysis of crowdsourced content curation. In *The 3rd Workshop on Social Computing and User Generated Content* (2013), vol. 16.

[10] ATZEI, N., BARTOLETTI, M., AND CIMOLI, T. A survey of attacks on ethereum smart contracts. In *Principles of Security and Trust*. Springer, 2017, pp. 164–186.

[11] BAMMAN, D., O'CONNOR, B., AND SMITH, N. Censorship and deletion practices in chinese social media. *First Monday 17*, 3 (2012). `https://journals.uic.edu/ojs/index.php/fm/article/view/3943/3169` Accessed: 2018-08-03.

[12] BERG, J. E., AND RIETZ, T. A. Prediction markets as decision support systems. *Information systems frontiers 5*, 1 (2003), 79–93.

[13] BOSANKIC, L. Blockchain governance: takeaways from nine projects. `https://medium.com/@leo_pold_b/blockchain-governance-takeaways-from-nine-projects-8a80ad214d15` Accessed: 2018-08-04.

[14] BURNISKE, C., AND TATAR, J. *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond*. McGraw Hill Professional, 2017.

[15] BUTERIN, V. Prediction markets for content curation daos. `https://ethresear.ch/t/prediction-markets-for-content-curation-daos/1312`. Accessed: 2018-08-01.

[16] BUTERIN, V., AND GRIFFITH, V. Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437* (2017). `https://arxiv.org/pdf/1710.09437.pdf`. Accessed: 2018-08-01.

[17] CASTRO, M., LISKOV, B., ET AL. Practical byzantine fault tolerance. In *OSDI* (1999), vol. 99, pp. 173–186.

[18] CATALINI, C., AND GANS, J. S. Some simple economics of the blockchain. Tech. rep., National Bureau of Economic Research, 2016. `https://j2-capital.com/wp-content/uploads/2017/11/Some-Simple-Economics-of-the-Blockchain.pdf`. Accessed: 2018-07-28.

[19] CATALINI, C., AND GANS, J. S. Initial coin offerings and the value of crypto tokens. Tech. rep., National Bureau of Economic

Research, 2018. http://ide.mit.edu/sites/default/files/publications/SSRN-id3137213.pdf. Accessed: 2018-08-01.

[20] CHAUM, D., FIAT, A., AND NAOR, M. Untraceable electronic cash. In *Conference on the Theory and Application of Cryptography* (1988), Springer, pp. 319–327.

[21] CHOHAN, U. The concept and criticisms of steemit. https://dx.doi.org/10.2139/ssrn.3129410. Accessed: 2018-08-01.

[22] COHEN, B. Incentives build robustness in bittorrent. In *Workshop on Economics of Peer-to-Peer systems* (2003), vol. 6, pp. 68–72. https://www.cs.swarthmore.edu/~newhall/readings/bittorrentecon.pdf Accessed: 2018-08-01.

[23] CONG, L. W., LI, Y., AND WANG, N. Tokenomics: Dynamic adoption and valuation. http://files.sitebuilder.name.com/3b/6d/3b6d9eaf-35e8-4e34-8ff8-48f4c921328b.pdf. Accessed: 2018-08-02.

[24] DAVENPORT, T. H., AND BECK, J. C. *The attention economy: Understanding the new currency of business*. Harvard Business Press, 2001.

[25] DELMOLINO, K., ARNETT, M., KOSBA, A., MILLER, A., AND SHI, E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In *International Conference on Financial Cryptography and Data Security* (2016), Springer, pp. 79–94.

[26] DWORK, C., AND NAOR, M. Pricing via processing or combatting junk mail. In *Annual International Cryptology Conference* (1992), Springer, pp. 139–147.

[27] EHRSAM, F. Blockchain governance: Programming our future. https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74 Accessed: 2018-08-04.

[28] FORTE, A., AND BRUCKMAN, A. Scaling consensus: Increasing decentralization in wikipedia governance. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (2008), IEEE, pp. 157–157.

[29] FREY, B. S., AND JEGEN, R. Motivation crowding theory. *Journal of economic surveys 15*, 5 (2001), 589–611.

[30] GILAD, Y., HEMO, R., MICALI, S., VLACHOS, G., AND ZELDOVICH, N. Al-

gorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles* (2017), ACM, pp. 51–68.

[31] GLENSKI, M., PENNYCUFF, C., AND WENINGER, T. Consumers and curators: Browsing and voting patterns on reddit. *IEEE Transactions on Computational Social Systems 4*, 4 (2017), 196–206.

[32] GONZÁLEZ, J. Author and curator rewards in hf19. https://steemit.com/steemit/@jga/author-and-curator-rewards-in-hf19. Accessed: 2018-07-01.

[33] GONZÁLEZ, J. Self-voters can achieve an interest of 248% apr!! https://steemit.com/utopian-io/@jga/self-voters-can-achieve-an-interest-of-248-apr. Accessed: 2018-07-05.

[34] GONZÁLEZ, J. Steem proposal to reduce voting rings and self-voting. https://steemit.com/utopian-io/@jga/steem-proposal-to-reduce-voting-rings-and-self-voting. Accessed: 2018-07-05.

[35] GUPTE, M., HAJIAGHAYI, M., HAN, L., IFTODE, L., SHANKAR, P., AND URSU, R. M. News posting by strategic users in a social network. In *International Workshop on Internet and Network Economics* (2009), Springer, pp. 632–639.

[36] KAPLAN, A. M., AND HAENLEIN, M. Users of the world, unite! the challenges and opportunities of social media. *Business horizons 53*, 1 (2010), 59–68.

[37] KAYES, I., AND IAMNITCHI, A. A survey on privacy and security in online social networks. *arXiv preprint arXiv:1504.03342* (2015). https://arxiv.org/pdf/1504.03342.pdf. Accessed: 2018-07-20.

[38] KIAYIAS, A., RUSSELL, A., DAVID, B., AND OLIYNYKOV, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference* (2017), Springer, pp. 357–388.

[39] KLING, C. C., KUNEGIS, J., HARTMANN, H., STROHMAIER, M., AND STAAB, S. Voting behaviour and power in online democracy: A study of liquidfeedback in germany's pirate party. *arXiv preprint arXiv:1503.07723* (2015).

[40] KONFORTY, D., ADAM, Y., ESTRADA, D., AND MEREDITH, L. G.

Synereo: The decentralized and distributed social network. *Self-published* (2015). https://pdfs.semanticscholar.org/253c/c4744e6b2b87f88e46188fe527982b19542e.pdf Accessed: 2018-08-04.

[41] LESKOVEC, J., HUTTENLOCHER, D. P., AND KLEINBERG, J. M. Governance in social media: A case study of the wikipedia promotion process. In *ICWSM* (2010), pp. 98–105.

[42] LIU, C.-C., LIANG, T.-P., RAJAGOPALAN, B., AND SAMBAMURTHY, V. The crowding effect of rewards on knowledge-sharing behavior in virtual communities. In *PACIS* (2011), p. 116.

[43] LUEG, C., AND FISHER, D. *From Usenet to CoWebs: interacting with social information spaces*. Springer Science & Business Media, 2012.

[44] MALKIEL, B. G. The efficient market hypothesis and its critics. *Journal of economic perspectives 17*, 1 (2003), 59–82.

[45] MAY, A., CHAINTREAU, A., KORULA, N., AND LATTANZI, S. Filter & follow: How social media foster content curation. In *ACM SIGMETRICS Performance Evaluation Review* (2014), vol. 42, ACM, pp. 43–55.

[46] MERKLE, R. DAOs, democracy and governance. http://kawin.io/wp-content/uploads/2017/10/Ralph-Merkle-DAOdemocracyDraft.pdf Accessed: 2018-08-04.

[47] MONTEOLIVA, A. Financial incentives on decentralized social media platforms. *Informatics Project Proposal* (2018).

[48] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. https://web.eecs.umich.edu/~manosk/assets/papers/bitcoin.pdf. Accessed: 2018-07-02.

[49] OTHMAN, A., PENNOCK, D. M., REEVES, D. M., AND SANDHOLM, T. A practical liquidity-sensitive automated market maker. *ACM Transactions on Economics and Computation 1*, 3 (2013), 14.

[50] PERCIVAL, C. Stronger key derivation via sequential memory-hard functions. *Self-published* (2009), 1–16. http://www.bsdcan.org/2009/schedule/attachments/87_scrypt.pdf. Accessed: 2018-08-01.

[51] PETTERSSON, J., AND EDSTRÖM, R. *Safer smart contracts through type-driven development*. PhD thesis, Master thesis, Chalmers University of Technology, Department of Computer Science and Engineering, Sweden, 2016.

[52] RAMACHANDRAN, A., AND CHAINTREAU, A. Who contributes to the knowledge sharing economy? In *Proceedings of the 2015 ACM on Conference on Online Social Networks* (2015), ACM, pp. 37–48.

[53] SERVAN-SCHREIBER, E., WOLFERS, J., PENNOCK, D. M., AND GALEBACH, B. Prediction markets: Does money matter? *Electronic markets 14*, 3 (2004), 243–251.

[54] SOCKIN, M., AND XIONG, W. A model of cryptocurrencies. http://wxiong.mycpanel.princeton.edu/papers/Crypto.pdf Accessed: 2018-08-03.

[55] SZABO, N. Smart contracts. *Unpublished manuscript* (1994). http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Accessed: 2018-08-01.

[56] SZABO, N. Bit gold. *Website/Blog* (2008). https://nakamotoinstitute.org/bit-gold/. Accessed: 2018-08-01.

[57] TARABORELLI, D., AND CIAMPAGLIA, G. L. Beyond notability. collective deliberation on content inclusion in wikipedia. In *Self-Adaptive and Self-Organizing Systems Workshop (SASOW), 2010 Fourth IEEE International Conference on* (2010), IEEE, pp. 122–125.

[58] TARAR, I. How does steemit reward system work? https://steemit.com/steemit/@ilyastarar/how-does-steemit-reward-system-work-complete-research-paper-on-steemit-economy-and-reward-system. Accessed: 2018-07-01.

[59] THELWALL, M. Can social news websites pay for content and curation? the steemit cryptocurrency model. *Journal of Information Science* (2017), 0165551517748290. http://journals.sagepub.com/doi/pdf/10.1177/0165551517748290. Accessed: 2017-07-03.

[60] WOLFERS, J., AND ZITZEWITZ, E. Prediction markets. *Journal of economic perspectives 18*, 2 (2004), 107–126.

[61] WOOD, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper 151* (2014), 1–32. http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf. Accessed: 2018-07-16.

[62] XU, X., WEBER, I., STAPLES, M., ZHU, L., BOSCH, J., BASS, L., PAUTASSO, C., AND RIMBA, P. A taxonomy of blockchain-based systems for architecture design. In *Software Architecture (ICSA), 2017 IEEE International Conference on* (2017), IEEE, pp. 243–252.

[63] YASSERI, T., SUMI, R., RUNG, A., KORNAI, A., AND KERTÉSZ, J. Dynamics of conflicts in wikipedia. *PloS one 7*, 6 (2012), e38869.

[64] YEUNG, C.-M. A., LICCARDI, I., LU, K., SENEVIRATNE, O., AND BERNERS-LEE, T. Decentralization: The future of online social networking. In *W3C Workshop on the Future of Social Networking Position Papers* (2009), vol. 2, pp. 2–7.

[65] ZHONG, C., SHAH, S., SUNDARAVADIVELAN, K., AND SASTRY, N. Sharing the loves: Understanding the how and why of online content curation. In *ICWSM* (2013).