

Univerzita Karlova

Filozofická fakulta

Ústav informačních studií a knihovnictví

Utilization of Decentralized Technology in Scholarly Communication

Využití Decentralizovaných Technologí ve Vědecké Komunikaci

Matěj Krejčířík

Diplomová práce

Vedoucí práce: Jan Dvořák

2021

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně, že jsem řádně citoval všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 22.7.2021

Matěj Krejčířik

Poděkování

Z celého srdce bych rád poděkoval nejdůležitějším osobám, které stály při vzniku této práce. Tímto děkuji vedoucímu práce, Janu Dvořákovi, za nesmírně produktivní diskuze a kvalitní vedení. Ambroidovi za obecné diskuze ohledně blockchainu. Nathanovi Heilmannovi, Andymu Stringerovi a Siru Corkymu za poznámky k anglickým formulacím.

Abstract

This thesis presents a detailed explanation and argumentation of why modern decentralized technologies could be utilized in order to improve scholarly communication on many fronts.

The current model of scholarly communication, which is dominated by scientific journals, is analysed together with the current economic models in use. The thesis also briefly investigates peer reviews. It also endeavors to explain how scholarly goods might be perceived from an economic standpoint.

Blockchain technology offers functionalities that could potentially solve many problems associated with scholarly communication through decentralization. Both permissioned and permissionless blockchains, their implementations, interesting technical/economic/governance aspects and why they are such a unique match for scholarly needs are thoroughly analyzed and explained.

Finally minimal viability criteria suitable for assessment of decentralized scholarly projects are proposed. Existing decentralized applications which try to migrate scholarly communication from a current centralized system to a decentralized one are described and examined through the prism of this framework.

Klíčová slova

Decentralizace, Blockchain, Vědecká komunikace, Implementace, Open Access, Club Goods, Správa, Reputace

Keywords

Decentralization, Blockchain, Scholarly communication, Implementation, Open Access, Club goods, Governance, Reputation,

Table of contents

Table of contents	5
1 Introduction	7
2 A Brief History of Scholarly Communication - Faustian Bargain	8
3 Scholarly Communication	11
3.1 Article - Publication Stages	12
3.2 Peer Review	13
3.3 Scholarly Journal	14
3.3.1 Journal as a Club	16
3.3.2 Journal and Its Reputation	17
3.3.3 Alternative Journals	18
3.4 Paywalled Subscription Model	20
3.5 Open Access Movement	24
4 Blockchain	27
4.1 Features	28
4.1.1 Decentralization	28
4.1.1.1 Permissioned Blockchain	29
4.1.2 Authorization	29
4.1.3 Consensus Mechanisms	30
4.1.3.1 Proof of Work	31
4.1.3.2 Proof of Stake	34
4.1.3.2.1 Delegated Proof of Stake	35
4.1.4 Immutability	36
4.1.4.1 Timestamp	36
4.1.5 Turing Completeness	36
4.1.6 Smart Contracts	37
4.1.7 Sharding	40
4.1.8 Tokenomics	40
4.1.8.1 Premine	41
4.1.8.2 Utility	42
4.1.8.3 Problem Solving	42
4.1.8.4 Issuance	42
4.2 Implementations	43
4.2.1 Bitcoin	43
4.2.1.1 Money vs. Currency	43
4.2.1.2 Electricity Consumption	44
4.2.1.3 Relationship to Conventional Banking	47
4.2.1.4 Security	48
4.2.2 Ethereum	50
4.2.3 Polkadot	51

4.2.4 Cardano	51
4.2.5 Hive	52
5 Blockchain for Scholarly Communication	53
5.1 Blockchain Journals	53
5.1.1 Permissioned X Permissionless Blockchain	54
5.1.2 Consensus Mechanism	55
5.2 Viability Criteria for Blockchain Journals	57
5.2.1 Problems Addressed	58
5.2.2 Type of Data Storage and Decentralized Solutions	58
5.2.3 Tokens and Fees	59
5.2.4 Interoperability with Scholarly Tools	60
6 Review and Analysis of Current Blockchain-based Projects	60
6.1 Review of Theoretical Blockchain-based Scientific Solutions	62
6.1.1 Bitviews	62
6.1.2 PEvO	62
6.1.3 Open Science Network	64
6.1.4 Decentralized Research Platform	66
6.1.5 Decentralized Science	68
6.1.6 Frankl	68
6.1.7 Knowbella	69
6.2 Analysis of Launched Blockchain-based Scientific Solutions	70
6.2.1 ScienceRoot	70
6.2.2 Eureka	71
6.2.3 Stemsocial	72
6.2.4 Orvium	72
6.2.5 Scientific Coin	74
6.2.6 Delphus	75
6.2.7 Scholar Chain	75
6.2.8 Moringa Science Publishing	76
6.2.9 Bloxberg	76
6.2.10 The Journal of Raw Data	76
7 Discussion and Conclusion	77
8 References	79

Preface

My long-term goals are to unite the scientific community, to completely reform the journal model, and to customize many areas of several blockchain implementations to meet the specific needs of specific scholarly fields. These blockchain customizations would focus on current issues the scholarly community often faces, including the measurement of reputation, user interfaces, financial models and other commonly problematic areas. Ultimately, it is my goal that the scientific community could once again become a self-sustainable coherent entity via unique, sometimes free/public, and sometimes paywalled club goods. This may be too visionary an undertaking for the mere span of my life but once the seeds are planted, I hope others will follow suit.

My planned PhD research is to work towards utilization of the following Diploma thesis to build or improve upon an existing blockchain scholarly implementation that will offer (hopefully) a variety of improvements over the current status quo. The highest priority would be a) better reputation model, b) creation of an effective decentralized network ameliorating both internal (mutual projects, information dissemination/retrieval etc.) and external scholarly communication (reaching natively non-scholarly entities), d) giving the copyright back to the authors (and institutions providing upfront funding).

The thesis consists of 178962 characters, therefore 99 standard pages.

1 Introduction

Scholarly communication plays an essential role in knowledge creation and its effective dissemination. This said, its role for humanity as a whole is of utmost importance. While it is a hot topic among researchers in all scientific fields and changes have occurred throughout history (such as transition to online publishing) a whole new level of efficiency both for the scholarly community and the general public still remains to be unlocked. Despite crucial contributions to mankind, the nature of this communication itself has changed little in the past few decades. This thesis presents a detailed explanation and argumentation of why that is the case and why it could prove to be useful to make a transition to decentralized systems.

This thesis presents modern decentralized technologies based on blockchains. It thoroughly explains their features and presents some implementations that could prove to be useful for a transition of scholarly communication onto a decentralized sphere. The thesis also shows which of the blockchain features have the potential to improve scholarly communication on many fronts. It also tries to tackle risks associated with individual features, their possible mitigations and it tries to pinpoint which features should be avoided completely.

This thesis will be dedicated to an in-depth explanation of scholarly communication (chapter 3), blockchains (chapter 4), and will demonstrate their possible effective synergies (chapter 5). It will present a description and analysis of currently implemented models (chapter 6). In conclusion a brief summary is presented (chapter 7).

2 A Brief History of Scholarly Communication - Faustian Bargain

The following set of carefully chosen citations is supposed to illustrate the modern history of scholarly communication and its context rather than to provide its in-depth explanation. The set of citations starts with Harnad's old article which was written at the time when public Internet usage was taking off and is supplemented by a group of economists who have built upon the theory of club goods. It is supposed to show how visionary scientists across various fields, from the end of 20th century up until now, perceive the systemic and economic model of scholarly communication as flawed and outdated.

The first version of today's model of scholarly communication was started during the Gutenberg age. Typography was the first technological solution for scientific peers all over the world that enabled them to mass produce scientific articles quickly and accurately. In fact, the main scientist's responsibility and goal is getting the information about their discoveries to scientific peers in a timely and succinct fashion. During the Gutenberg age, there was no other effective way of doing so,

than to have the ideas printed onto paper and disseminated. That is why many scientific communities sacrificed lots of resources in order to more widely spread their knowledge. [1,2]

“It was because of the high cost of this process, the only means of making one's ideas and findings public at all, that scientific authors have stood ready to go even farther than that. They have been willing to make the "Faustian" bargain of trading the copyright for their words in exchange for having them published. From the publishers' standpoint, the bargain was eminently fair: They asked for nothing more than they asked from trade authors, which was the right to protect the product from theft, so costs could be recovered and both author and publisher could make a fair profit. For the trade author, this bargain was not Faustian, because both he and his publisher stood to gain from it - and to lose from theft. But the need to pay a ticket at the door was the last thing a scientific author would have wanted to impose by way of a deterrent for his already minuscule potential readership.”[2]

“From the perspective of economic analysis, this (journal) model is predicated on the efficient organisation of the specialised capital and skills required to produce and distribute scholarly journals, and recognition that these capabilities were not efficiently possessed by scholars as the producers and consumers of scholarly output. The economic logic of this situation resulted in the papyrocentric business model of a closed-access journal in which a private publishing company holds the intellectual property rights and is supplied with free content and free labour.”[3]

“The small society presses, struggling to cope with growing scale, were supported and then largely supplanted by the ‘Big 5’ commercial presses: Elsevier (which acquired Pergamon in 1991), Wiley, Springer, Taylor & Francis and Sage. These newly-empowered players brought an industrial approach to the publication and dissemination process, for the first time realising the benefits that these specialised capital and skills could provide by operating at a scale that was unprecedented to that date. The successful publishers grew (and consolidated to grow further) alongside a pre-Cambrian explosion and specialisation of journals to create the modern landscape in which the majority of journals is owned, controlled or at least produced by a handful of globalised companies.” [3]

"In the past, this model was working reasonably well, or, rather, there was not much of an alternative. Early dissemination as well as social or collaborative creation and evaluation of knowledge is impractical without the Web. Papers, just like software, were produced using the waterfall model¹. Furthermore, until recently, scale was not a big problem. The number of articles submitted to conferences (and journals) was under control." [8]

"But with the arrival of the computer, the internet and soon the blockchain, the economics of this model shifted. The wide availability of desktop hardware and software enabled new capabilities among authors, and an expectation from publishers that authors would self-manage much of the layout and editing of articles. Meanwhile, technologies for storing articles (databases), discovering articles (digital object identifiers and advanced search technologies), citing and reviewing, made it easier for academics to engage with each other's work." [3]

There has been a continuous migration from papyrocentric journals to digital publishing ever since the invention of computers. Publishing companies were experimenting with a hybrid subscription model² that was hoped to provide a gradual transition to electronic-only publishing. But the expensive subscription remained and so did the apparently obsolete Faustian bargain, which was envisioned by Harnad 26 years ago [2] and is still true today.

"Most categories of expenses (e.g., not just paper, printing and distribution, but marketing, advertising and fulfilment) vanish with purely electronic publication (and of course overhead from lingering paper operations should not be reckoned in either). The only inherent expenses of purely electronic publication are those of (1) peer review (which requires only editorial administration, because the peers [i.e., us] have always reviewed for free) and (2) editing (including formatting, mark-up and archiving). My own (*Harnad's*) estimate (based on experience from editing both a paper journal, Behavioral & Brain Sciences (BBS), published by Cambridge University Press, and a purely electronic one, PSYCOLOQUY, sponsored by the

¹ A classical model used in project management where each project phase is tackled chronologically.

² Hybrid meaning printed and digital form, not hybrid OA model.

American Psychological Association, a large learned society) is that the savings would be more like 70-90%.”[2]

“The twentieth-century publishing model made economic sense as outsourced specialisation, but technological change has upended that logic by dramatically lowering the cost of in-house production. The old model holds on through legacy effects and competitive ‘costly signalling’ of perceived prestige through selected mastheads, and has transformed into a model of monopoly exploitation. This is costly in pecuniary terms, but also in the ability of scholarly communities to develop and change publishing institutions to suit their own needs. There is now a broad consensus that the economics of scholarly publishing is broken and that a new way forward turns on exploitation of new, open access, business models. But open access models, including hybrid models, are also proving difficult to implement, running into problems of cost, free-riding and incompatibility with extant scholarly research institutions.” [3]

It is a responsibility of information scientists (information science in general) to come up with a more effective (in terms of attaining its goals while being more cost-efficient) and up to date (utilizing modern technologies in order to deal with current problems) systemic model that will ensure the healthy growth and measurement of scholarly output. The scientific community should be concerned that it is them who rapidly come up with innovative technologies, yet they often fail to implement these ideas themselves in order to fulfil their own needs. The scientific community should be concerned that fruits of their research remain underutilized for their own purposes.

Thus said, the scholarly community finds itself in a spot, where it uses an obsolete and expensive legacy system that has only undergone minimal changes since its strictly papyrocentric days. The next section will be dedicated to an in-depth analysis of this legacy scholarly communication system.

3 Scholarly Communication

Today's system of scholarly communication will be analysed in this section. Reputable channels used for scholarly information dissemination will be introduced, scholarly articles will be investigated and finally, economic models will be explained.

To simplify, three main channels through which scientists disseminate information are in existence. These are: conferences, books and scholarly articles - published mainly through scholarly journals.[8,4] Channels such as research and project reports - which are presented to funding agencies and other stakeholders - are perceived as secondary scholarly channels. Fortunately, in response to today's digital environment and regional funding policies these are open access in some countries. [4]

Conferences are *offline*³ symposium-like events where scholars share information and receive feedback in real-time. Usually conference organisers review submitted articles and decide which ones are worth being presented to the audience. [4] During the preliminary investigation of scholarly decentralized solutions it was uncovered that the vast majority of those projects concentrate solely on scholarly articles and research data, therefore scholarly journals will be the main focus of this thesis, while conferences and books won't be further addressed.

"Today, there exist three high-level models of academic publishing: paywalled (peer reviewed, free or fee for authors, readers pay to access the articles), open access (peer reviewed, fee for authors to publish, free access to published articles), and preprint repository (self-archiving or centralized archives of preprints, no fees, but no peer-review either)." [5]

In the following subsection the important aspects of scholarly communication will be explained.

3.1 Article - Publication Stages

³ In fact, due to the COVID-19 pandemic most scientific conferences have moved online.

Scholarly articles progress through several stages before they are finally published in a journal. Before an article is submitted for publication, it is called a manuscript.

The first public version of an article is called a manuscript. A manuscript becomes a preprint upon the author's decision to share the article on any preprint server (such as the first ever preprint server - Arxiv, other discipline-specific repositories, or institutional open access repositories, etc.). Preprints haven't yet undergone the peer review process.

Since 2012, scholarly communication has seen a considerable expansion of preprint usage. Some open access journal platforms are even incorporating such dissemination, prior to peer review, into their workflow. [7] They are thus extending the original preprint intent, which was to increase the speed of dissemination, increase the amount of received feedback and making the article publicly available on the internet.

Upon publication of a manuscript, provided that it successfully passed the peer review process, the text is called paper/article and is assigned its DOI. It is then ready to be shared and cited upon with greater validity.

3.2 Peer Review

Peer review is an evaluation process done by scientific experts with long publishing histories, academic experience and scholarly reputation [8,4]. Its purpose is to ensure conformity to prevailing norms and select scholarly content. It's an effective self-regulating tool used by the scholarly community. It also is an effective source of feedback for scientists and their articles [4]. Usually 3-4 peers review any given submission. The best articles among those submitted are accepted for publication in a journal [8]. 2 peers usually review conference submissions.

„There are two broad methods, namely, Blind Review and Open Review. Blind Review methods usually follow pre-publication peer reviewing, i.e., peer reviewing before acceptance of a paper in a journal. On the other hand, Open Review methods follow both pre-publication and post-publication peer reviewing. Pre-publication peer review follows two broad methods, namely: (i) Single-Blind Review where reviewers

know the authors but the reviewer's name is not disclosed to the author; (ii) Double-Blind Review where the identity of the reviewers and the authors are not disclosed to either party. In Open Review methods, no identities are concealed; both author and reviewer names are disclosed. In Pre-Publication Open Review, any comment related to a submitted manuscript of a paper, which is normally mediated by the editor, can be posted by reviewers before the journal publishing an article. It only can be posted by the reviewers pre-assigned by the editors. In Post-Publication Open Review, any reviewer comments related to a submitted manuscript of a paper, which is normally mediated by the editor, can be posted by readers and reviewers after the article has been published.“ [4]

Typically there are four possible outcomes of a peer review. It is either accepted with or without editorial revision, requiring an author to make changes before a decision is reached, rejected with an indication that further work may justify resubmission or it is outright rejected. [4]

Currently, no or minimal monetary compensation for the vast majority of peer revision is in place. [3][5]

3.3 Scholarly Journal

“Traditionally we would consider a journal as a node that organises market relations between authors, readers and specialist publishing capabilities.“ [3]

Scholarly journals are either for-profit (maximizing profit) or non-profit (trying to break even) [4,6]. Journals were initially started by scientific societies, national science academies and other learned communities. They were (and are) meant to aggregate unique scientific articles by thematic areas, geographical focus, etc. They have a predetermined scope and target audience. [4] “Scholarly publishers provide, from an economic point of view, rivalrous or non-rivalrous goods (research articles in the form of physical or digital texts) that can be excludable or non-excludable (behind paywall or free to access).“ [5]

“Most academic journals are published by non-profit publishers such as learned societies, research councils, research institutions, university presses, research and literary academies. On the other hand, in the twentieth century we see that for-profit

publishers such as publishing companies and multinational enterprises are taking great interest in publishing academic journals, usually in collaboration with learned societies. In a recent study, it has been revealed that for-profit publishers Elsevier, Springer and Wiley now have a large market share – about 42% of journal articles in STM (Science, Technology and Medicine) disciplines. They also have made high profit margins in recent years – between 30% to 40% – by charging high subscription fees as well as open access publishing fees. Thus, STM journal publishing has gone into the hands of monopolistic corporations. However, non-profit academic publishing ventures are also flourishing due to easy availability of electronic publishing (or e-publishing) avenues and more particularly open access channels for achieving universal and free dissemination of scholarly literature, global authorship and global readership of journal contents.“ [4]

Scholarly journals can now be understood as competing information systems trying to uncover unique high quality articles and aggregate them by niche science domains.

At the time of writing (2021), tens of thousands of scholarly journals are in existence. Depending on which economic school colors one’s perspective, the top players would either be called “dominant” or “monopolistic”. Even though I cited several authors that chose to call those players monopolistic, I strongly disagree with such a term.

Granted there's no perfect competition (as perfect competition does not exist in the real world) between scholarly journals, there is no power (from the point of view of the Austrian economic school only the state government has that power - which is granting exclusive privileges) that would restrict other players from participation in the competitive market with the rest of the providers. [12] That is proved by the existence of over 30k scholarly journals, many of them flourishing. The low barrier to entry to the market is also evidenced by the recent emergence of predatory publishers. If there truly was a monopoly, the cause of once again decentralizing science and bypassing redundant third parties would be legally bound to fail from the start. The “monopoly” definition provided by Austrian economics may be too anarchistic for the readers' liking. Regardless of whether the reader chooses to label the top journals “dominant” or “monopolistic” an important premise for the present

argument and throughout this research is that competition under market conditions is allowed and happening.

3.3.1 Journal as a Club

In section “Scholarly Journal” we defined a journal as a node that organises market relations between authors, readers and specialist publishing capabilities.

In addition to that, “to reform scholarly publishing, we need to start by recognizing that a journal is a club. A scholarly journal is neither a private good nor a public good—it is a club good.” [3]

„If a journal is a club, what then is a club? Economic theory has a very specific answer to this question. Club goods are distinguished from private goods (where consumption is both rivalrous and excludable) and public goods (where consumption is nonrivalrous and exclusion is not possible) by being non-rivalrous (up to a congestion point) and excludable. Completing the standard four-term matrix are common pool resources, which are rivalrous but non-excludable. Club goods are also known as ‘toll goods’, because the congestion point requires a toll for efficiency; and also as ‘local public goods’ because groups are often spatially organized.“ [3]

But ever since humanity entered the Information age “the internet and its digital affordances makes that group formation less a spatial phenomenon and more a cultural phenomenon.“ [3]

„Clubs, then, refer to the formation of groups of people who share a common concern, who are willing to pool their common resources and specialization-skills, and act in concert in pursuit of ‘shared externalities’.“ [3]

„The externalities here are those of reading, understanding, citing, and refereeing the papers that each scholar writes. Scholarly papers are written to be read and then to be acted upon by other scholars.“ [3]

„A club, therefore, is a self-organising group that, in the language of microeconomics, expects to benefit from the net externalities they impose on each other, minus the costs of doing so, and organized such that an optimal club size exists (because of crowding). Clubs are ‘voluntary’ (in the microeconomic rather than

cultural sense), and clubs involve pooling resources, and clubs involve exclusion mechanisms, which are endogenous aspects of the voluntary pooling mechanisms that define the economics of a club. The implication is that clubs have optimal sizes that are determined by technological and institutional factors.“ [3]

Clubs can be a centralized, but also decentralized (in our case scholarly) community. Club goods are the net positive products of those communities (knowledge created). Clubs of certain sorts (in our case scholarly clubs) are in need of information systems through which the products can be internally utilized and externalized.

As will be shown in section “Paywalled Subscription Model” and “Open Access Movement”, most of the “specialist publishing capabilities” is actually voluntarily outsourced and behind a “toll” (subscription/APC). Few big companies managed to gather a significant percentage of the scholarly market. Up-to-date data shows, for instance, South Korea spends 71% of their budget on top 3 publishers annually. The USA and the EU spend around 4 billions USD annually on subscription and OA publishing (see section “Open Access Movement”).

Rational questions the scholarly community should be concerned about are: Is it worth it? Can we quantify the added value the scholarly club receives for their money? How hard would it be to set up equivalent and cheaper alternatives? How big would the new associated costs be?

If scholarly communities are indeed clubs and answers to the above mentioned question isn't in definitive favour of the current publishing giants, then scholarly communities should be trying to create new types of journals. In fact this trend has already started.

3.3.2 Journal and Its Reputation

In 2008, an article was published that initiated a discussion about the competencies of peer-reviewers in various journals among various scientific fields. The authors found out sometimes peer-reviewers have published minimal amounts of articles and attracted minimal amounts of citations. The article claimed this was rather an exception but should not be ignored. [85]

Numerous articles have been written in direct or indirect reaction to this initiation of discussion. Those articles chose to compare the h-index of the editorial board to the impact factor of their journals. Correlation has been proven among various scientific fields such as Sports Medicine [86], Anaesthesia [87], and Radiology [88].

Although other articles point out there are potential malicious behaviours regarding selection of editorial members [89].

At the end of the day, the metrics the individual authors choose to compare ultimately decide whether the results are positive or negative. It isn't in the scope of this article to prove which metrics are optimal to use when the legitimacy of editorial members is to be investigated. An important premise for this thesis is the editorial members are at least partly responsible for the reputation of their journal since they select which articles are going to be published and which are going to be denied. I believe this premise can be held due to the proven correlation between h-index of the individual editors and impact factor of their journals. On top of that editorial boards can, and have in the past, completely migrate from one journal to another [148], thus greatly influencing equilibrium in between for-profit, not-for-profit, or possibly even decentralized journals.

3.3.3 Alternative Journals

Before the brainstorm about theoretical decentralized journals will be provided (in chapter 5), the current alternative journal models will be briefly investigated in order to demonstrate the possibilities (rather than to prove or claim anything).

For starters eLife journal will be briefly investigated. eLife is not an average journal. According to JCR it is ranked among the top 5% journals in Biology [67]. eLife realized that over 70% of articles under review in the journal were already published on preprint Arxiv-like repositories. This means in practice, eLife is no longer a journal but rather an organization that reviews already “published” articles. It decided to further move in this trend. By July 2021 it shall abandon the prevalent scientific method of “review, then publish” and adopt the opposite “publish, then review”

approach. By that time, all the published articles in eLife have to be published in a preprint Arxiv-like repository. [68]

eLife doesn't stop there. It decided to not only review already published articles, but also to make the reviews public. Their long-term goal is to move away from the concept of journal titles as the primary measurements of the quality and move towards the “richer evaluation metrics” as the primary measurement of the quality. But until the method of how scientists are evaluated for promotion to higher status is changed, eLife will still “publish” some articles of the highest quality. [68]

At the same time eLife decided to increase its APC from 2500 USD to 3000 USD [69]. While this price is still in the range of the majority of the journals (as explained in section “Open Access Movement”) the reasoning behind the decision remains unclear and further investigation is not in the scope of this text.

Another example of alternative journal creation is the Open Journal System (OJS). OJS is an open source software tool managing the creation of Open Access journals. [70] Since its release in 2001 more than 2 million records have been submitted in more than 10,000 journals alongside 6000+ publications using the tool (and similar tools such as Open Monograph Press and Open Conference System) [70,71]. The funds for development and hosting of OJS are gathered directly by PKP through voluntary contributions. It is unclear how frequent the contributions are or how many contributions below the 500 USD mark have actually been provided. Counting only the lowest limit of contribution ranks, assuming the contribution has happened only once, PKP has gathered at least 235,000+ USD for their work so far [74].

Two random journals utilizing the tool were chosen to provide an example - Brazilian Sociobiology and Czech Acta Polytechnica. According to JCR, Sociobiology is oscillating in-between upper 4th quartile and lower 3rd quartile in Entomology [72]. Acta Polytechnica is, according to SJR, in an uptrend and has managed to stay in 2nd quartile in Engineering since 2018 (2020 data is not yet provided) [73]. Both

journals are completely APC free. There may or may not be even better ranking journals utilizing OJS. Those two examples are only supposed to demonstrate there is an open source software that gathered enough funds and managed to operate for two decades. This software enables thousands of journals. Among those is even Czech Acta Polytechnica which is completely free of charge and still managed to climb to the top 50% of all the scientific journals in Engineering.

3.4 Paywalled Subscription Model

„This modern economic model, with its attendant commercial players and profits, is a departure from the original model of journals. While part of the original motivation of the first research publication in serial form – the Philosophical Transactions of the Royal Society in 1665 – was to make money, the early history of scholarly publishing is largely one of community subsidy to cover losses or breaking even. The first serials to which the name ‘journal’ was applied in the nineteenth century often struggled to find audiences sufficiently large to justify the printing of content of interest to professional researchers.“ [3]

Nowadays, a substantial amount of scholarly articles are behind paywalls. [9] Journals are either being sold as standalones, or they are being sold in personalized bundles to individual libraries and scientific organizations. [10,11]

Obtaining up to date data of journal prices or journal bundle prices is close to impossible due to the fact that almost none of this data is publicly available. The big players keep their pricing confidential as a trade secret. Individuals and groups who try to somehow bypass these trade secrets are treated as hostile actors. Heavy lawsuits are brought against those challenging the established power structures. In order to further help with shaming the dominant players practicing these shady trade practices, they shall be named - Elsevier and Springer. [10] [11]

Luckily for our cause, most of the state-funded universities in the USA are required to reveal information about their contracts, regardless of confidentiality agreements, due to the Freedom of Information Act. This legislation has been called upon in the cited paper and some data has been acquired due to that move. [10] This said, there

isn't enough open access data to chronologically illustrate the situation, rather there is just enough data to roughly estimate/visualize the situation.

Before embarking on price analysis, we have to address claims that dominant journals conduct monopolistic actions, since the internet allowed them to exercise more supposedly shady barter techniques. [10] As previously stated, there is no economic consensus about the term “monopoly” as different economic schools perceive it fundamentally differently. It is not important to settle on one definition of the word, rather it is important to acknowledge that despite the word used, big journal players don't have their position secured by state law and effective competition can greatly diminish their market share.

Bergstrom et al. claim that a monopolist's ability to price is limited by two factors - arbitrage (deals with the monopolist intention of charging different prices to different entities) and hard-to-determine willingness to pay. They also claim that journals bypassed the arbitrage limitation by “noninterchangeable electronic site licences” and the “willingness to pay” by offering “journal bundles” for lump-sum fees. [10]

Both statements are debatable. Firstly, as the following presentation of data will show, it is not monopolistic by default to charge different prices to different entities. The fact that wealthy scientific institutions are charged more than small scientific institutions is a valid market strategy (It could be defended on ethical grounds. At least the lesser scientific institutions can get their hands on the scientific material in this broken system. Such a phenomenon would probably occur even if the scientific community did not outsource publishing itself). The problem is rooted in how high prices are achieved, maintained and bargained, not that small institutions are allowed to pay less for the same content. Upon an identification of a behaviour where smaller scientific institutions (thus less wealthy) are charged more than bigger institutions, swift measures should be taken. The information should be brought to light and mutual trades (subscriptions, reviews, publishing...) should be abolished as soon as possible. While the actions of the publishers are not monopolistic, they are evidence of an immoral effort to earn as much money as possible at the expense of the trade partner (scholarly community). Bergstrom et al. also acknowledge that interlibrary loans (or often time free internet copies) and scientific entities without

subscription allow readers to get their hands on paywalled material, albeit with a time delay, as a result of cooperation [10].

Secondly, lump-sum fees cannot in any way be perceived as a monopolistic strategy. Lump-sum fees are a part of so many services that using the word “monopoly” wouldn't make any sense anymore if it was supposed to be used for any service offering lump-sum fees. [10]

It cannot be stressed enough that the problem is the high initial price tag, not prices that cannot be customized, nor lump-sum fees. The constantly increasing initial price tag for scholarly journals in comparison with scholarly budgets is also referred to as the “Serial crisis”. This term refers to the fact that journal prices are annually rising more than the libraries' and scientific institution's budgets. [4,11]

The journals are being sold as predefined bundles most of the time. Average cost of those bundles increases annually by 5-7%. The initial estimation for the price is derived from original historical print subscriptions. This said, bundles with an annual growth of 5.5% would double their price between 1999-2012. During that period of time the US consumer price index (in other words “how much is an average american willing to pay for services and goods”) grew “only” by 38%. [10] Consumer prices have continued to grow at a roughly same rate ever since then. [13]

A significant disturbance to this trend has come from libraries and scientific institutions bargaining with the journal providers in order to get better deals. For example, in 2003, California Digital Library took a hard bargaining stance and as a result managed to lower the immediate payment by 9% in 2004, plus the future annual growth was guaranteed to be only 1.5%. Thus, by 2013 their annual cost was “only” \$9.3 million instead of \$13 million. [10]

The acquired data implies that multiple entities independently bargain with scholarly publishers. For example Elseviers Freedom package was sold to University of Georgia (\$1.9 million), University of Colorado (\$1.7 million), University of Texas (\$1.5 million) and University of Wisconsin (\$1.2 million). Just for the record, Wisconsin and Texas produce about twice as many PhDs and managed to get a lower price at the same time. [10]

It has also been found that the University of Virginia paid a bit less (\$450k) than the University of Dartmouth (\$480k) for the Springer package while being a much larger scientific entity. The University of Arizona paid \$108k for the Sage package whereas the Brigham Young University \$185k. The University of Kentucky paid \$490k for the Wiley bundle, whereas the University of Oklahoma paid \$500k. [10]

Despite clear evidence that hard bargaining can influence the price, the average pattern of the data is as follows. On average, both for-profit and not-for-profit journals charge big scientific entities more than the smaller ones. Elsevier's full price for all their journals (year 2009) was \$3.132.000. The discount for large scientific entities (the bundle discount) was 21%, for medium scientific entities 60% and for the small ones 84%. Springer's price prior to negotiations was \$2.218.000, the discount for large scientific entities was 50%, for medium scientific entities 72% and for the small ones 85%, etc. The average price of a subscription journal is \$2k for the top 10 publishers per year [11]. In general, for-profit providers reduce prices more sharply than for not-for-profit ones when it comes to discounts. Clearly, not-for-profit providers are cheaper, but at the same time have fewer scientific journals at their disposal. [10] According to JCR The average price⁴ the subscription of the top 10 journals according to JCR (before any discount) is estimated to be \$2.3k. Summing the prices of all subscription based journals listed in JCR (10.535 journals), results in roughly \$24 million. [11]

In 2020 “according to the publishers’ annual reports, Elsevier’s subscription sales are about 2.5 billion USD, Springer’s are 1.4 billion USD, and Wiley’s are 1.3 billion USD”. [11] In 2011 Elsevier reported profits equal to 36%, Springer equal to 33.9% and Wiley equal to 42%. [10]

Meanwhile, in the years 2006 to 2012 (as I wasn't able to acquire more up-to-date data - but I was not alone, see [147]) a declining minority of scholarly institutions in the USA have or continue to sign big deal bundle contracts from for-profit providers. On the other hand, not-for-profit providers signing bundle contracts are on a steady rise and have already signed a slight majority of scholarly institutions during the same years. [10]

⁴ The prices were handpicked.

3.5 Open Access Movement

The second publishing option, a semi-paywalled one, although with a name that does not directly imply any paywall at a first glance, is the Open Access method. There are several main sub-methods. The most notable ones, namely Green, Gold, Hybrid (combination of Green and Gold) Bronze, Diamond and Black (this list is most probably not comprehensive), will be introduced.

The Green Open Access method was invented first. It represents an act of publishing in a paywalled journal that allows retainment of copyright for the authors to some extent. This said, the author can self-archive his article before, or after the publishing act. [14,15]

The copyright isn't preserved fully. The publishers put an embargo on "where, how and when" the copyright is applied. For example, the author is restricted from self-archiving the article for a certain period of time, or he has to do it on a specific platform, or he cannot monetize the article in any way and so on. The current "more restrictive" trend has been tracked to be closely connected to the invention of the Gold Open Access method. There is also an ongoing competition between publishers in terms of "looking as green as possible" to the authors/institutions. According to Gadd and Covey the data indicates that it is more a war for customers rather than a genuine effort to get as close to full Open Access as possible. [14]

It can be said that, regarding Green Open Access, the payment to the publisher is done via partial abnegation of one's copyright without a standardized framework - every journal makes their own rules as to what is restricted and what is allowed with the pre/postprints.

The Gold OA method requires direct financial payment. Publishers provide immediate free access to published articles in exchange for a so-called article processing charge (APC). Thus said, not only do authors yield their copyright to the publisher for the fruits of their work - they also have to somehow gather a significant amount of finances in order to pay for APC from their institutions, grants, or in rare cases from their own pockets.

As the data at my disposal about APCs contains both prices of Gold and Hybrid OA journals combined, Hybrid OA will be explained prior to presentation of the data.

Hybrid OA method is a combination of Green and Gold. That means that publishers offer a journal that has both paywalled and APC paid OA documents. Institutions can therefore access the OA documents, or access the whole portfolio of documents after paying the toll. Hybrid journals are closely connected to a “double dipping” problem. [16]

Double dipping is a phenomenon where publishers get paid twice for the same content from the same institution (via APC and general toll). Even though most publishers make a promise to follow a “no double dipping policy” it is entirely impossible to validate those statements. As all the accounting details are held secret the entire scholarly community finds itself in a position where it needs to completely trust an arguably untrustworthy third party. The publishers were confronted with direct questions regarding their “double dipping strategy”. In return they provided sometimes vague, sometimes less vague answers, but never direct accounting proof. [16] Third parties that refuse to provide complete accounting proof should not be trusted as long as there are trustless systems at our disposal. Trustless systems will be discussed in chapter 4 - Blockchain.

The Bronze category has only recently been named and defined. It refers to a dissemination method where publishers provide a free-to-read article on their site, but do not provide any specific Open Access (OA) licence. Any re-use of such articles is therefore problematic. According to the creator of the name - Piwowar - the Bronze method resembles Gold and Hybrid methods through its publisher-hosted nature. [15] However, the no-monetary-fee-for-publishing resembles the Green method, but is less user friendly due to missing licences.

Collecting data on APCs was as hard as collecting subscription costs, therefore data at our disposal is yet again limited, and thus only illustrative of the current situation. The data acquired represents only the top 10 publishers so the prices are comparable to those listed in the previous chapter. While investigating the top 10 publishers, the highest APC was found to be \$3.871, the lowest was \$2.017. In

general the APC prices range from \$500 to \$5k+. More than 50% of the journals have APC of \$2.5k-\$3k. The average estimated APC is \$2.652. [11]

An average APC is more expensive than an average annual subscription for a journal. [10,11]

„The average expenditures of institutions are 87.5% for subscriptions, 11.8% for APCs, and 0.6% for administrative costs. The OA publishing market was estimated to be around 758 million USD in 2019, and therefore, the APC market share was estimated to account for 7.7% of the world journal market.”[11]

„According to prior studies, in 2016, academic libraries in the USA paid 2.3 billion USD for journal subscriptions, and the 31 consortia in European countries spent 726 million EUR.“ [11]

„According to the National Research Council of Science and Technology, the total journal budget of 25 government-funded research institutes in South Korea (focused on the science and technology fields - excluding medicine - and not including university libraries) was about 12 million USD in 2020. In the materials budgets of 25 research libraries in 2018 to 2020, the share of journal subscriptions was 71%. The top three publishers accounted for 67.1% of those expenditures, and the top 10 for 78.8%.” [11]

„According to journal prices and APCs the market influence of the top three publishers was 48.0%. However, in combination with information on actual subscriptions obtained from the annual reports and other studies, their market share was finally estimated to be 55.2%. The difference was caused by Elsevier’s real market share, which was higher than its market influence.“ [11]

„In this situation, Outsell estimated that English-language science, technology, and medicine journal publishing had global revenues of 9.9 billion US dollars (USD) in 2017.“ [11]

The last actual OA method is Diamond. Diamond OA is what seems to be the theoretical pinnacle of OA methods. It represents a state where there are no monetary fees for anyone. The articles are free-to-access and even reuse, there are

no APC. As there are no financial gains, there can be no financial rewards for peer-reviewing and other scientific jobs. The cost to sustain such a journal is covered through grants. [17]

There is also something called Black OA which basically stands for illegally uploaded articles. [15] From a very twisted standpoint, those documents can also be perceived as OA, but they should rather be perceived as what they are - illegal activity and partial proof that the prices are set too high, therefore an economic incentive to steal these documents grows larger.

According to a dataset of randomly selected 100.000 articles in 2015 around 55% is behind a paywall, 17% is Bronze, 10% is Hybrid, 11% is Gold, 6% is Green. It is important to note that newly published articles are much more likely to be OA. [15]

4 Blockchain

In this chapter blockchain technology will be presented and explained. There are severe shortcomings (disregarding the complexity of the topic) in basically all of the scientific articles about blockchain technology that I have read so far (apart from IEEE Transactions on Cybernetics articles). For the purpose of presenting complete information, not only scientific articles and whitepapers of several projects are going to be used, but also blogs from the most prominent blockchain pioneers.

Blockchain is a distributed ledger technology that supports append only function. It organizes data which are ordered chronologically into so-called “blocks” while being cryptographically secured. [131] Once validated blocks cannot be reworked as long as the implemented consensus mechanism is not bypassed by a so-called 51% attack. Thus a database is created.

This distributed database is maintained by individual hardware systems (nodes) that interact in peer-to-peer (P2P) manner [47] to record, synchronize, store and share the appended data [19].

4.1 Features

The term blockchain connotes the several technologies (already in existence prior to the invention of blockchain) that were brought and used together in order to achieve unique properties, previously unheard of.

The elements are decentralization, consensus mechanism, immutability, time stamping, asymmetric cryptography, Turing completeness and smart contracts. Those elements were combined to create a “trustless” system. [18,19] We shall break down all those terms.

Note that there are thousands of blockchain implementations in existence and they vary in the degree of successfulness of achieving these features. Sometimes systems that are based on blockchain technology don't necessarily have to be decentralized, nor immutable. Blockchain is an information system, rather than just a technology. Governance aspect and the people themselves cannot be separated when defining blockchain.

4.1.1 Decentralization

Decentralization is an implementation of a P2P network. P2P networks are characterised by the absence of a single point of failure (centralized server). All the information in its entirety is distributed into several (in some cases even all) voluntarily cooperating nodes. [18,19] As long as there is one surviving node the whole network can be recreated no matter the problem (collapse of internet network, electricity breakdown, etc.). Non-blockchain based representatives of P2P networks are for example InterPlanetary File System (IPFS - see [129]) or the Bittorrent protocol.

Absolutely crucial aspect of a decentralized system is its openness. A “single point of failure” problem is not only associated with technical aspects (centralized server), but also with an “oracle problem” (further explained in subsection “Smart Contracts”). As long as there is any authority that can restrict potential users from participation in the system, the system is not decentralized and trustless. The authorizing oracles are entrusted with complete control over who will be granted a permission to use the

system - and who will not. This argument is further supported by the fact that only users of the system (those that have been granted the permission) can participate in consensus mechanism voting (see subsection “Consensus Mechanism”). Only the previously entrusted entities can therefore try to change the rules and possibly strip the oracle(s) of their right. The permission to use the system could also be withdrawn by the oracle(s) prior to that.

4.1.1.1 Permissioned Blockchain

A vast majority of blockchain projects are so-called “permissionless blockchains”. Permissionless blockchain stands for a network that can be joined and subsequently run by any entity. Each and every user/node can unconditionally participate. [18]

On the other hand, permissioned blockchains follow an inverse approach. Participation in the network is conditioned by authorization. [19, 26]

At the start of the chapter it was stated that several elements (previously in existence), when combined, provide a decentralized and secure P2P network - thus effectively creating a trustless system. Unification of those elements - with a trustless outcome - was called blockchain. Just the fact that data is chronologically hashed doesn't make the information system blockchain [46].

If blockchain is defined by decentralization and trustlessness and “permissioned” by definition means authorized by a trusted party, thus centralized, it doesn't make any technological sense to call “permissioned blockchains” blockchains. [46]

4.1.2 Authorization

It's time to explain how come the users can use the network without the need to trust in each other's honesty and access what is rightfully theirs (authorize themselves not to an oracle, but to a decentralized system). In order to achieve that attribute, blockchains use encryption. [18]

It made perfect sense to use asymmetric cryptography. Such a system operates with two-keys-model - public key and private key. Bitcoin for example uses Elliptic Curve

Digital Signature Algorithm (ECDSA). A public key (as the name implies) is subsequently hashed into smaller units that serve as public addresses (note that more than one public address can be associated with any given private key) [132]. This hashed public key can be freely and publicly displayed. That is safe because there is no plausible way to derive the private key from the public one, which is true not only for RSA algorithm [43], but for ECDSA too [134] unless a strong enough quantum computer is invented [44]. This is ensured by a mathematical “one-way” function whose inverse has NP complexity [133].

Therefore any user can generate any number of private keys and any number of public keys (associated to each private key). Users can securely transfer funds without any third party involved. The blockchain accounting book is transparent and can be accessed by anyone with an internet connection or a mobile phone [135]. What is hidden are the identities of the account holders.

Thus a truly trustless system was created where no one needs to trust anyone but themselves while being able to personally validate that all the rules are being upheld.

4.1.3 Consensus Mechanisms

The common goal of consensus mechanisms across all implementations is to a) choose a node that will sign the next block of transactions into the blockchain, thus securing the network and b) resolve disputes / cooperate and settle on the future state of the code. This said, a consensus mechanism is a set of rules used by a decentralized community to reach an agreement (consensus) among users about the future changes of the whole network. As there is no central authority to enforce its decision upon the whole network, it needs a way to settle the disagreements on its own.

Consensus mechanisms are one of the most complex elements of the whole blockchain movement. For this reason only the 2 main consensus mechanisms will be explained in this thesis - namely Proof of Work (PoW) and Proof of Stake (PoS). While PoW aims to provide a provable immutability of the records, PoS directly supports more complex organization of decentralized autonomous organizations - at

a cost (see chapter “Turing completeness”). For more complex information see resource [47].

4.1.3.1 Proof of Work

PoW (just like any other consensus mechanism) is a set of rules that support execution of the daily operations of the blockchain as well as decision making purposes regarding the protocol. Unlike other consensus mechanisms the ability to sign new blocks is based on total hashing power of each node, which is fuelled by electricity.

PoW is effectively a need to perform specific brute force scanning for appropriate bit value. Whoever manages to do so first, gets the right to hash the next block into the blockchain, thus receiving block reward (monetary incentive) + transaction fees from all incorporated transactions. [18] The difficulty of brute force scanning isn't constant, but it adapts to the total hashing power securing the network in predetermined intervals.

On top of that users vote about possible code changes. Networks usually demand a consensus of 51%-100% users agreeing when debating code changes.

In order to deal with a one-IP-one-vote problem (which would enable bad players to manipulate consensus formation through unlimited account creation) it implements a sort of one-CPU-one vote system. In other words, the majority of hashing power in the system decides which changes will be implemented in the network. [18]

Proof of work was initially suggested as a way of fighting email spams [20], but its first effective application is Bitcoin. In Bitcoin it serves several absolutely vital purposes: as a consensus mechanism, it provides intrinsic monetary value, it serves as a financial distribution system and most importantly it provides long-lasting immutability/security [18].

Security/immutability, intrinsic value and environmental impact are interconnected. In order to explain the topic in an appropriate complexity and depth, an ample description is needed. While the actual energy consumption, comparison with its competing systems and the actual security of a single implementation will be further

analyzed in subsection “Bitcoin”, it's vital to explain what makes PoW as a consensus mechanism so unique.

Never before in human history a truly unique digital object has existed. Humanity was capable of creating unique identifiers for digital objects, but nothing has ever stood in our way to copy those objects, provided we had the necessary tools and skills (this is true for all digital objects: texts, images, videos...). Many years of cryptographic research lead to an outcome, where humanity is capable of provably spending unique digital objects across secure blockchain. [136]

In order for the above mentioned uniqueness to be true, the blockchain needs to be provably secure. PoW for the first time in human history have also connected quantifiable “work done” in the real world with a digital network/commodity. The quantifiable “work done” is the CPU brute force scanning fueled by electricity. This “work done” hinders the ability to make retrospective changes to the appended data in the blockchain even if the network was indeed successfully attacked.

With reference to [22] we can make the following explanation of transformation of energy to a scarce digital commodity:

Around the 1832 Gaspard-Gustave de Coriolis introduced the idea that “energy is work done”. The idea of “energy is work done” crystallized during the industrial revolution, which was the first time in human history when most of the “work done” was not done by humans anymore. The amount of work done by machines and nature has gradually risen ever since then.

“It from Bit” theory describes bit as the cornerstone of the universe [21]. Since a bit is energy, it could be deduced that “everything is formed by energy” and everything “costs energy”. Nowadays all things in our lives are linked to the price of energy since both nature and machines produce work through utilization of energy. In its absolute core, our economy is energy-based, not money-based. “In a free market, the cost of any good largely reflects the energy used in producing that good. Because free markets encourage the lowest priced goods, the energy used in producing any good is minimized. Money, which is the representation of the work required to generate goods and services, can also be viewed as stored energy.”

Energy consumption and world GDP has had the exact same linear growth from 1956 to 2016.

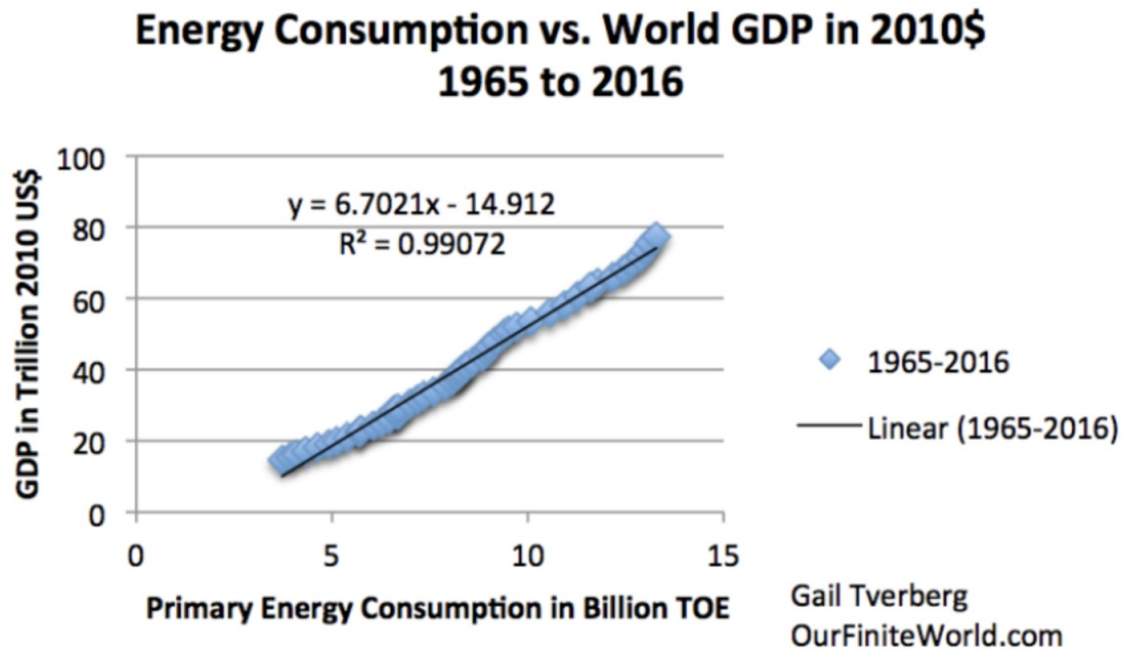


Figure 1. Growth of Energy Consumption and GDP [22].

In the light of this information, it shouldn't come as a surprise that industry leaders in the 20th century like Henry Ford or Thomas Edison have been experimenting with the idea of replacing dollars with “the energy dollar” or “units of energy”. The concept failed due to missing technology for effective transmitting and storing of such units of energy.

One of the fundamental roles of PoW is to convert electricity into Bitcoin (converting a part of the cornerstone of the physical world into the digital one). Bitcoin is capable of both proving that electricity has been burned (P2P network) and transmitting (asymmetric cryptography) this “burned energy” from one person to another. PoW is the proof that electricity has been burned [18]. PoW transmutes electricity into a digital commodity that is scarce by design, thus is sometimes rightfully referenced to as the “digital gold” (as it is provably scarce and it costs energy to mine gold too).

The security equation therefore relies on three main factors: a) upfront cost associated with hardware acquisition/leasing, b) continuous costs associated with the electricity that has to be burnt in order to perform the CPU scanning and its

difficulty, c) devaluation of one's cryptocurrency holdings upon the decision to abuse the network. [18,47]

4.1.3.2 Proof of Stake

PoS on the other hand was invented as a “greener” alternative. A very similar framework of security equation is being used, but the voting power allocation and the right to sign new blocks is based on the total amount of “staked” tokens instead of hashing power. The need to burn electricity associated with the CPU scanning has been completely removed. While this method (utilizing Turing completeness - see the eponymous subsection) unlocks unimaginable possibilities and manifests in many unique forms, it also comes at a cost. [47]

The costs will be analyzed first. As was described (and will be further addressed in subsection “Bitcoin”), signing a block in PoW requires a significant amount of electricity powering all the hashing. Possible ways to attack the PoW network will also be described in the same chapter. It was also stated that Proof of Stake uses a very similar framework of security equations. The problem that has been proven across multiple projects in history is when the substitution of PoW for PoS happens, while the rest of the “security equation” remains almost the same, the outcome of actual security differs. It was stated (and will be further described and proven in chapter Bitcoin) how the electricity burned hinders the actual ability of re-doing the blocks if one entity acquired 51%+ of the hashing power. The problem of PoS is when one entity acquires 51%+ of the tokens that are “staked” (does not equal “in circulation”) so far, since there is actually (almost) no computing “work done” behind the block creation, then re-doing the block also requires no computational power. Therefore an entity with the majority of the staked tokens can very easily re-do any amount of blocks, thus breaking the immutability. [56]

The PoW security algorithm not only counts on the cost of hardware that needs to be purchased/leased but also the cost of electricity and the actual time spent due to the network's “difficulty” (note that when the network's hashing power is not strong enough, attacks do happen [58]). In the case of PoS not only that the second

(electricity) and third (time spent) variable is completely taken away from the equation, but even the first (staking) variable can be gamed.

The economic disincentive to game the original PoS system is the investment one has to make in order to acquire the 51%+ stake. As such a move would vastly increase the demand for such a token, its cost would skyrocket and the attacker would have a hard time being profitable at the end of the whole endeavour.

In reality those tokens are almost never being bought, but either stolen [53], utilized through exchanges directly due to fraud [54], fake-staked [51], abused from within [55], short-sold [57] and violated in many other ways [47,56]. Different projects running on different Turing complete models employ different mitigating strategies which makes the topic even more complex and important [56].

The advantages will be explained next. Undeniable advantage mentioned by the multitude of resources is the marginal environmental impact in comparison with PoW [19,24,26,28,47]. While many advantages are employed in conjunction with Turing complete protocols, one is strictly connected to the PoS consensus mechanism. In PoW the native coins can be utilized for value transfer and fee payments only. In PoS they are being “locked in” the system in order to grant “strength” or certain “rights”. While the most important role of “staking” in original PoS systems is to gain the ability to sign blocks, various PoS systems implementations experiment with other possibilities of “stake utilization”.

4.1.3.2.1 Delegated Proof of Stake

For instance one of those implementations will be mentioned and further explained in subsection “Hive”. One of the PoS variations is called Delegated Proof of Stake consensus mechanism. DPoS is an implementation that enables users to delegate their stake to other users without forfeiting the actual possession. This enables users to utilize their voting power in matters where they don't want to make direct decisions . [59]

In the original PoS consensus mechanism delegations were not allowed and the users either exercised their network rights individually or they effectively forfeited those rights.

4.1.4 Immutability

As long as the implemented consensus mechanism resists 51% attacks, blockchain systems remain immutable. The extent to which this feature is achieved differs greatly across blockchain projects due to the differences in their consensus mechanisms.

It was described, and will be further addressed in subsection “Bitcoin” why PoW - namely Bitcoin - is the closest to an immutable system as we can get. PoS systems are immutable only until 51% attack is successfully mounted.

4.1.4.1 Timestamp

Immutability was explained. It's time to explain what a timestamp is. As the hash of each new block contains a unidirectional link to the preceding hash, which has multiple implications. One cannot change anything in the block retrospectively as it would change the hash too and one cannot change the position of blocks as suddenly a hash mismatch would occur, thus we can be quite sure that the chronological order of blocks can be trusted. It can therefore be trusted that hashed data must have existed at a certain time in order to get into that hash. [18]

This feature (in connection with the rest of the features mentioned at the start of the whole chapter) also for the first time in human history solves the double-spending problem in a decentralized environment. As the blockchain (an accounting book) can be trusted in its chronology, one cannot use funds that were previously sent to a different account as those funds are already attributed to a different account. [18]

4.1.5 Turing Completeness

Arguably the biggest fundamental difference between Bitcoin and most of the descendant projects is that Bitcoin is Turing incomplete. But first Turing completeness will be explained.

Note that when something will be labelled as Turing complete/incomplete it will mean that the project (on the scale between those two poles) inclines towards the mentioned pole due to current lack of consensus as to which projects are complete/incomplete. [27,47,48,49]

Turing completeness stands for the ability of programming language/software/protocol to simulate any algorithm that can be logically constructed in a replicable manner. [47,49]

Bitcoin is Turing incomplete due to the fact that its script can only perform one function - transfer funds. This (on purpose) severely limits the utility of the Bitcoin blockchain. On the other hand, protocols that are Turing complete allow more functions on top of the basic functions, such as general-purpose functionalities of autonomous organizations. In other words, with bigger Turing completeness bigger and more complex programming of Smart contracts is allowed. [47,49]

Both options have their advantages and disadvantages. A generally unknown historical fact is that original Bitcoin theoretical versions (1997) were Turing complete. Long discussions were held on the cypherpunk forums which led to Satoshi Nakamoto's final decision to make Bitcoin Turing incomplete. Since the singular purpose of Bitcoin is to store and transfer value, it doesn't need other functionalities. Turing completeness would actually make it more prone to all sorts of digital attacks. Other functionalities can be implemented as 2nd layer solutions. [27]

As was implied in the previous paragraph, Turing completeness unlocks multitudes of options at the expense of security. Computer hardware has been subject to all sorts of security vulnerabilities for the past 30 years. [50] The more options one unlocks the bigger possibility of a potential breach.

4.1.6 Smart Contracts

Smart contracts are an experimental attempt for trustless execution of contracts between engaged parties without the need of a third party utilizing blockchain technology. [52]

But first a regular contract is going to be explained. Contract is a legal document between two or more parties that binds them to something in the future. An example would be - Alice agrees to repair any damage to Bob's car in the future in return for monthly payments (= car insurance contract). Regular contracts (when not respected by any party) are evaluated and subsequently enforced by lawyers and judicial systems. [52]

What makes smart contracts special is conditions are both evaluated and executed by computers using a rather simple if/then function. Using the same example - Alice pledges to repair future car damage, while Bob locks a certain amount of money into escrow. Monthly payments are then being regularly executed. In theory none of the parties should be able to back down from the deal. [52]

In reality there are some problems. The first one has something to do with Turing completeness. Bitcoin, too, has smart contract compatible language but it is Turing incomplete [52]. On the other hand Ethereum (the biggest Smart contract blockchain) can be Turing complete [27,52,61]. As was described in subchapter Turing completeness, while Turing completeness grants the ability to code complex programs, it comes at the cost of security breaches [52]. This was proven many times, for example during the short history of Ethereum Classic/Ethereum where Smart contract hacks resulted in the loss of hundreds of millions of dollars [61,63] (in today's market prices). It takes a long time and highly skilled personnel to avoid those mistakes [52]. In theory it is possible to deal with this problem.

The second, this time a tremendous problem, is a so-called Oracle problem. When the reader carefully examines the stated example of a possible smart contract usage (car insurance), it becomes obvious the disagreement cannot be solved by code alone. While Bob's money is in escrow and cannot be pulled back he still needs to trust Alice to repair the car if any damage occurs. If she refuses to do so, Bob would nevertheless need to seek an arbiter who would determine the outcome of the dispute and force the losing side to either keep the promise and repair the car or find other means of compensation - in other words Bob would need a trusted oracle. A need for a trusted third party ruins the Smart contract purpose. [52]

The Oracle problem is a common occurrence when the Smart contract is supposed to solve a problem happening in the physical realm. Many cases which seem to be suitable for Smart contract solutions, in fact, aren't. Another example could be a house ownership represented by a non-fungible token. While Bob and Alice could swap the ownership-representing-token, both parties need to trust that the token actually represents the house. In addition to that, what if the token gets stolen? Would the house be in the thief's ownership? What if the private key to that token is lost? Does the house lose the ability to be traded? Or can the token be re-issued? And by whom? All those problems could only be solved by a trusted oracle which would break the Smart contract purpose. Simply put - "The ownership of the token cannot have dependencies outside of the smart contract platform". [52]

So far some effective use cases strictly bound to the digital platforms have been found. Two ineffective Smart contract usages have already been stated, therefore two effective usages will be mentioned now. First example could be a Decentralized Autonomous Organization (DAO). Although it could be hard to code due to Turing completeness it could provide an effective self-organizing tool for communities. The communities could then trustlessly vote on community matters, such as distribution of communal resources and decision making of what should be supported next [59]. Another use case that has emerged quite recently is called Decentralized Finance (DeFi). For a long time the crypto community has struggled to trustlessly swap cryptocurrencies without a need for centralized exchanges. Smart contracts were successfully used as a solution to this problem. Users themselves provide liquidity for cryptocurrency pairs which can then be trustlessly traded, thus bypassing the need for third party exchanges [62].

Summary of the section is in order. Blockchain is basically an information system built on top of a decentralized database. This information system has many variable attributes, hence it can be customized. It can be run on varying Turing completeness versions. At the moment it can concentrate mainly on immutability of past records or prioritize governance functions instead. It can provide tools for effective community governance. It is mostly used for organization of digital relations and objects, and

can be used to anchor the physical realm without forfeiting the aspect of decentralization only in rare circumstances (for example PoW mining).

4.1.7 Sharding

Sharding is an optional onchain (blockchain native) scalability solution that is recently being tested. A sharding blockchain system has the network nodes dynamically partitioned into subsets (shards). Each of those shards is responsible for managing its own blockchain which are mutually interoperable. Thus the same version of the blockchain is not stored by all the nodes. Instead each shard is responsible for storage of a portion of the data. By increasing the number of shards the total transaction throughput is increased as well. Sharding comes with a plethora of problems too. Sharding is yet to be thoroughly studied. Time is needed to uncover reliability and/or weaknesses of individual implementations. For more information see [142].

4.1.8 Tokenomics

Tokenomics is a term that stands for the economics of token(s) within their ecosystem. It covers all the token's aspects such as its creation (possibly backing), distribution, role in the ecosystem, removal (burning) etc. [77]

This said, the economy in tokenomics does not only represent monetary rules, but it also covers the governance of the whole ecosystem (in PoS systems). As such, it plays a crucial role for any system that aims to be sustainable. As will be shown in chapter 6, it is the most underrated and underdeveloped aspect of all decentralized scholarly projects.

This thesis tries to provide a framework that should be followed in order for a project to be perceived as viable. There are no truly objective metrics on how to evaluate this matter. The closest effort performed by the scholarly community regarding analysis of tokenomics is an empirical study of tokenomics from 2020 [78]. While all the hypotheses made in that article are relevant, the project sample contains a huge problem. For some of the analyzed projects the authors do not distinguish between what the creators of individual tokens “say” and what they “hard code” - which is of a major significance. Just because a creator says staked tokens will yield X tokens in

Y time doesn't mean it's true before the algorithm can be validated in the code. The only proven hypothesis in that article is that tokens based on ETH network correlate (price-wise) with the ETH network [78]. As a consequence, such tokens would be in existential danger in case of an ETH security breach.

There are almost no sources tackling tokenomics from a non-economic point of view. There is only one source I have managed to find which partly does so [90].

Burniske's book will be cited and utilized in section 5.5. Apart from the actual proof in the code that should be required by decentralized communities, the actual framework used in [78] is viable and will be partly used to assess viability criteria in section 5.5.

4.1.8.1 Premine

Premine is a term that stands for attributing X% of the initial supply to the creators of the platform before it is launched. Bitcoin had 0% of its supply premined for instance. Vast majority of the descendant projects chose to implement some sort of premine into their tokenomics structure. The theory behind premine is that the creators are further incentivized to work on the platform as their actual income is as big as the financial success of the token. The premine varies in between 5%-25%+. It is important to understand that premine in PoS system skews the voting power in the system as the creators gain uncontested voting strength by default. Premine is also oftentimes used in order to scam reckless investors [90].

The best practices that were implemented by funds I have been part of⁵ were - the lower the premine the better. 15% premine was the maximum and was only accepted if accompanied by superb utility and problem solving solutions and if the premine funds were locked for several years in an escrow. It was almost impossible to find a project that did not utilize premine in some way.

⁵ A rigorous evaluation has taken place with an aim to identify projects that can skyrocket price-wise. The price hike has not always turned out to be the case.

4.1.8.2 Utility

Utility is the core of tokenomics. Utility of the token represents what the actual use cases of the token are. The individual utilities are - payment method [18,78], yield (through staking) [59,62,78], store of value [18], ability to vote/strength of a vote [59], the ability to operate on the blockchain [18,59], etc.

Most tokens serve as a payment solution. That is already solved by Bitcoin (see the eponymous subsection) [18]. New projects need to differentiate themselves from the pre-existing ones. Some projects offer yield for liquidity providing [62], some in exchange for staking grant bigger votes in governance matters [59]. The utilities are usually combined together (meaning a token has more utilities) [59].

Just because the token has some sort of utility doesn't necessarily mean other projects don't offer better deals/solutions, nor that such a mechanism is actually needed. Nevertheless the golden rule is the utility mechanism/algorithm is thoroughly revealed and explained [90] and ideally implemented in code. Without the proof the utility remains just a brainstorm.

4.1.8.3 Problem Solving

Projects exist to solve problems. The problem has to be clearly defined. It has to be compared with the current market in order to validate projects plausibility as competitors may have already solved that issue. Its solving has to be aligned with the nature of the blockchain (permissionless/permissioned), its consensus mechanism and with the utility of the underlying token(s). [90]

4.1.8.4 Issuance

Increase of an ongoing rate of supply is extremely important too. The utility of the token has to grow in line with the supply rate, otherwise the token is going to erode in value [90]. A more in-depth economical explanation is provided by Liu [92]. The right amount of tokens have to be minted in order to support the intended utility of the token. For instance Ethereum has changed its supply rate throughout its history, therefore any asset that was significantly tied to its network had been affected too - which is a thing to keep in mind too.

4.2 Implementations

Thousands of implementations are in existence. Described implementations in this thesis have been selected indirectly by analyzed scholarly projects in chapter 6 (any project proposed as a possible solution) or directly by me (the project is a valid competition to the projects proposed in chapter 6).

4.2.1 Bitcoin

Bitcoin is a secure digital gold-like commodity. Bitcoin is global money with a predictable monetary policy, unlike government currencies such as Dollar or Euro. No third party is in control of Bitcoin and can manipulate its monetary policy to suit any personal benefit.

There will be 21 mil. bitcoins in total. Bitcoin uses the PoW consensus mechanism (see subsection "Proof of Work"). Unlike currencies issued by the state governments Bitcoin is deflationary. This feature is accomplished by a so-called "quantitative hardening", which means that roughly every 4th year the reward for every mined block is halved (currently 6,25 BTC) until the 21 mil. cap is reached. The difficulty of the scanning required in order for a single block to be mined roughly every 10 minutes, changes every cca 2000 blocks. [18]

Bitcoin is a valid option to opt-out of the state controlled currencies - in some countries partly, in some countries fully, but the same is true even for online information systems. [139]

In order to validate those statements, historical and factual excursions are in order. Reading the subsection "Proof of Work" again could be helpful too.

4.2.1.1 Money vs. Currency

The difference between "money" and "currency" needs to be explained first. According to some economic theories money is a superior term to currency. In order for a commodity to be perceived as money it has to carry out certain aspects. It has to be durable, scarce, transferable, verifiable and divisible. Currency on the other hand is merely a medium of exchange that is backed by underlying value of money - for which it can be exchanged at a precisely defined rate of exchange. "Money" therefore is commodities such as gold, silver, or the digital counterpart of precious

metals - Bitcoin. On the other hand “currencies” were state currencies during the age of the gold standard. [137]

Let's investigate the history of money used in the geographical location of today's Czech Republic. Throughout most of the well documented recent history (1750-1952 with an exception during 1914-1919 and 1938-1945) money was used either directly or it was backing its currency (although not always fully). A common aspect of currencies used in this era was its continuous devaluation compared to gold - which was backing them.

Since 1953 currencies enforced by state governments were not backed by money anymore. On top of that, those currencies are being deliberately inflated for various reasons by the Central bank [137,138]. Bitcoin is a form of self-defence against a constant loss of value. Despite the fact that Bitcoin is very volatile, whoever has held Bitcoin for 4+ years has a 100% chance of being net positive up until now (third quartile of 2021) [140].

4.2.1.2 Electricity Consumption

The intrinsic value has been outlined in subsection “Bitcoin” and “Proof of Work”, now the environmental impact will be discussed. Environmental impact is the most commonly occurring argument against Bitcoin in scientific articles [19,26,28] and in general [24]. The scientific articles that I have read disregarded PoW due to its high energy consumption [19,26,28] and proposed that Proof of Stake (PoS) or permissioned blockchains should be used instead. None of them thoroughly investigated PoW and its implications. They simply stated it exists and disregarded it as an “environmental catastrophe”.

At the time of writing Bitcoin's PoW consumes roughly around 78 TWh⁶ of electricity per year which is more than what Czech republic as a whole consumes annually (this number has been gradually rising since the inception of Bitcoin and as the document is being updated) [24]. Significant portion of this electricity is coal-based, as (not only) Chinese Bitcoin miners often tap into cheap coal-based electricity.

⁶ Note that it peaked at around 130 Twh throughout the year and dropped drastically following Chinese ban of mining and Bitcoin's drop in value.

[24,27,28]. Sources are claiming that Bitcoin is polluting the earth directly (PoW) [19,24,28] and indirectly (hardware creation) [24,28]. The fundamental problem in those studies is that they are one-sided. They fail to create an in-depth comparison with competing systems, they fail to recognize PoW as an instrument that brings benefits at a cost (as everything costs energy). They only provide information that PoW costs a lot of energy and is therefore partly responsible for CO2 pollution - and even that is only partly correct.

We will investigate the direct pollution theory first. Such a claim is based on the flawed causation and consequence. Such a claim would be correct if the electricity creation would be caused by the invention of Bitcoin. Truth is quite the contrary. Vast majority of power plants causing the pollution have already been built prior to the invention of Bitcoin. The pollution would be happening anyway if not regulated (self-regulation or governments) by any means (there may be unique exceptions, for example reopening of a coal mine in Austria - 2018 news - but after thorough research I wasn't able to validate whether that's true). As proof of that is yet again directly correlating energy consumption (thus energy creation) and worldwide GDP [22]. According to professional miner's testimonies (the owner of the very first decentralized mining pool) [27] and people that were in the Bitcoin space since its emergence [22,37] miners are proactively seeking the cheapest excess electricity, moving their rigs if necessary. This electricity is oftentimes being sold for less than \$0,09-\$0,02 per kWh [29] which at least partly validates the statement that mainly excess electricity is being used since this price is much lower than usual. In the USA, the average electricity price is \$0,13 [30] and in the Czech Republic the average price is cca \$0,27 [31]. Better yet, electricity does not equal energy. It costs energy to create electricity but there is no possible way to uncover how much "energy" is actually used to create a single Bitcoin. We can only estimate the value and amount of electricity burned. Electricity accounts for only a fifth of the world's energy consumption [41]. Comparing electricity consumed to energy consumed doesn't make any rational sense [37].

⁷ These are residential prices. Industrial prices are lower.

A better argument that requires more research in order to validate or disprove is the hypothesis that due to rapidly increasing efficiency of new ASIC miners there will be a horrendous amount of hardware waste⁸. The hypothesis also claims that in order to pay for newly created ASIC miners, the mining has to run nonstop, therefore it is hard to utilize volatile renewable sources of electricity. Studies claim that roughly every one and half years, the improvement of newly created ASIC miners is of such a magnitude that older ASIC miners are rendered more or less useless as they serve singular purposes (PoW mining) [28]. In reality the cycle of new generations of ASIC miners is slowing down as the race towards lower nm chips is reaching current technological limits. The latest generation of ASICs are 5nm and it has taken 4 years to improve upon the most efficient 7nm model from 2017. Prior to 2017 whoever had stronger ASIC miner was making the most money, but ever since then the price of electricity is the new denominator. According to the up-to-date ASIC miner profitability calculator, nowadays SHA-256 ASIC miners created in 2017-2018 are still profitable when the price of electricity is \$0,05 [32]. As of now, the above mentioned statement seems to be invalidated. There are other factors to be taken into account. It needs to be stated that the Bitcoin network has undergone another halving on May 11th 2020 (Bitcoin reward for every single block reduced from 12,5 BTC to 6,25 BTC). As a byproduct of such an event, a large number of miners are immediately rendered priced out by more effective competition [29] thus creating sell pressure of older generation ASIC miners. These are then sold off to more efficient miners, or they become electronic waste. Another factor to be taken into account is that in nominal numbers the total hashing power in the Bitcoin network has skyrocketed since 2018. Although when switched to logarithmic scale (which is more suitable when dealing with positive figures that at any given point underwent exponential growth) it is clear that, percent-wise, the growth is resembling an asymptotically bounded function - the growth is slower and slower as time passes by – see Figure 2 and [34]. The increase in effectiveness of newly manufactured mining machines compared to older generations is also slowing down [22,34]. The future of this matter is still unclear. That said, breaking even at the moment, while not farming nonstop, especially if the newest mining rigs are not bought at the start of the halving cycle (4 years long cycle), can prove difficult when the price of electricity isn't low

⁸ This argument could be used for any given electronic gadget.

enough, but it is by no means unreachable. It also is possible⁹ that Bitcoin will be consuming less electricity in the future which means that regularities observed now will not be the same in the future as changes to one variable in the equation will of course change the outcome [37].

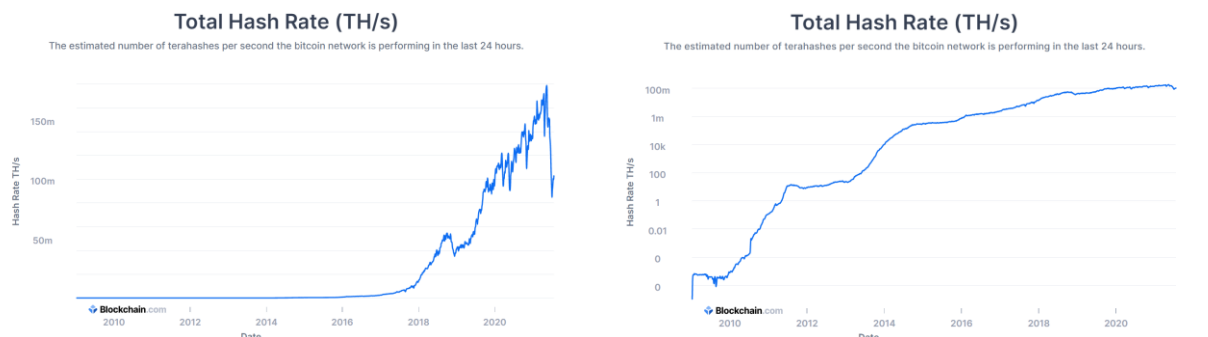


Figure 2. Total Bitcoin hash rate: linear (left) and logarithmic (right) scale [34].

There are very different research results both from opposing groups as to how much of the overall electricity consumption is renewable. In its earliest stages of their research Coinshares claimed that overall “green” energy consumed is 80% [35]. On the contrary Digieconomist (who has proven time and time again on their twitter account that he is an anti-Bitcoin fanatic) claims that it's only 28%. In reaction to that, Coinshares stated that they might have underestimated the magnitude of rig migration due to Sichuan’s dry and wet seasons and that the actual number would be around 42% from October until March [36]. As of now it is virtually impossible to make truly precise calculations (moreso after the Chinese ban). Nevertheless, all evidence points towards the Bitcoin mining energy mix being geared generally higher towards renewable sources than all other industries due to the amount of stranded and curtailed sources of renewables, which other industries have troubles exploiting.

4.2.1.3 Relationship to Conventional Banking

Another argument against Bitcoin's PoW is the comparison between Bitcoin's expensive solution to “money management” compared to traditional banking like

⁹ Due to halvings and lesser BTC rewards as time goes by.

systems. Most commonly used sub-argument is the comparison between Bitcoin and VISA transaction cost. According to research a single Bitcoin transaction cost equals 476 084 VISA transactions. While this statement is mostly correct, it shows severe misunderstanding of the depth of the problem. One cannot simply compare the Bitcoin network to a single representative of the traditional financial system. Nor is the author's knowledge represented by his statement that there are cheaper consensus mechanisms that Bitcoin could switch to, such as PoS [24]. The author is completely misunderstanding the security and the depth of the problem. But first things first. Bitcoin is not in competition with VISA. Bitcoin is in competition with the entire traditional banking and monetary system and should be instead compared to it [22,25]. The entire banking system (counting only branch costs, ATM costs and finance related server costs, not employee consumption, ERPs, accounting systems, websites, if one wanted to get more philosophical - the enforcing system component, etc.) is according to rough estimates around 100 Twh [25]. Total estimated energy consumption exceeds 650 Twh per year (of course without the enforcing component) [28], but if we wanted to fairly compare those systems we would need to take into account more than just electricity consumption spent on mining. Comparing morality and effectiveness of those monetary systems is not in the scope of this thesis, only finding out whether PoW is a viable consensus mechanism, therefore further comparisons won't be made. If interested, a reader should pursue his own further research (for example about the number of transactions in both systems, scalability solutions, annual improvements, emittment of money, state monetary policies through central banks etc.).

4.2.1.4 Security

Bitcoin as a competitor to the traditional monetary system has been outlined. It's time to make the final connection to the security/immutability problem. Bitcoin and its PoW was explained as a "proof of electricity burnt". The enormous amount of electricity required to run the network was estimated. Now, once the CPU effort has been expended, a new block is hashed into the blockchain in a way where the hash of the previous block is stored in the new block, thus becoming part of its hash. This renders all the blocks practically immutable as the blockchain would refuse changes to any blocks due to inevitable hash mismatch. In theory, there is a way to change both old and new blocks. In order to change the old blocks all the CPU work that has

been done so far would need to be redone. In other words the attacker would need to start from scratch. As electricity cannot be “reburned”, an attacker would need to spend a similar amount of new electricity while also acquiring enough hashing power to be “stronger and faster” than the honest blockchain and then finally overrule the honest blockchain by becoming “the longest chain”. That is economically implausible.

More viable attack option is a so-called “51% attack”. In order to successfully perform such an attack the attacker would need to start working “silently” on his own defiled version of the blockchain (instead of starting from the scratch, this could be done at any point, say 100 blocks back). Again the attacker would need to have larger hashing power met with the electricity requirement at his disposal for the whole time in order to be faster than the honest chain. An attacker could theoretically double-spend using a 51% attack by intentionally not incorporating his transaction in the defiled blockchain version. Then, if his version of the blockchain became the longest, he could broadcast it back to the honest nodes, which would take the defiled version as the correct one (since the longest blockchain is always deemed as the correct one). The protocol would return all the funds from the missing transaction (that were intentionally removed) back to the owner - thus effectively allowing to double-spend.[18] The 51% attack is currently also economically implausible, but during the hashing power downtimes that can occur under specific circumstances (such as hard forks¹⁰ or mining bans) it could happen. Slush, the creator of the first decentralized mining pool, also fears the 51% attack as the most plausible jeopardy to Bitcoin [27]. In line with his fear is also Dominik Stroukal who explains from the economical point of view why there is a real danger that in the future Bitcoin will be consuming less electricity than it would ideally need to in order for its security (implausibility of any vector of attack) to remain above an acceptable level [37,39]. Due to the enormous amount of electricity hashing power and the limited ways to attack the blockchain, it can be safely stated that Bitcoin is very secure and will be for a dozen years to come at minimum, provided the security equation will not change drastically, for instance due to possible disruptive innovations improving hashing energy efficiency. In about two halvings the future reality will need to be reevaluated.

¹⁰ See <https://www.investopedia.com/terms/h/hard-fork.asp>

Few more facts need to be stated in order to sum up this long subsection. It is a mental fallacy to think that this matter (morality of PoW mining) has a clear and scientifically comprehensive solution. It does not, but unfortunately a lot of people are unable to change their perspective on a matter where they have already acquired significant knowledge [38] as they become “trapped prior” [42]. As value adjudged to all, physical/mental/digital, things are strictly subjective [40], it all comes down to individual preferences. It is a fact that Bitcoin is one of the few successful decentralized worldwide digital monetary systems that cannot be controlled by any government state and their debt policies. It's also a fact that Bitcoin does consume a lot of electricity and the nominal value of “electricity consumed” will only grow over time (although it may do so at a lesser rate). The current state of electricity consumption is nowhere close to “too much” for people that value monetary freedom and free money over enforced monetary systems run on endless inflation and debt. On the other end of the scale, people that do not feel oppressed by current state-enforced monetary policies and do not fear the debt, nor the inflation (or better yet, can use it to their advantage), may not find value in enormous electricity consumption that comes hand-in-hand with Bitcoin. It is up to each individual to choose their preferences. As long as people will voluntarily choose to buy Bitcoin, its price will rise as the information that people value the project highly will be reflected in its price, thus the knowledge about that fact will be spread across society [23]. Miners will then have enough resources at their disposal to continue mining and burning electricity.

4.2.2 Ethereum

Ethereum has consistently been the 2nd best blockchain project in terms of market capitalization for several years in a row. Ethereum was invented with an intention to further scale up programmable options regarding Smart contracts. It is very close to Turing completeness, the only limitation (for security reasons) being the Gas limit of ETH transactions - the language itself does not have limitations, but the Turing iterations are not allowed to run endlessly.

Ethereum is currently undergoing a profound transition to v.2.0. It is switching from PoW to PoS. It is enabling ETH staking. It is completely reworking its security equations. It is completely reworking its incentives. It is transitioning from “one blockchain” to a sharding scaling solution. Its Lindy effect [76] will thus be effectively reset to 0. As of now (June 2021), only the layer 1 (“The Beacon Chain”) has been launched and with it ETH staking. The merge with the current ETH blockchain and sharding itself hasn't been launched yet. [141]

Ethereum has decided to follow the path (PoS, sharding) of its younger competitors, such as Polkadot or Cardano.

4.2.3 Polkadot

Polkadot is another sharding blockchain system. Polkadot network forms around a main (layer 1) blockchain - this time called “Relay chain”. Individual shards are called “Parachains”. In Polkadot, Parachains will implement their own consensus mechanisms and rules. Auctions will be held for Parachain slots. Polkadot aims to scale up to 100 Parachains. There is also an option for smaller applications to share a Parachain slot together, thus lowering their transaction throughput. When a Parachain is being shared by multiple entities it is called a “Parathread”. [143] At the time (June 2021) of writing Parachain rollout is being tested on Kusama testnet and will soon be available on mainnet too. Parachains slot number will be much lower during the rollout than the intended 100 Parachains in total.

4.2.4 Cardano

Cardano [145] is a PoS blockchain network that aims to serve a similar purpose as Ethereum or Polkadot. Its distinguishing feature is that its development process is based on detailed conversations. Cardano is the only blockchain protocol among the top cryptocurrencies that has been peer-reviewed [146]. As a result it experiences one of the slowest (but most thoroughly planned) roll outs.

Its roll out is divided into 5 so-called eras. Since roughly 2015 up until now Cardano has successfully gone through 2 eras - Byron and Shelley. While Byron wasn't technically decentralized, Shelley era concentrated solely on incentivization and increase of community run nodes. Cardano aims to roll out several other

functionalities. During its Goguen era (current) it aims to enable smart contracts. Then during the Basho era it aims to make a transition to a sharding blockchain system. Finally during the Voltaire era it will aim to maximize governance options for the community. [144]

4.2.5 Hive

Hive is an example of a DPoS blockchain project. It originated as a blockchain-based blogging platform. It supports appending articles directly into the blockchain as long as they do not contain pictures and are formed by fewer than 32,000 characters.

Hive is governed in a way where the community votes in 20 validators (block producers) and any protocol changes require 85%+ consensus - meaning 17 validators agreeing. The project found many other ways of token utilization. The more tokens a user “stakes,” the bigger allocation of the network's bandwidth (called resource credits) they receive. It also grants larger voting power both in terms of token distribution and in terms of token allocation to development projects. The system supports sending of encrypted messages, decentralized private key recovery, additional 51%+ attack mitigation techniques and “communities” system. [59]

The project itself is a fork (which happened in 2020) of Steem as a reaction to a 51%+ attack where dozens of my colleagues and friends lost assets worth millions of dollars in total. Justin Sun, using fraud, acquired the majority of stake by (ab)using exchanges. Luckily 85%+ of the validators are needed in order to make changes to the protocol and to sign blocks. This position wasn't allowed by the community which powered just enough tokens to force a stalemate. That bought enough time to prepare the Hive fork. [60]

This section presented five examples of blockchain implementations, ones that are the most relevant for the topic of this thesis. There are many more consensus mechanisms, including combinations between PoW and PoS, which were not covered, and more are bound to come in the future.

5 Blockchain for Scholarly Communication

In this chapter a theoretical analysis of the possible connection of Scholarly communication and blockchain technology will be provided. Blockchain journals will be theoretized more thoroughly.

5.1 Blockchain Journals

So far in this thesis a theory was provided, claiming that the scholarly community is a club and a decentralized group (see “Journal as a Club”). Then it was shown how the actual people behind the journals are the true flag-bearers of merit, while having the option of abandoning the journal when deemed immoral (see “Journal and its Reputation”). Finally some examples were shown demonstrating various approaches utilized by various journals that can lead to scientific success (see “Alternative Journals”). It's time to delve deeper into the possible connection of blockchain and scholarly communication.

If the scholarly community truly is a decentralized club (as outlined in subsection “Journal as a Club”), then “any innovative technological solution to scholarly communication problems must primarily focus on providing support for communities and their governance structure, for which the blockchain technology is a promising match” [5]. Not only that blockchain could empower the communities themselves and enable them to manifest in a truly decentralized manner due to the consensus mechanisms. It would also make the actions of the researchers behind those decentralized journals as true flag-bearers more transparent. It would also make the utilization of scientometrics more transparent and agile. If the blockchain features would be set up and utilized correctly and a critical mass of scholars would be active on the platform, the scientific community could unlock a whole new level of efficiency through decentralized self-governance [111].

Let's delve deeper into what should be visualized behind the term “blockchain journal”. Blockchain journals should rather be perceived as a blockchain platform that would support creation of journals. Such a platform would support high customizability for specific needs of specific scholarly domains. Coding an effective

and secure blockchain/decentralized application of such a scale is not an easy, nor cheap task. A single blockchain journal platform would most likely, but not necessarily, encompass a multitude of scholarly journals, sharing the same journal framework (similarly to OJS).

It's time to dissect which blockchain attributes are useful for scholarly journals. This chapter is partly a practical part of this work. At the end of the chapter a viability criteria suitable for creation of decentralized journals will be presented, based upon the analysis of scholarly communication (provided above), blockchain (provided above) and theoretical projects trying to figure out possible ways of setting up such a decentralized system.

5.1.1 Permissioned X Permissionless Blockchain

Subsection “Permissioned blockchain” tackled the difference between permissioned and permissionless blockchains. The permissioned blockchain was recognized as a (semi)centralized solution. Permissioned blockchains are perceived as a potential solution by the very same articles that recognize it as (semi)centralized. (except [19] which concludes incompatibility between permissioned blockchain and Open Science) [26,46,47] There are two main arguments supporting this claim. First argument is an arbitrary division of roles - “as non-experts/non-scientists lack the necessary experience to make well-funded decisions in such a system” [19]. Another argument is that trusted third parties do exist in the form of research institutes and government agencies. The author of the claim goes as far as saying “it is hard to believe that even under the worst circumstances a government or other entity would try to infringe blockchain securing computers in a blockchain for science to censor research results” [26].

The first argument is valid. On the other hand as was shown in chapters “Scholarly journals”, “Peer review” and “Journal and Its Reputation” reputation, experience and skill are absolutely incremental for science. This said, any purely decentralized scholarly system would be heavily relying on well thought-out and implemented reputation models. Next subsection will provide an in-depth explanation why that would solve the problem too, while not discarding the decentralization aspect.

The second argument is absolutely invalid and oblivious to history.

Dictatorial/totalitarian regimes have proven time and time again there is nothing that would stop them from enforcing their vision through propaganda. Propaganda rarely stays solely in politics and is oftentimes forced through “information dissemination” channels. The history of libraries in Czech Republic during the communist era can serve as an example. Libraries during that time were under the direct command of the government leaders and their sole purpose was to spread the “correct” perception of reality [75]. Whoever claims government institutions can be unconditionally trusted is simply wrong. Scholarly communities have to make sure their findings cannot be altered when the need for some party arises.

As such, a permissioned system would be in competition with the current journals, they would definitely want to be a part of it if they saw the system is about to succeed. Journals are the flag-bearers of reputation in the scholarly community at the moment. Any system trying to compete with them cannot be set up in a way where it would grant the journals the same (or even bigger) power than they already have. It was explained in many examples throughout the work - journals cannot be unconditionally trusted as well. Such a permissioned system would maintain the same problems we are facing now.

Authorized nodes in permissioned blockchains can mutate the blockchain itself. Permissioned systems do not solve the trust problem that exists in science at the moment. And most importantly permissioned blockchains are centralized. As the name of this whole thesis is “Utilization of Decentralized technology in Scholarly Communication” it would be an oxymoron if a centralized solution was proposed.

While others are free to explore permissioned solutions, my future work will solely concentrate on permissionless decentralized solutions.

5.1.2 Consensus Mechanism

Consensus mechanisms are one of the most complex elements of blockchain technology as explained in the eponymous subchapter. I, from my position, can merely analyse which paths should be considered for further research, and which ones are objectively bound to fail.

It was explained how PoS does not guarantee immutability of past records. All the sources claiming that PoS is immutable are fundamentally wrong [19,24,28]. In the previous subsection it was mentioned that the scholarly community has to make sure their findings cannot be altered in any way, no matter which third party would find value in doing so. Science has to stay as objective as humanly possible. Luckily this doesn't mean PoS cannot be utilized in any way. Although if the PoS consensus mechanism was to be utilized on its own, the scholarly system could be susceptible to retrospective changes regarding data only stored on the blockchain, such as for example scholarly reputation - which is unacceptable.

On the other hand PoW, when backed by strong enough hashing power (like Bitcoin), is immutable. It was also shown in the eponymous subsection that PoW doesn't mean fundamental immutability either, but some projects, such as Bitcoin, have accumulated strong enough Lindy effect [76] that back the economic equation of immutability. From the point of view of immutability, PoW is the right choice. Voting power in pure PoW systems is solely reliant on hashing power which does not suit the needs of the scholarly community either. It isn't in the best interest of the scholarly community to allow the wealthiest people to have the strongest vote regarding the scholarly problems (which is also a problem of today's PoS systems).

This said, the scholarly community needs to utilize PoW in order to achieve immutability and PoS in order to achieve voting that accurately represents and reflects the scholarly reputation.

There are multiple ways to approach this problem. From my point of view the most logical way to go seems to be the utilization of Bitcoin for the storage of hashes of scientific findings/reputation while setting up some sort of PoS DAO (DAJ) utilizing weighted votes based on the users reputation regarding scholarly matters on top of existing implementations such as ETH, DOT, or Cardano. The other option is to explore hybrid PoW/PoS systems.

5.2 Viability Criteria for Blockchain Journals

We'll now summarize this chapter and provide examples of scientific solutions using the knowledge acquired in subsection "Tokenomics" and put together viability criteria for Decentralized Autonomous Journals (DAJs).

Scholarly community has been recognized as a decentralized club (see "Journal as a Club"). The most suitable blockchain implementation enabling the most effective digital manifestation of such an entity is permissionless (see "5.1.2 Consensus Mechanism").

Scholarly community has to define the problem that is supposed to be solved by the DAJ. Current problems hindering scholarly communities are described by dozens of articles investigating some sort of decentralized solutions (exceptions not investigating decentralized solutions will be cited too). Those problems are oftentimes recognized by a multitude of articles with only little nuances. The problems are namely - suboptimal¹¹ journal pricing, suboptimal Open Access solutions, rigid journal platforms, rigid articles that have not undergone any change since the papyrocentric era (apart from being digitized), suboptimal usage of scientometrics (mostly relying on citations and impact factor), the only real option of how to farm scholarly reputation is via publishing and citations (other indispensable scholarly commitment such as peer-reviewing doesn't directly boost the reputation) and suboptimal peer-reviewing processes [1,3,4,5,7,8,9,10,11,17,19,26,68,79,80,81,82].

One of the responsibilities of scholarly communication is to make sure the scientific data and findings cannot be tampered with by any third party. If blockchain is the solution of choice¹², it is vital to utilize PoW either directly (ideally through Bitcoin as explained in chapter "Proof of Work" and "4.1.3 Consensus Mechanism") or in Hybrid PoW/PoS implementations. If any scholarly community wants to organize itself or its DAJ in a decentralized manner, PoS also has to be utilized in order to provide an

¹¹ Word suboptimal is being used since it isn't clear what is the price, scientometrics, etc. that would reflect the reality the most accurately.

¹² Centralized solutions such as Digital Archives following the OAIS Reference model are also an option.

option for in-depth decentralized governance models. Potential usage of smart contracts that could further improve the DAJ should be investigated (while keeping in mind their limitations).

There are numerous alternative approaches to how DAJ can be set up and what its ultimate goal should be (problem to solve). This is a (incomplete) list of the core fundamental decisions every scholarly decentralized project has to make:

- What are the problems that are going to be solved by the project and how
- Type of scholarly data that is going to be stored
- Which blockchain or other decentralized solution can store this data
- OA/Paywall and fees associated with those solutions
- Which tokens are going to be used and which utilities are going to be associated with them (including votes that alternate reputation of other peers)
- Interoperability with other scholarly tools

5.2.1 Problems Addressed

At the beginning of this section the majority of the currently recognized scholarly problems have been stated. Decentralized projects have to either choose one or more of the stated ones or come up with a new one. The problem has to be clearly defined and a thorough explanation of the intended solution that the platform is going to offer has to be provided.

5.2.2 Type of Data Storage and Decentralized Solutions

This thesis is exclusively concerned with journals and their potential solutions and will continue to be so. There are other scientific data that are too big to fit into a blockchain - such as raw measurement data in Astronomy [83], or any other big data. Even storage of pictures (therefore scientific attachments and supplements) may be too expensive on certain blockchains - like Ethereum (current Ethereum v1.0) [84].

Projects can therefore decide either that the decentralized database will only store the articles and reviews, therefore no 2nd layer solution is needed (as blockchains

that chose as its “problem to solve” a censorship free appending of articles exist [59]). Or they can choose to store bigger data while utilizing other decentralized solutions suitable for data storage such as IPFS (see [129]), LOCKSS (see [130]) or Storj (which uses blockchain to reward its users) [93].

5.2.3 Tokens and Fees

Every permissionless decentralized blockchain has to have its underlying tokens and fees associated with the maintenance of the network. It is of course technologically possible to set up a blockchain without a token. But blockchain is a rather expensive form of database. If there were no tokens how would the operations of the network be financed? It's very hard to find examples of tokenless blockchains. Those few articles that try to prove their point that blockchain can be sustainably done without tokens mention only permissioned blockchains (where the companies/government running the blockchain have to pay its expenses) [94].

There are permissionless decentralized projects that are not based on blockchain technology such as IPFS which are tokenless. IPFS relies mainly on the inner motivation of the contributing users. But the team behind IPFS is well aware of the fact that inner motivation may not be enough to permanently sustain the IPFS network and the team has been working on an incentive system using blockchain and tokens via Filecoin [95]

It has been explained (5.1.2 Consensus Mechanism) that science needs to utilize PoS in order to utilize the DAO governance option - therefore it needs a native blockchain token of some sort. The token has to have clearly defined tokenomics (issuance, backing, burning, fees, etc.) which will ensure its sustainability. There has to be a clear distinction between matters that money can decide and between science matters that only “scientific reputation” can decide (non-fungible non-tradable tokens are the best option). This said it needs more types of tokens to operate effectively.

Scholarly communication is also in need of an onchain payments solution. It was explained in this work why Bitcoin is a very good solution. Occasionally using volatile solutions may not be in the best interest of scholarly communication (it may overpay

certain tasks at certain times due to the volatility). As a solution to that a project should use trustworthy stablecoins as a stable option to execute onchain payments if necessary.

Finally, the information about the cost of running the blockchain has to be calculated and it has to be demonstrated that the incentives are set up correctly in order to sustain the network.

5.2.4 Interoperability with Scholarly Tools

Throughout the history of scholarly communication many supplemental tools have been created. The most utilized ones are DOI and ORCID. There are also new services being created and tested - such as Scite [96]. As decentralized structures by default lack the enforcement of interoperability standards, the strength of those decentralized systems increases when they voluntarily make themselves interoperable with the currently utilized tools. As those projects have their APIs documented and operational, creation of new tools on top of the network is effectively supported.

This said, the new models of scientific frameworks should mention which of the existing tools can be utilized and possibly under which circumstances (for example authors of scholarly articles conventionally state their names and their ORCID IDs, but they can also choose to stay anonymous; some can avoid ORCID usage completely).

6 Review and Analysis of Current Blockchain-based Projects

Now that the basic framework of “minimal viability” has been presented, a qualitative analysis and review of current market solutions and disclosed theories will be performed. Possible proposed scientometrics will not be evaluated.

First part will be the review of theoretical blockchain-based solutions. This category has been defined as “projects that have not yet launched its product, nor tried to

gather funds for the project and projects that have already failed/ceased to exist and left only their ideas behind”.

The second part will be the analysis of launched blockchain-based projects. This category has been defined as “projects that have publicly disclosed their testnet or mainnet versions or that have tried to gather funds in order to launch”.

Pretty much the same template will be used for the description of projects in both categories. The template has three parts:

- Focus and usage
- Tokenomics
- Open source and livability check

Focus and (for launched project) usage will concentrate mainly on:

- Definition of problems and projects' solutions
- Which blockchain is going to be utilized and how
- Support for 2nd layer solutions and interoperability
- Journals' topics
- How many articles have been published

Tokenomic will concentrate on:

- Analysis of the tokens and their utility
- The “OA” methods supported

Open source check and livability check will concentrate on:

- Github open source check
- Github commits check

Two main sources have been used in order to gather all the projects for review/analysis [19,110], which were complemented by ad-hoc internet searches. Those sources contain over 60 (not only) scholarly decentralized projects. All of them have been inspected and the relevant ones were selected for this addition.

6.1 Review of Theoretical Blockchain-based Scientific Solutions

6.1.1 Bitviews

Bitviews aimed to solve the journal exploitation (price, centralized servers, etc.) problem. It has decided to use a permissioned chain for this purpose [9].

The Bitviews team estimated the project would cost 250,000 GBP. It aimed to raise the funds via closed crowdfunding that would be held between research institutions. The team promised funds would be returned if the target was not met. [9] The target of the crowdfunding that occurred from February to May 2020 was not met and there is no up to date information about the project.

The price is the only aspect that can be reviewed in comparison with the template set up. The Bitviews paper does not provide an in-depth calculation of the price. The team only estimates the price. That is the exact opposite of what was proposed in this work. While the price target is roughly comparable to the minimal estimated OJS costs (see "5.3 Alternative Journals"), that is not enough. On top of that it doesn't provide calculation about the associated further costs. The calculations are ultimately vague/nonexistent. According to the implication of this thesis and its outlined scientific framework, Bitviews project was bound to fail - and it did.

6.1.2 PEvO

PEvO targeted two main scholarly problems - centralized repositories and no monetary compensation for scholars' direct contributions (articles and reviews). [82]

As a solution it proposed to utilize the original Steem blockchain. The Hive project [59] is a Steem fork that was created in a reaction to a Chinese invasion [60] which effectively centralized the original Steem blockchain - which disqualifies it as a decentralized technology. As the idea of PEvO has been born long before the Steem takeover, for the purposes of this review the Steem blockchain will be understood in its former decentralized state.

The Steem blockchain was originally a blogging platform. It supported appending articles directly into the blockchain as long as they did not contain pictures and were formed by less than 32,000 characters. Users that have staked Steem tokens were also capable of directing new token inflation to the appended articles via weighted likes.

It was correctly assessed by the PEvO team that the Steem blockchain had a lot of traffic and a way had to be found to filter out the non-scientific stuff. For that purpose an API was planned that would broadcast only the science-related articles to the users. Authors would also have an option to make anonymous comments. [82]

The PEvO team also correctly identified the Steem's limitations and proposed utilization of a 2nd layer solution in the form of IPFS in order to store picture appendices and articles longer than 32,000 characters. [82]

Had the project succeeded, it would have been open sourced. The project would also be totally free to use. All the minimal fees associated with the Steem blockchain would have been paid by some members of the PEvO team. [82]

But other algorithms than those inherently coded in the Steem blockchain were never created. “The algorithms for the rankings, and how each different factor like titles, impact points, community ranking, publications, reviews and self-proclaimed expertise is weighted, will be transparently developed by a scientific advisory board. The data is public, so other algorithms can be used for different kinds of weightings. “ [82]

So at the end PEvO managed to propose a project where scholars could publish their articles and receive financial rewards from the Steem community via inflation allocation. Without the reputation algorithm (therefore possibility of alternative peer-reviews) such an information system would rather serve as an informal dissemination space where scientists could re-publish their articles in order to farm some cryptocurrency.

As a face-to-face communication with the creator of PEO at the Steem conference in November 2018 confirmed, the project has been dormant for many years as no valuable scientific traction has been gathered. The idea has been used in the project Stemsocial (section 6.2.3).

6.1.3 Open Science Network

OSN is one of the most complex decentralized projects related to science. It defines three main problems that are currently negatively affecting science: ineffective usage of scholars' time due to the need to apply for grants and serve in the evaluation panels of funders, expensive monopoly-like journals that don't financially compensate scholars for peer-reviewing and the research reproducibility crisis. [81]

The first problem is supposed to be solved by the ability of the OSN information system to support any imaginable funding/contract scheme with any rules associated with it by any user [81]. This would unlock new ways for scholars to raise funds for the project or even sustain themselves, but it's not clear how much of the scholar's time would be saved. In fact, more scholars would need to spend time doing financial decisions and calculations (which is in direct contradiction to the defined problem).

The second problem is supposed to be solved simply by OSN blockchain existence. The paper claims that strictly money-wise decentralized blockchain solutions would be cheaper by order of magnitude than the current journal systems. They would also help with the securing of full ability to exercise the authors' copyright [81]. The payment for peer-reviewers would rather be solved by the ability to create flexible contract schemes. If the project stated which blockchain architecture would be used, then precise calculations that would back the monetary efficiency could be provided - but that is not the case.

The third problem is supposed to be solved by directing a portion of revenues from patents, applied technology and donations into a so-called "reproducibility fund". This fund would exist in order to provide an additional monetary incentive for scholars to reproduce and validate research. The community would vote which findings need to be validated. The validation would be compensated from this fund [81]. While the

idea makes sense it relies on the success of the platform or donations. If the project succeeds it may solve the outlined problem. Further validation will have to occur if OSN actually launches.

The selection of blockchain technology for the project hasn't been done yet. The candidates are (a) Ethereum with a custom ERC-20 token and (b) Rootstock with smart contracts realized in Bitcoin. An IPFS based second layer storage architecture is planned with Filecoin for integrity and as an incentive. [81]

An unusual component of the project is that in the long run it wants to diverge from the centralized identifiers (ORCID, researchID) and utilize decentralized identifiers where researchers own the data and can decide to whom they'll show it. Although initially users will be incentivized to have them in order to receive the native tokens. [82]

The project also correctly assesses it is a viable option to fairly distribute scholarly reputation and credit it to individual tasks in collaborative works [82]. On the other hand this project also hasn't revealed any reputation algorithm (which means it doesn't exist and such a solution couldn't be practically implemented yet).

The article also proposes something like Universal Basic Income (UBI) for scientists - "By utilizing tokens and having a pseudo anonymous ID representation for members of the network, we can subsidize research work utilizing a monthly emission of research tokens. The specific rules for this have to be analyzed in detail to manage inflation control. Cutting dependence on grants and the time and overheads spent on research applications and their analysis represents a potentially huge increase in efficiency per dollar spent." [81]

Tokenomics of the project is described in [99]. 100 million research tokens (RES) are planned to be minted in total. The utility of this token will be the weighted DAO voting. In addition to that, every action on the network will have an associated fee which will be accumulated in a fund. The initial proposal is to distribute this fund into three categories: (1) applications and development, (2) reproducibility and review, and (3) special research initiatives. [99]

There is no reasoning behind the 100 million token cap. In general no distribution algorithms, nor potential fee prices are calculated.

This said the RES token is a financial instrument, plus it grants voting power. It was explained in this thesis (see “5.2.3 Tokens and Fees”) why it isn't in the best interest of the scholarly community to have the voting power measured in financial strength. Unfortunately that is the exact approach of RES token which mainly serves as money (for which we already have solutions such as Bitcoin). Furthermore the explanation of the token is vague considering its importance to solve the defined problems.

6.1.4 Decentralized Research Platform

I have requested permission to see the detailed whitepaper in March 2021 which I was not granted. For that reason the only source of information about the project is their official Medium account¹³. Decentralized Research Platform (DEIP) is in its architecture yet again a Steem clone. The authors of the project have already produced such a clone called Scorum which was a sports related Steem platform. Therefore similar features and properties (including 2nd layer solution needs) as explained in subchapter “PEvO” can be expected. They can be expected but they are not directly mentioned.

This said, similar problems and solutions can be expected too, although they are not precisely defined. According to one of their articles “DEIP has many potential applications, but the market it fits most is that of funding scientific research, whose major players are funding agencies, governmental institutions, and enterprise R&Ds.” [102] Such a statement can be validated by tokenomics analysis.

On DEIP there are 3 native tokens - Expertise token, DEIP token and Research token [100,101]. Expertise tokens are non-fungible reputation tokens. Expertise tokens are utilized in governance voting. DEIP is DPoS where the decision about the

¹³ <https://medium.com/@deip>

system's 21 active block producers is made using the Expertise token. This said the strength of vote regarding voting about scientific and network matters cannot be bought. This strength of vote can be delegated to anyone when the user doesn't want to participate in the voting mechanisms directly. [100]

When an article is published a reward is distributed after some time (on Steem/Hive the period is set to 7 days - but it can be prolonged). Researchers will receive Expertise tokens (reputation) and DEIP tokens (money) for their effort [101] (assuming the same mechanism used in Steem/Hive is maintained) relative to the amount of the Expertise token voting for the articles. The votes can be positive and negative.

According to one of the articles Research tokens are somehow attributed to individual research projects. According to that article those tokens somehow gain monetary value too: “this is possible due to **Research Tokens** that are attributed to each research project. As the scientific community assesses a project, Research Tokens gain more value to be further sold to attract financing to the project.” [101]

The vagueness of the monetary tokens is a big problem. DEIP stated that its best use case is to improve the funding of scientific research. While they utilize NFT tokens to measure reputation and voting strength of scientists (this thesis came to a conclusion that this is the best way to utilize PoS for science), they completely fail to attribute any utility for their “money” tokens. And that is the most important thing in order to solve the market fit they themselves defined. The DEIP token can be freely substituted for Bitcoin/Dollar - and it would make more sense. On top of that the statement about the Research token value gain is an economical nonsense. Value increases if the demand for the token is bigger than its supply. Someone has to buy the token in order for the gain to be actualized. Just because scientists vote for a project doesn't mean that its token's value is going to increase (if there is no buyer at that price). The project simply failed to attribute any utility to their “money” tokens.

The Github of the project is active. Based on commits statistics the project appears to be developed for a Polkadot blockchain [103]. The project may be released in the future to be further analyzed.

6.1.5 Decentralized Science

I have requested permission to see the beta app in March 2021, which I was not granted. This said I can only rely on two scientific articles explaining the project.

In the first article the blockchain that is supposed to be utilized is not defined [79], but in the second article authors settle with Ethereum because Bitcoin doesn't have smart contracts [80] (which is a wrong statement as explained in this thesis).

As a 2nd layer solution IPFS is proposed [79] (which is indeed needed if the Ethereum network is going to be utilized, since on-chain storage costs would be prohibitively high).

The defined problems are: paywalled and OA costs, outdated peer review process. [79,80]

Solution to the first problem is the Ethereum blockchain itself. By nature of utilizing Ethereum and IPFS the articles would be OA [79]. I would expect more calculations and revealed equations regarding a well known and established blockchain. Not a vague statement that it will be OA by nature.

The second problem is a much more thoroughly analyzed problem. The project rightly identifies that there are numerous options for how peer-reviews could be done on the platform. Cryptography could be utilized to support blind reviews while the reviewers could still be held accountable (reputation-wise) for their reviews [79]. For that a reputation system would need to be in place. Unfortunately neither the first, nor the second paper propose any reputation system [79,80], therefore the problem defined by the platform cannot be solved by the platform yet.

The Github project [104] is not super active, but it isn't dead either. At least one of the authors is still engaged in theoretical scientific articles regarding blockchain [111], therefore we may still see further work on Decentralized Science too.

6.1.6 Frankl

Frankl defines the problem as lack of infrastructure for scholarly reproduction and cooperation [106]. As a solution it proposes to utilize usage of "secure repositories"

(which from my perspective is a very awkward word usage - as the “security” is not inherent but relies on specific calculations) while the metadata is going to be hashed into blockchain and stored in 2nd layer solution - IPFS, Filecoin [106]. IPFS and Filecoin are a viable solution but the data there is not necessarily permanent.

The biggest weakness of the project is its tokenomics. The Frankl token is strictly a payment solution (bad Bitcoin). Every action on the blockchain would have fees associated with it which is the only utility the token has. On top of that the team wants to fully premine 600 000 mil. tokens. 55% of those tokens would be distributed to the buyers through ICO [106]. Which means that 45% of the tokens would stay in the possession of the team. It was explained in the subchapter “Premine” why this is a really bad thing.

It isn't a surprise that the official Github is dead since 2018. [107]

6.1.7 Knowbella

The Knowbella platform tackles several problems. First problem is defined as a “lack of a LinkedIn like platform for scientists”. It then makes a general reference to common scholarly communication problems. [123]

The whitepaper is 38 pages long, yet ultimately vague. The project is closed sourced and on top of that there are no equations, algorithms, nor technical architectures revealed to back the intended mechanisms. That is not how trust is gained.

Knowbella chose to utilize the Ethereum blockchain. Its decision is backed by quotes such as “Ethereum’s ingenuity and leadership clearly demonstrate that it is a key innovator of the technology’s development. Integrating Ethereum blockchain technology into the Knowbella platform not only enables removal of long-standing barriers to scientific innovation, but it fuels the growth of the Knowbella community with the power of cryptocurrency, and anchors Knowbella Tech firmly in a prime position to realize the promise of the blockchain.” [123] Such an “argumentation” is in direct contradiction to the processes outlined in this thesis.

It needs to be stressed that the Knowbella Github is closed sourced, therefore nothing said in the whitepaper can be validated and trusted [124]. We can therefore conclude that Knowbella is not a decentralized project. It shouldn't even be part of this review, but I decided to demonstrate the bad practices on it.

On top of that tokenomics of their Athrotokens is yet again just a payment solution. But this time, since the code is closed sourced, no one can validate anything about the token. It's the same as if Blizzard argued that their World of Warcraft gold is cryptocurrency. This is exactly how scam looks like.

The only bright idea of the project is to utilize non-fungible tokens as some sort of reputation. The problem is that this non-fungible token is a binary function - one can either have that token, or the contrary. One can only have a single unit of the token. Whoever has the token can vote about scientific matters, such as where the conferences are going to be held, vote about future functions of the platform, voting about proposals/grants etc. [123] The tokenomics of the non-fungible tokens have to be more complex. If it was a binary function then professors would have the same exact strength of vote as bachelors if they acquired that token. On top of that Knowbella platform has no clue how those tokens would be distributed [123].

6.2 Analysis of Launched Blockchain-based Scientific Solutions

6.2.1 ScienceRoot

According to ICOHolder¹⁴, the ICO for ScienceRoot has already been held. It is unknown how many funds have been gathered. Their webpage is dead¹⁵. Their whitepaper has been withdrawn from the internet. The project is dead and cannot be analyzed in any way.

¹⁴ <https://icoholder.com/en/scienceroot-23156>

¹⁵ https://www.scienceroot.com/?utm_source=icoholder

6.2.2 Eureka

Eureka is supposed to be a blockchain solution for the Science Matters journal. The ICO occurred about two years ago [113]. At that time the last Github commit had occurred [114]. The Eureka solution is nowhere to be found.

While the problems are clearly defined - slow publishing model, unaccountable peer reviewing, absence of credit for peer reviewers and editors - the rest of the whitepaper is a complete chaos. It seems that the Eureka team wants to utilize Ethereum just for the ICO smart contract. They state in the whitepaper that: „EUREKA has a SaaS (software as a service) business model in which the technology remains under EUREKA’s ownership while customers pay for software usage. The software services are bundled (freemium) into packages differentiating by value adding functionalities and services. Customers pay either on a monthly, yearly, or multiyearly subscription to use the software and additional services whilst receiving either EUREKA’s publishing services and/or data analytics services...Although, the blockchain-based system aims for decentralisation, a centralised backend provides a convenience layer to access the blockchain.“[115]

It is unclear how exactly the blockchain is going to be utilized. In order to understand that a more in-depth technical whitepaper would need to be investigated. The original whitepaper does contain the link to the technical whitepaper, but the access is restricted. [115]

The official Eureka website does not support English language and contains articles of a very low quality. [116]

On top of that the tokenomic of the Eureka token is extremely underdeveloped. EKA is almost only a payment solution. The utility of the token is that the holders will receive 1% cut from every transaction that occurs on the blockchain. Apart from that the EKA token is again just a “bad Bitcoin”. In addition to that EKA runs on a 15% premine. [115] The project is an obvious scam.

6.2.3 Stemsocial

Stemsocial is the actual manifestation of the PEvO project. While it is a different project created by a different team, it is greatly based on the original PEvO idea. The project was born on the original Steem blockchain. Its original name was “Steemstem”. Since the Chinese occupation and migration of the Steem community to the Hive fork, the project was rebranded to Stemsocial.

In reality Stemsocial isn't actually a scientific journal. It utilizes the Hive blockchain to store mainly popular articles. Stemsocial rules incentivize the authors to correctly cite the sources and structure the texts. Those published articles are then rated by Hive community and Stemsocial reviewers and can attract financial rewards somewhere between 2-50 dollars. When the article is positively rated by the Stemsocial reviewers it gets published on the official Stemsocial website where only the popular articles that have met the “scientific requirements” are handpicked from the whole Hive blockchain.

Stemsocial will probably serve as a free OA repository where scientists could publish their articles before/after they get published by a scientific journal in order to receive some additional funds for their effort. It is unlikely that Stemsocial would become a platform where serious peer reviews would take place.

Unfortunately the official website [117] remains broken for several months now which greatly hinders the ability to calculate the amount of accepted articles by the Stemsocial reviewers.

6.2.4 Orvium

The scholarly problem is quite simply defined as “centralized journals” by Orvium. As a solution they offer a blockchain based platform that supports creation of multiple journals. Orvium is one of the few actually functioning blockchain scholarly implementations that can be fully analyzed.

The team utilizes Ethereum blockchain for that purpose. Unfortunately the project does not rely on any 2nd layer storage solution. In the case of Ethereum that may

prove to be a problem due to the high costs of appending files on-chain, even more so as Orvium wants to support appending of research data too. Orvium is trying to disrupt science as a whole but unfortunately provides minimal technical data [118]. On the other hand it provides some very interesting thoughts. The only supported 2nd layer solution is ORCID [118].

As of now (22.7.2021) there are 63 articles published via Orvium, mainly tackling Biology and blockchain domain. Most of the articles were published between 2019-2021 and outside of the singular journal that was set up on the platform. There are also some very old articles dating back to 2008 that were subsequently republished on Orvium.

The main goal of Orvium is to provide a framework for DAJs. It greatly accents individual freedom. It provides a whole plateau of choices both for authors and institutions regarding copyright. Every created DAJs is free to choose its OA policy and its fees (excluding ETH transaction fees that need to be covered). Orvium also supports instant Arxiv-like publishing. [118]

Although there are some problems too. Orvium is supposed to serve as a DAJ framework, but so far there is only one inactive DAJ created on the platform. The DAJ is supposed to have an individual decentralized governance, but that cannot be observed on the one DAJ. It only contains some sort of publishing rules. The project relies heavily on reputation, but just like all the other scholarly decentralized projects it lacks anything resembling reputation calculation. Anyone can review articles and the reviews are either of a really low quality or aren't submitted at all.

Regarding tokenomics the project also presents interesting ideas backed by bad actual implementation. Yet again the project proposes a token that is used solely as a payment solution. Those tokens can be locked in an escrow in each article. Those funds are then released to peer reviewers if they provide a review of a high quality. Interestingly enough even third parties can lock ORV tokens in those escrows if they want to support further reviewing. The voluntarily set up fees for articles are also paid in ERV. Users can also create challenges for scientists and lock ORV in them (similarly to the articles). Users can thus incentivize scientists to do research in

certain areas. The token lacks any real non-financial utility though. Bitcoin should have been used instead and the whole idea would make much more sense.

Github hasn't been active for more than a year which is a big problem, since the project still doesn't have all the proclaimed functionalities. [119]

6.2.5 Scientific Coin

Scientific coin deems the current funding system in science as flawed. It's trying to solve the problem by evaluation of scientific projects and enabling their crowdsourcing.

Their blockchain of choice is Ethereum (for the purpose of ICO smart contract creation), but they intend to make a transition into a blockchain of their own.

According to their Github only the ETH smart contract has been developed so far [120]. Their platform is online, but it is doubtful that it utilizes blockchain in any way, nor can the opposite be validated through Github. The Scientific coin whitepaper proclaims that the evaluation will be done both by superb AI and users themselves and will be decentralized [121]. There are no AI algorithms revealed, the github is basically closed sourced (apart from the smart contract) and on the site itself users themselves don't appear to have any voting strength that can be validated. Such an evaluation can hardly be described as decentralized.

According to the whitepaper the platform can be used only if the account has some Scientific coins staked which can be perceived as a minor utility of the token. On top of that "users" would receive 5% of all the raised funds of all the projects [121]. Such a utility though by no means justifies a statement that 1SNcoin would cost 1,5 USD at the time of release [122]. In addition to that no clear token emission model exists [121]. This is exactly how the economy and formation of prices doesn't work. This project is likely a scam.

6.2.6 Delphus

Delphus is a scholarly project that aims to provide a solution to certain research data storage and its sharing. It is an exception that doesn't tackle scholarly journals which I chose to incorporate in the research due to its well structured tokenomics.

Delphus tries to utilize IPFS to store the research data from questionnaires and associated consents of the participants. It tries to utilize Ethereum blockchain to hash the IPFS location and to create questionnaire bounties that can be filled by participants. The whole platform as of yet runs on Kovan Ethereum testnet. [125]

Delphus manages to create a good tokenomics model. It utilizes native ETH tokens where possible as the payment solution. To avoid volatility, the questionnaire bounties have stable coins locked in its escrow instead of ETH. Such a solution ensures that the scholarly community wouldn't be overpaying questionnaire participants in case of sudden increase in value of ETH token. [125]

The project is simple, yet effective. Unfortunately neither the website, nor the Github [126] are no longer active and the potential release on mainnet is questionable.

6.2.7 Scholar Chain

Scholar chain has no documentation. The only source available is their website. That website contains exactly two pieces of information. Scholar chain looks like a centralized solution with transparent rules and cheap APC. The website says that the project utilizes blockchain to store IPFS hashes and has a better blockchain solution than the competition. Yet not even the basic information is disclosed, such as which blockchain is being used. [108]

The Github is empty and dead [109]. This project doesn't deserve any further investigation and greatly resembles predatory journals.

6.2.8 Moringa Science Publishing

Moringa science publishing is a centralized journal that backs up its data using IPFS and Dogecoin blockchain. It seems like only three articles have been backed that way. [107]

Dogecoin is a well-known crypto meme. If a project unironically uses a meme blockchain they better provide an explanation - which is not the case. Nevertheless this thesis tackles decentralized solutions. Centralized journals using decentralized storage do not fall into that category.

6.2.9 Bloxberg

Bloxberg is a permissioned blockchain and is being mentioned here due to its exceptionally well structured governance model [127]. Bloxberg has managed to avoid any vagueness regarding its governance model. This example should be followed across all relevant parts (governance, tokenomics, blockchain selection etc.) by all the projects. However as the project is centralized it isn't really in the scope of this thesis to analyze its tokenomics as the incentives in centralized systems are different.

6.2.10 The Journal of Raw Data

The Journal of Raw Data is yet again a centralized solution that utilizes blockchain Arweave to store research data. By calling itself "journal" it promises that scientists can climb the scholarly ranks by publishing their research data in it. [128]

At the end though The Journal of Raw Data is still a centralized solution that utilizes blockchain but at the same time stores the very same data on their servers as well. I wasn't able to uncover any data stored in the journal even when the search was done in tandem with my instructor. The project may be well thought out but cannot be validated and yet again is not in the scope of this thesis.

7 Discussion and Conclusion

Scholarly communication with its instrumental features was explained, its history was briefly outlined. Blockchain technology was introduced. It was demonstrated why and how scholarly communities could utilize blockchain technology in order to increase their efficiency and decrease their costs. It was explained how blockchain should be utilized. A set of minimal viability criteria was formulated which enables the success of blockchain communities. These viability criteria were applied to 17 scholarly communication projects most of which did not pass.

While projects were mostly able to define an existing scientific problem and construct its theoretical solution, they were almost never able to premeditate all the important consequences. Aspects such as tokenomics, governance and reputation were almost exclusively only circumlocuted (or had severe shortcomings). That is one of the main reasons why no successful truly decentralized implementation exists yet. From my perspective, the scholarly community needs to keep on taking the matter into its own hands and concentrate on those topics themselves.

The recommendations so far are the following:

- The aim shouldn't be to earn free money through premine. Vast majority of cryptocurrency projects operate on high premine (where the founders attribute huge amounts of the newly created cryptocurrency to their own pockets/wallets), yet they fail to solve problems or create new functionalities. They code a new blockchain because thus they can attribute the new (worthless) cryptocurrency into their own pockets. They cannot do so with established and provably secure cryptocurrencies such as Bitcoin - that's why they don't utilize it. The aim shouldn't be to try to come up with new worthless tokens. When it comes to money and on-chain transactions, Bitcoin should be utilized where possible.
- Stablecoins should be utilized where needed.
- In order to block the possibility of reputation buying, non-tradable, non-fungible tokens should be utilized to measure the reputation.

- The data stored in PoS blockchains should be backed directly on Bitcoin to ensure immutability, possibly via projects such as Veriblock or Komodo.
- Most importantly tokenomics, governance and reputation model has to be created first. Then we can concentrate on the creation of an actual implementation and choose a suitable blockchain. It doesn't work the other way around which was indirectly indicated by my analysis.

Scholarly communication hasn't changed for such a long time that the community can take a few more years to cooperate, analyze and prepare working solutions.

Most projects chose Ethereum for no evidence-based reasons. Ethereum deserves no favouring over other similar blockchains such as Polkadot, Cardano etc. since Ethereum will soon implement EIP 1559 protocol and will subsequently make a transition to PoS from PoW its Lindy effect will effectively reset to 0 just like the rest of its competition with the notable exception of Bitcoin. If Bitcoin is not utilized directly, the blockchain of choice has to be analysed more thoroughly too. More calculations regarding finances have to be undertaken in order for a more complex comparison between current journals and decentralized solutions.

Bloxberg is clearly the most in-depth concept created up to date (governance-wise). Despite the fact that permissioned solutions such as Bloxberg aren't truly decentralized, they deserve more attention regarding their individual aspects. If anyone wants to implement the scholarly framework presented in this thesis in a permissioned manner and utilize Bitcoin instead of Ethereum, Liquid from Blockstream is a perfect candidate.

It's important to note that permissioned blockchains are most of the time externally funded by subsidies from state governments, agencies or institutions. In that case they do not need sustainable tokenomics, or they don't need tokens at all.

Tokenomics, decentralized governance and reputation models are key aspects for creation of decentralized communities utilizing blockchain technology. Yet decentralized governance and reputation models were not specified among the analyzed projects at all. While tokenomics was described it had serious

shortcomings among most of the projects. Only after these three aspects are specified suitable blockchain implementation can be selected. I personally would like to concentrate on these problems throughout my PhD studies and future scientific engagement.

8 References

1. HARNAD, Stevan. POST-GUTENBERG GALAXY: THE FOURTH REVOLUTION IN THE MEANS OF PRODUCTION OF KNOWLEDGE. *Public-Access Computer Systems Review* 2. 1991, 39-53. Accessible from: <http://cogprints.org/1580/1/harnad91.postgutenberg.html>
2. Harnad, Stevan. 1995. "Post-Gutenberg Galaxy: How To Get There From Here". *Times Higher Education Supplement*. Accessible from: <https://eprints.soton.ac.uk/253349/1/thes.html>
3. Potts, Jason, John Hartley, Lucy Montgomery, Cameron Neylon, and Ellie Rennie. 2017. "A Journal Is A Club: A New Economic Model For Scholarly Publishing". Online. *Prometheus* 35 (1): 75-92. <https://doi.org/10.1080/08109028.2017.1386949>.
4. Anup, Kumar. 2015. *Scholarly Communication*. Paris: United Nations Educational, Scientific and Cultural Organization. <https://unesdoc.unesco.org/ark:/48223/pf0000231938/PDF/231938eng.pdf.multiple>
5. Stojmenova Duh, Emilija, Andrej Duh, Uroš Droftina, Tim Kos, Urban Duh, Tanja Simonič Korošak, and Dean Korošak. 2019. "Publish-And-Flourish: Using blockchain Platform To Enable Cooperative Scholarly Communication". Online. *Publications* 7 (2). <https://doi.org/10.3390/publications7020033>.
6. New Data on Journal Prices in Economics [online]. 2004 <http://www.econ.ucsb.edu/~tedb/Journals/2004EconJournalsAllInfo.xls>
7. Hill, Steven A. 2018. "Decoupling The Academic Book". Online. *Learned Publishing* 31: 323-327. <https://doi.org/10.1002/leap.1201>.
8. Casati, F., Giunchiglia, F., Marchese, M. "Liquid Publications: Scientific Publications meet the Web". Technical Report 1313, University of Trento (2007)
9. Lamanna, Camillo, and Manfredi La Manna. 2019. "The Fundamental Problem Blocking Open Access And How To Overcome It: The Bitviews Project". Online. *Insights The Uksg Journal* 32 (November). <https://doi.org/10.1629/uksg.488>.
10. Bergstrom, Theodore C., Paul N. Courant, R. Preston McAfee, and Michael A. Williams. 2014. "Evaluating Big Deal Journal Bundles". Online. *Proceedings Of The National Academy Of Sciences* 111 (26): 9425-9430. <https://doi.org/10.1073/pnas.1403006111>.

11. Kim, Sang-Jun, and Kay Sook Park. 2020. "Market Share Of The Largest Publishers In Journal Citation Reports Based On Journal Price And Article Processing Charge". Online. *Science Editing* 7 (2): 149-155.
<https://doi.org/10.6087/kcse.210>.
12. Rothbard, Murray N. 1984. Monopoly And Competition. University lecture.
13. "United States Consumer Price Index". Online. Trading Economics.
<https://tradingeconomics.com/united-states/consumer-price-index-cpi>.
14. Gadd, Elizabeth, and Denise Troll Covey. 2019. "What Does 'Green' Open Access Mean? Tracking Twelve Years Of Changes To Journal Publisher Self-Archiving Policies". Online. *Journal Of Librarianship And Information Science* 51 (1): 106-122. <https://doi.org/10.1177/0961000616657406>.
15. Piwowar, Heather, Jason Priem, Vincent Larivière, Juan Pablo Alperin, Lisa Matthias, Bree Norlander, Ashley Farley, Jevin West, and Stefanie Haustein. 2018. "The State Of Oa: A Large-Scale Analysis Of The Prevalence And Impact Of Open Access Articles". Online. *Peerj* 6.
<https://doi.org/10.7717/peerj.4375>.
16. Mittermaier, Bernhard. "Double Dipping In Hybrid Open Access – Chimera Or Reality?". Online. *Scienceopen Research*. <https://doi.org/10.14293/S2199-1006.1.SOR-SOCSCI.AOWNTU.v1>.
17. Gajović, Srećko. 2017. "Diamond Open Access In The Quest For Interdisciplinarity And Excellence". Online. *Croatian Medical Journal* 58 (4): 261-262. <https://doi.org/10.3325/cmj.2017.58.261>.
18. Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-To-Peer Electronic Cash System".
<https://bitcoin.org/bitcoin.pdf>.
19. Leible, Stephan, Steffen Schlager, Moritz Schubotz, and Bela Gipp. 2019. "A Review On blockchain Technology And blockchain Projects Fostering Open Science". Online. *Frontiers In blockchain* 2 (November).
<https://doi.org/10.3389/fbloc.2019.00016>.
20. Laurie, Ben, and Richard Cleyton. 2004. "'Proof-Of-Work Proves Not To Work". Accessible from: <https://www.cl.cam.ac.uk/~rnc1/proofwork.pdf>
21. Wheeler, John Archibald. 1989. "Information, Physics, Quantum: The Search For Links". Accessible from: <https://philpapers.org/archive/WHEIPQ.pdf>
22. Held, Dan. 2018. "Pow Is Efficient". *Medium*. Accessible from:
<https://danheld.medium.com/pow-is-efficient-aa3d442754d3>
23. Hayek, Friedrich A. 1945. "The Use Of Knowledge In Society". *The American Economic Review*. Accessible from:
<https://www.econlib.org/library/Essays/hykKnw.html>
24. "Bitcoin Energy Consumption Index". 2021. *Digiconomist*. Accessible from:
https://digiconomist.net/bitcoin-energy-consumption?fbclid=IwAR0fLAI2wflsNg3dHqokXQEipsqeQekQh_r5mMXH6aeRwottcANRQcqmfdo (Accessed 2020-03-07)
25. Domingo, Carlos. 2017. "The Bitcoin vs Visa Electricity Consumption Fallacy". *Hackernoon*. Accessible from: <https://hackernoon.com/the-bitcoin-vs-visa-electricity-consumption-fallacy-8cf194987a50>

26. S. Bartling, blockchain for Open Science and Knowledge Creation, Technical Report, blockchain for Science. Accessible from:
https://docs.google.com/document/d/1Uhjb4K69I0bSx7UXYUStV_rjuPC7VGo0ERa-7xEsr58/edit
27. Urza, and Slush. 2020. *Studio Svobodného Přístavu: O Kryptoměnách Se Slushem*. Youtube: Kanál Svobodného přístavu. Accessible from:
https://www.youtube.com/watch?v=QU6KEe8sU54&list=PLmwDL0IIJTxC9KltdmCmJFA3v49C8XBpN&index=82&ab_channel=Kan%C3%A1Svobodn%C3%A9hop%C5%99%C3%ADstavu
28. de Vries, Alex. 2019. "Renewable Energy Will Not Solve Bitcoin's Sustainability Problem". Online. *Joule* 3 (4): 893-898.
<https://doi.org/10.1016/j.joule.2019.02.007>.
29. Redman, Jamie. 2020. "45 Older-Generation Bitcoin Miners Are Unprofitable After The Reward Halving". *Bitcoin.com*. Accessible from:
<https://news.bitcoin.com/45-older-generation-bitcoin-miners-are-unprofitable-after-the-reward-halving/>
30. *ElectricChoice*. 2021. Accessible from:
<https://www.electricchoice.com/electricity-prices-by-state/>
31. *Porovnej24*. 2020. Accessible from: <https://www.porovnej24.cz/clanky/cena-elektřiny-za-1-kwh>
32. Miners profitability. 2021. Accessible from: <https://www.asicminervalue.com/>
33. Total Hash rate (TH/s). 2021 Accessible from:
<https://www.blockchain.com/charts/hash-rate>
34. Bloomberg research. 2018. Accessible from:
<https://research.bloomberg.com/pub/res/d3bgbon7nESTWTzC1U9PNCxDVfQ>
35. The Bitcoin Mining Network: Trends, Marginal Creation Costs, Electricity Consumption and Sources. *Coinshares*. 2018. Accessible from:
<https://coinshares.com/research/bitcoin-mining-network-november-2018>
36. Twitter discussion. 2020. Accessible from:
https://twitter.com/C_Bendiksen/status/1263539879935442944
37. Stroukal, Dominik. 2020. "Three Myths about Bitcoins Energy Consumption". *Medium*. Accessible from: <https://blog.trezor.io/three-myths-about-bitcoins-energy-consumption-ef613a1f3d5>
38. Drummond, Caitlin, and Baruch Fischhoff. 2017. "Individuals With Greater Science Literacy And Education Have More Polarized Beliefs On Controversial Science Topics". Online. *Proceedings Of The National Academy Of Sciences* 114 (36): 9587-9592. <https://doi.org/10.1073/pnas.1704882114>.
39. Stroukal, Dominik, and Jan Skalický. 2018. *Bitcoin A Jiné Kryptopeníze Budoucnosti: Historie, Ekonomie A Technologie Kryptoměn, Stručná Příručka Pro Úplné Začátečníky*. 2., rozšířené vydání. Finance Pro Každého. Praha: Grada Publishing.
40. Menger, Carl. 1871. *Principles Of Economics*. Austria: Braumüller.
41. Thomas, Wim, and Martin Haigh. 2017. "Shell world energy model: a view to 2100". Accessible from: <https://www.shell.com/energy-and-innovation/the->

- energy-future/scenarios/shell-scenarios-energy-models/world-energy-model/_jcr_content/par/textimage.stream/1510344160326/2ee82a9c68cd84e572c9db09cc43d7ec3e3fafa7/shell-world-energy-model.pdf
42. Alexander, Scott. 2021. "Trapped Prior As A Basic Problem Of Rationality". *Astral Codex Ten*. Accessible from: https://astralcodexten.substack.com/p/trapped-priors-as-a-basic-problem?r=f8y91&utm_campaign=post&utm_medium=web&utm_source=facebook&fbclid=IwAR2dOg6ZhzJ5zqaMysbkiAvZNQRumTyxm8HLXzt8EXorF_u-Vn1gXruW6Bk
 43. Ivánek, Jiří. 2007. "Vybrané kapitoly z kódování informací". Accessible from: https://sites.ff.cuni.cz/uisk/wp-content/uploads/sites/62/2016/01/Vybran%c3%a9-kapitoly-z-k%c3%b3dov%c3%a1n%c3%ad-informac%c3%ad_iv%c3%a1nek.pdf
 44. Minutephysics. 2019. "How Quantum Computers Break encryption: Shor's Algorithm Explained". Youtube. Accessible from: https://www.youtube.com/watch?v=lvTqbM5Dq4Q&ab_channel=minutephysics
 45. "Git: About". Accessible from: <https://git-scm.com/about/branching-and-merging>
 46. Konashevych, Oleksii. 2019. "Why 'Permissioned' and 'Private' are not blockchains". *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3496468>.
 47. Wang, Wenbo, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. 2019. "A Survey on Consensus Mechanisms and Mining Strategy Management in blockchain Networks". *IEEE Access* 7: 22328-22370. <https://doi.org/10.1109/ACCESS.2019.2896108>.
 48. Wright, Craig. 2018. "A Proof of Turing completeness in Bitcoin Script". *Medium*. Accessible from: https://medium.com/@craig_10243/a-proof-of-turing-completeness-in-bitcoin-script-3cf5aa7aeb83
 49. Singh, Niharika. 2019. "Turing Completeness and the Ethereum blockchain". *Hackernoon*. Accessible from: <https://hackernoon.com/turing-completeness-and-the-ethereum-blockchain-c5a93b865c1a>
 50. Collective Work. "Meltdown: Security vulnerability". *Wikipedia*. Accessible from: [https://en.m.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)?fbclid=IwAR0JsRsjmyH54Zjw_06hc8olOz9GXTLy6Rai0-RSDUVPdW3IE9RilkXVvGc#Affected_hardware](https://en.m.wikipedia.org/wiki/Meltdown_(security_vulnerability)?fbclid=IwAR0JsRsjmyH54Zjw_06hc8olOz9GXTLy6Rai0-RSDUVPdW3IE9RilkXVvGc#Affected_hardware)
 51. Decentralized Systems Lab. 2019. "'Fake Stake' attacks on chain-based Proof-of-Stake cryptocurrencies". *Medium*. Accessible from: https://medium.com/@dsl_uiuc/fake-stake-attacks-on-chain-based-proof-of-stake-cryptocurrencies-b8b05723f806
 52. Song, Jimmy. 2018. "The Truth about Smart Contracts". *Medium*. Accessible from: <https://jimmysong.medium.com/the-truth-about-smart-contracts-ae825271811f>

53. Unknown. 2020. "A Comprehensive List of Cryptocurrency Exchange Hacks". *Selfkey*. Accessible from: <https://selfkey.org/list-of-cryptocurrency-exchange-hacks/>
54. VALENZUELA, JOËL. 2020. "The Steem Takeover and the Coming Proof-of-Stake Crisis". *Cointelegraph*. Accessible from: <https://cointelegraph.com/news/the-steem-takeover-and-the-coming-proof-of-stake-crisis>
55. Yoon, Han. 2019. "[UPDATE #2] PIVX and 200+ PoS Chains Currently Vulnerable; Chains Already Under Attack". *Hackernoon*. Accessible from: <https://hackernoon.com/pivx-and-all-pivx-forks-vulnerable-in-a-pos-exploit-several-chains-already-under-attack-vx13xf3vqy>
56. Deirmentzoglou, Evangelos, Georgios Papakyriakopoulos, and Constantinos Patsakis. 2019. "A Survey on Long-Range Attacks for Proof of Stake Protocols". *IEEE Access* 7: 28712-28725. <https://doi.org/10.1109/ACCESS.2019.2901858>.
57. Lee, Suhyeon, and Seungjoo Kim. 2019. "Short Selling Attack: A Self-Destructive But Profitable 51% Attack On PoS blockchains". Accessible from: <https://eprint.iacr.org/2020/019.pdf>
58. Nesbitt, Mark. 2019. "Deep Chain Reorganization Detected on Ethereum Classic (ETC)". *The Coinbase Blog*. Accessible from: <https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de>
59. Collective work. 2020. "Hive: Whitepaper". Accessible from: <https://hive.io/whitepaper.pdf>
60. Garg, Deepika. 2020. "People's Hive vs Justin Sun's Steem: Decentralization Wins!". *AltcoinBuzz*. Accessible from: <https://www.altcoinbuzz.io/cryptocurrency-news/spotlight/peoples-hive-vs-justin-suns-steem-decentralization-wins/>
61. Firmo Network. 2018. "3 Famous Smart Contract Hacks You Should Know". *Medium*. Accessible from: <https://medium.com/firmonetwork/3-famous-smart-contract-hacks-you-should-know-dffa6b934750>
62. Adams, Hayden, Noah Zinsmeister, and Dan Robinson. 2020. "Uniswap v2 Core". Accessible from: <https://uniswap.org/whitepaper.pdf>
63. Tarasov, Anton. 2020. "Millions Lost: The Top 19 DeFi Cryptocurrency Hacks of 2020". *Crypto Briefing*. Accessible from: <https://cryptobriefing.com/50-million-lost-the-top-19-defi-cryptocurrency-hacks-2020/>
64. "IEEE Transactions on Cybernetics". 2021. *SJR*. Accessible from: <https://www.scimagojr.com/journalsearch.php?q=21100274221&tip=sid&clean=0>
65. "IEEE Transactions on Cybernetics". 2021. *JCR*.
66. "IEEE Publication Services and Products Board Operations Manual". 2020. Accessible from: <https://pspb.ieee.org/images/files/files/opsmanual.pdf>
67. "eLife". 2021. *JCR*.

68. Eisen, Michael B, Anna Akhmanova, Timothy E Behrens, Diane M Harper, Detlef Weigel, and Mone Zaidi. 2020. "Implementing a "publish, then review" model of publishing". *ELife* 9 (December). <https://doi.org/10.7554/eLife.64910>.
69. eLife. 2021. "Publication Fees". Accessible from: https://submit.elifesciences.org/html/elifesciences_author_instructions.html#fees
70. "Open Journal System" Accessible from: <https://pkp.sfu.ca/ojs/>
71. "PKP Index" Accessible from: <http://index.pkp.sfu.ca/>
72. "Sociobiology". 2021. JCR.
73. "Acta Polytechnica". 2021. SJR. Accessible from: <https://www.scimagojr.com/journalsearch.php?q=21100200605&tip=sid&clean=0>
74. "Sustainers". 2021. PKP. Accessible from: <https://pkp.sfu.ca/sustainers/>
75. Šámal, Petr. 2009. *Soustružníci lidských duší: lidové knihovny a jejich cenzura na počátku padesátých let 20. století : (s edicí seznamů zakázaných knih)*. Šťastné zítřky (Academia). Praha: Academia.
76. Mandelbrot, B. Benoit. 1983. *Fractal geometry of nature*. Vyd. 3. New York: Freeman and company.
77. Hussey, Matt. 2019. "What is Tokenomics?". *Decrypt*. Accessible from: <https://decrypt.co/resources/tokenomics>
78. Lo, Yuen C., and Francesca Medda. 2020. "Assets on the blockchain: An empirical study of Tokenomics". *Information Economics and Policy* 53. <https://doi.org/10.1016/j.infoecopol.2020.100881>.
79. Tenorio-Fornés, Antonio, Viktor Jacynycz, David Llop, Antonio A. Sánchez-Ruiz, and Samer Hassan. 2018. "A Decentralized Publication System for Open Science using blockchain and IPFS". *PEERE International Conference on Peer Review Proceedings*. Accessible from: <https://decentralized.science/wp-content/uploads/peere2018.pdf>
80. Tenorio-Fornés, Antonio, Viktor Jacynycz, David Llop, Antonio A. Sánchez-Ruiz, and Samer Hassan. 2019. "Towards a Decentralized Process for Scientific Publication and Peer Review using blockchain and IPFS". *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Accessible from: <https://scholarspace.manoa.hawaii.edu/bitstream/10125/59901/1/0461.pdf>
81. "Open Science Network: The Future of Scientific Research". 2018. Accessible from: https://docs.google.com/document/d/1_PqjT8eASvIOmJmB1JiSyiTOoK7QuRgeJTOtFRIHaww/edit
82. Wolf, Michael, Marlies Wiegand, and Alexander Drichel. 2016. "PEvO: Decentralized Open Access and Evaluation". Accessible from: https://pevo.science/files/pevo_whitepaper.pdf
83. Zhang, Yanxia, and Yongheng Zhao. 2015. "Astronomy in the Big Data Era". *Data Science Journal* 14 (May). <https://doi.org/10.5334/dsj-2015-011>.
84. "Ethereum Whitepaper". 2013-2021. Accessible from: <https://ethereum.org/en/whitepaper/#fees>

85. Bedeian, Arthur G., David D. Van Fleet, and Hugh H. Hyman. 2009. "Scientific Achievement and Editorial Board Membership". *Organizational Research Methods* 12 (2): 211-238. <https://doi.org/10.1177/1094428107309312>.
86. Kay, Jeffrey, Muzammil Memon, Darren de SA, Nicole Simunovic, Andrew Duong, Jon Karlsson, and Olufemi Rolland Ayeni. 2017. "The h-Index of Editorial Board Members Correlates Positively With the Impact Factor of Sports Medicine Journals". *Orthopaedic Journal of Sports Medicine* 5 (3). <https://doi.org/10.1177/2325967117694024>.
87. Pagel, P.S., and J.A. Hudetz. 2011. "Bibliometric analysis of anaesthesia journal editorial board members: correlation between journal impact factor and the median h -index of its board members". *British Journal of Anaesthesia* 107 (3): 357-361. <https://doi.org/10.1093/bja/aer191>.
88. Asnafi, Solmaz, Tina Gunderson, Robert J. McDonald, and David F. Kallmes. 2017. "Association of h-index of Editorial Board Members and Impact Factor among Radiology Journals". *Academic Radiology* 24 (2): 119-123. <https://doi.org/10.1016/j.acra.2016.11.005>.
89. Burgess, Thomas F., and Nicola E. Shaw. 2010. "Editorial Board Membership of Management and Business Journals: A Social Network Analysis Study of the Financial Times 40". *British Journal of Management* 21 (3): 627-648. <https://doi.org/10.1111/j.1467-8551.2010.00701.x>.
90. Burniske, Chris, and Jack Tatar. 2017. *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond*.
91. Rozas, David, Antonio Tenorio-Fornés, Silvia Díaz-Molina, and Samer Hassan. 2021. "When Ostrom Meets blockchain: Exploring the Potentials of blockchain for Commons Governance". *SAGE Open* 11 (1). <https://doi.org/10.1177/21582440211002526>.
92. Liu, Yulin. 2019. "Cryptocurrency Valuation". *Medium*. Accessible from: <https://medium.com/coinmonks/cryptocurrency-valuation-d9979074404>
93. Storj Labs, Inc. 2018. "Storj: A Decentralized Cloud Storage Network Framework". Accessible from: <https://www.storj.io/storjv3.pdf>
94. Saifi, Azeem. 2019. "blockchain Without Tokens: is it a myth?". *Crypto-news*. Accessible from: <https://www.crypto-news.net/blockchain-without-tokens-is-it-a-myth/>
95. "IPFS Incentives?". 2018. *IPFS*. Accessible from: <https://discuss.ipfs.io/t/ipfs-incentives/24567>
96. <https://scite.ai/>
97. Úřad vlády České republiky. 2017. "Metodika hodnocení výzkumných organizací a hodnocení programů účelové podpory výzkumu, vývoje a inovací". Accessible from: <https://www.vyzkum.cz/FrontClanek.aspx?idsekce=799796>
98. Úřad vlády České republiky. 2017. "DEFINICE DRUHŮ VÝSLEDKŮ: Metodiky hodnocení výzkumných organizací a programů účelové podpory výzkumu, vývoje a inovací". Accessible from: <https://www.vyzkum.cz/FrontClanek.aspx?idsekce=799796>

99. "Open Science Network: OSN Tokenomics". 2018. Accessible from: https://docs.google.com/document/d/1RfnjcGVhcyjLdD9WHM_bErETvilj_lid6GBLr6inucB0/edit
100. DEIP. 2018. "DEIP — blockchain for scientific research launched public beta". *Medium*. Accessible from: <https://medium.com/@deip/deip-first-blockchain-for-science-to-launch-public-testnet-9506ae19dd4a>
101. Shkor, Alex. 2018. "How to enable self-governance in decentralized science". *Medium*. Accessible from: <https://medium.com/deip/delegated-proof-of-expertise-contribution-c6352241ff57>
102. Ruseckiy, Artyom. 2019. "The public beta of the DEIP blockchain platform". *Medium*. Accessible from: <https://medium.com/deip/the-public-beta-of-the-deip-blockchain-platform-fa9388d7b8ea>
103. DEIP. "Github". Accessible from: <https://github.com/DEIPworld>
104. Decentralized Science. "Github". Accessible from: <https://github.com/DecentralizedScience>
105. "Frankl: An Open Science Platform". 2018. Accessible from: <https://docsend.com/view/gn8t7k9>
106. Frankl. 2018. "Github". Accessible from: <https://github.com/FranklOpenScience>
107. "Moringa Science Publishing Publication Database". Accessible from: <https://pubreg.moringa.pub/>
108. "Scholarchain webpage". Accessible from: <https://www.scholarchain.eu/>
109. Web of Open Science. "Github". Accessible from: <https://github.com/Web-of-Open-Science>
110. "Distributed Science Infrastructure Projects". 2020. *Zenodo*. Accessible from: https://zenodo.org/record/3695199#.YHmhrK_7RPY
111. Rozas, David, Antonio Tenorio-Fornés, Silvia Díaz-Molina, and Samer Hassan. 2021. "When Ostrom Meets blockchain: Exploring the Potentials of blockchain for Commons Governance". *SAGE Open* 11 (1). <https://doi.org/10.1177/21582440211002526>.
112. "ScienceRoot". 2018. *ICOHolder*. Accessible from: <https://icoholder.com/en/scienceroot-23156>
113. "Eureka". 2018. *ICOHolder*. Accessible from: <https://icoholder.com/en/eureka-26261>
114. "Eureka-blockchain-solutions". Github. Accessible from: <https://github.com/eureka-blockchain-solutions/tokenapp-frontend>
115. Collective work. "Eureka: A peer-to-peer scientific data publishing platform powered by blockchain, to promote open science". Accessible from: <https://static.icoholder.com/files/26261/3ddb0c5312fd55786aac121ff364fe8e.pdf>
116. eurekatoken.io. Accessible from: https://www.eurekatoken.io/?utm_source=icoholder
117. Stemsocial. Accessible from: <https://stem.openhive.network/>

118. "Orvium: Whitepaper". 2019. Accessible from:
<https://docs.orvium.io/Orvium-WP.pdf>
119. "Orvium". Github. Accessible from: <https://github.com/orvium>
120. "Scientificcoin". Github. Accessible from:
<https://gist.github.com/yuriy77k/e0b122aeb0e5181725d37f83be8e3455>
121. "Scientific Coin: blockchain platform for scientific projects with decentralized evaluation". Accessible from:
<https://scientificcoin.com/Whitepaper.pdf>
122. "Participation Terms and Fee pattern". Accessible from:
<https://scientificcoin.io/account/bonus>
123. "Knowbella: Whitepaper". 2019. Accessible from:
<https://www.knowbella.tech/>
124. "Knowbella". Github. Accessible from: <https://github.com/Knowbella>
125. Scintillating Team. "Delphus: Revolutionizing Clinical Studies and Data Transparency through the Blockchain". Accessible from:
<https://delph.us/whitepaper.pdf>
126. "Delphus". Github. Accessible from: <https://github.com/delphus>
127. "Bloxberg: The Trusted Research Infrastructure". 2020. Accessible from: https://bloxberg.org/wp-content/uploads/2020/02/bloxberg_whitepaper_1.1.pdf
128. "Journal of Raw Data". 2018. Accessible from:
https://thejournalofrawdata.org/JoRD_v100.pdf
129. Benet, Juan. "IPFS: Content Addressed, Versioned, P2P File System (DRAFT 3)." Accessible from:
<https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf>
130. LOCKSS. Accessible from: <https://www.lockss.org/>
131. Bencic, Federico Matteo, and Ivana Podnar Zarko. 2018. "Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph." In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, 1569-1570. IEEE. <https://doi.org/10.1109/ICDCS.2018.00171>.
132. "Technical background of version 1 Bitcoin addresses." 2021. *Bitcoin Wiki*. Accessible from:
https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses
133. "NP (complexity)." 2021. *Wikipedia*. Accessible from:
[https://en.wikipedia.org/wiki/NP_\(complexity\)](https://en.wikipedia.org/wiki/NP_(complexity))
134. Naziridis, Nick. 2018. "Comparing ECDSA vs RSA." *SSL*. Accessible from: <https://www.ssl.com/article/comparing-ecdsa-vs-rsa/>
135. <https://blockstream.com/satellite/>
136. Chohan, Usman W. "The Double Spending Problem and Cryptocurrencies." *SSRN Electronic Journal*.
<https://doi.org/10.2139/ssrn.3090174>.

137. Tětek, Josef. 2020. "Bitcoin: Nestátní peníze: Bitcoin není kryptoměna." *Youtube*. Accessible from: https://www.youtube.com/watch?v=imzUsP9MSJA&ab_channel=Paraleln%C3%ADPolis
138. Tětek, Josef. 2021. "Historie koruny: od zlaťáku k fiat." *Alza*. Accessible from: <https://www.alza.cz/historie-koruny-od-zlataku-k-fiatu>
139. Tětek, Josef. 2020. "Bitcoin: odluka peněz od státu." *Alza*. Accessible from: <https://www.alza.cz/bitcoin-odluka-penez-a-statu>
140. <https://coinmarketcap.com/currencies/bitcoin/>
141. "The ETH2 Vision." 2021. *Ethereum Blog*. Accessible from: <https://ethereum.org/en/eth2/vision/>
142. Liu, Yizhong, Jianwei Liu, Marcos Antonio Vaz Salles, Zongyang Zhang, Tong Li, Bin Hu, Fritz Henglein, and Rongxing Lu. 2021. "Building Blocks of Sharding Blockchain Systems: Concepts, Approaches, and Open Problems." *Arxiv*. Accessible from: <https://arxiv.org/abs/2102.13364>
143. Wood, Gavin. "POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK." Accessible from: <https://polkadot.network/PolkaDotPaper.pdf>
144. "Cardano Roadmap." Accessible from: <https://roadmap.cardano.org/en/>
145. "Why Cardano." Accessible from: <https://why.cardano.org/en/introduction/motivation/>
146. Kiayias, Aggelos, Alexander Russell, Bernardo David, and Roman Oliynykov. 2017. "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol." In *Advances in Cryptology – CRYPTO 2017*, edited by Jonathan Katz and Hovav Shacham, 357-388. Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-63688-7_12.
147. Mongeon, Philippe, Kyle Siler, Antoine Archambault, Cassidy R. Sugimoto, and Vincent Larivière. 2021. "Collection Development in the Era of Big Deals." *College and Research Libraries*. Accessible from: <https://crl.acrl.org/index.php/crl/article/view/24833/32670...ani>
148. Sugimoto, Cassidy R. 2019. "New open-access journal Quantitative Science Studies." *Issi-society*. Accessible from: <https://www.issi-society.org/blog/posts/2019/january/the-international-society-for-scientometrics-and-informetrics-ends-support-for-journal-of-informetrics-launches-new-open-access-journal-quantitative-science-studies/>
- 149.