On the Sustainability of Blockchain Funding

Hamed Balogun
Lancaster University
Lancaster, United Kingdom
h.balogun@lancaster.ac.uk

Bingsheng Zhang
Lancaster University
Lancaster, United Kingdom
b.zhang2@lancaster.ac.uk

***Abstract*—Blockchain technology has pioneered a new consensus approach to building a distributed public ledger globally. A key feature expected from cryptocurrencies and blockchain systems is the absence of a centralized control over the operation process. That is, blockchain solutions should neither rely on "trusted parties or powerful minority" for their operations, nor introduce such centralisation tendencies into blockchain systems.**

On the other hand, real-world blockchain systems require steady funding for continuous development and maintenance of the systems. Given that blockchain systems are decentralized systems, their maintenance and developmental funding should also be void of centralization risks. Therefore, secure and "community-inclusive" long-term sustainability of funding is critical for the health of blockchain platforms.

In this work, for the first time, we provide a systematic exposition of blockchain development funding, planning, management, and disbursement mechanisms aka "treasury systems" (for cryptocurrencies and blockchain systems). Drawing from existing literature, we identify and categorise various treasury models, thereby enabling an exploration of their properties, benefits and drawbacks. Particularly, we perform an evaluation of real-world cryptocurrency treasury system of top cryptocurrencies e.g., Dash governance system, and ZCash Foundation. Finally, we briefly discuss desired properties of decentralised treasury systems and provide suggestions for improvement or alternative solutions to existing systems or implementations.

***Index Terms*—blockchain, sustainability, funding, treasury**

I. Introduction

Blockchain technology has pioneered a new consensus approach to build a distributed public ledger globally. Blockchains have become largely ubiquitous across various sectors, e.g., technology, academia, medicine, economics and finance, etc. Collectively, the net market capitalisation of top cryptocurrencies exceeds 200 billion USD according to CoinMarketCap.

Following the success of Bitcoin, a large number of other cryptocurrencies have emerged in recent years. Despite this increase in the number of cryptocurrencies, secure and "community-inclusive" long-term sustainability of maintenance and developmental funding of cryptocurrencies remains a serious issue for existing cryptocurrencies. Real-world blockchain systems require continuous maintenance, developmental projects and steady funding for continuous growth of the systems.

Ideally, for blockchain systems, maintenance and developmental funding should be decentralised. Given that blockchain systems are distributed/decentralised systems, therefore, its solutions (and by extension sustenance mechanisms) should be void of centralisation risks. That is, blockchain solutions should not rely on "trusted parties or powerful minority" for their operations or introduce such (centralisation) tendencies into blockchain systems. Similarly, solutions on blockchain systems ought to be compatible with core features of blockchain systems, such as tamper-proof, decentralisation, disintermediation, secure, and community-inclusive (open to all), etc.

Our contributions. In the literature, the study of blockchain sustainability mainly focuses on the environmental sustainability and energy consumptions; namely, proof-of-X, where X is some resource, stake, or combination of resources and stake. Whereas, funding sustainability is an issue that has been overlooked by the research community. Despite the increase in the number of cryptocurrencies, secure sustainability of maintenance and developmental funding of cryptocurrencies remains a serious issue. Real-world blockchain platforms require continuous maintenance, developmental projects and steady funding for continuous growth.

Traditionally, blockchain platforms are developed (and funded) by "founders", who are either developers, investors, researchers, etc., and typically they are responsible for driving the direction and growth of the platforms. However, in recent times, an alternative funding and decision making mechanism for blockchain systems is the treasury system [1]. A treasury system is a self-sustenance mechanism for the advancement of blockchain systems [2]. The treasury system is a decentralised, collaborative decision-making mechanism for cryptocurrencies and blockchain systems.

We examine existing development funding and management systems (viz-a-viz treasury systems) found in real-world cryptocurrencies and evaluate them with a view to identifying their strengths and weaknesses and provide suggestions for improvement (towards achieving solutions which are compatible with core blockchain features). Briefly, we remark that at the core of a truly decentralised treasury system are: regular and "secure" source(s) of funds, community-inclusive collaborative decision-making (with facilities to optimise collective intelligence and experience), absence/minimisation of centralisation risks, and (possibly) an enforcement mechanism to ensure compliance with community-wide decisions. It is important to note that a proportional amount of work in this area stem from non-academic venues and sources (due to the ubitquitous nature of cryptocurrencies). Particularly, this

is one area of research where practice seem to be ahead of theory [3]. An important portion of resources for the research comes from official websites of cryptocurrencies or third-party service providers (e.g., Coinmarketcap), official and unofficial chat forums (e.g., Reddit, Medium), mailing lists, Wiki pages, GitHub, etc.

Roadmap. The remainder of this work is divided into sections described as follows: Section II provides a high-level description of treasury systems for cryptocurrencies. In Section III, we discuss various funding sources for blockchain/cryptocurrency maintenance and development. Section IV provides an insightful description and categorisation of the various treasury models found on existing cryptocurrencies and beyond. In Sections V, VI we explore known treasury systems for cryptocurrencies by analysing details of their operations, features, strengths and weaknesses. We examine how these pioneer blockchain platforms address pertinent problems such as decision-making participants and rules, and privacy, fund utilisation, etc. (and their relevance towards developing secure treasury systems for sustainable blockchain technologies). Finally, we conclude the report with a brief summary of key findings and insights, as well as recommendations for improvement and future treasury systems in Section VIII.

II. Treasury System Overview

Simply put, a treasury system is a "self-sustenance" mechanism for blockchain platforms (particularly cryptocurrenies). Treasury on cryptocurrencies encompasses funding source, development, maintenance and advancement of the underlying cryptocurrency [2], as well as decision-making, and long-term sustainability. In blockchain technologies, a treasury system is a decentralised means of achieving and ensuring continued existence and improvement of its parent-system (e.g., cryptocurrency) by providing a regular source of funding for projects relevant to the survival and growth of the system.

These projects include marketing, software development, legal fees, advertising and publicity, etc. Typically, a treasury system covers proposal submissions (and discussions/feedbacks), community-inclusive collaborative decision-making mechanism for reaching decisions on proposals, and a securely reliable and sustainable means of funding for the treasury. Furthermore, treasury parameters and features should be compatible with, and reflect real-life choices and scenarios in which the blockchain community/proposers are expected to function. For example, a potential period for treasury systems is 30 days (one month) expressed in corresponding number of blocks in the blockchain. A justification for such a choice is its practicality and compatibility with the real-world (e.g., slalaries are paid monthly), as well as other benefits (e.g., sufficeintly reasonable time for planning, meetings, discussions, decision-making, etc.) it offers [2]. Additionally, we highlight below, pertinent issues that are essential to treasury system.

First, a *collaborative decision-making mechanism* e.g., a voting scheme. Treasury systems should integrate mechanisms that facilitates community-inclusive collaborative decision-making in order to maximise the collective-intelligence of the cryptocurrency community in particular and blockchain ecosystem at large. In addition to collective-decision making, flexible voting rules, that reflect the peculiarities of the blockchain rather than general voting rules, is important to the utility of treasury systems. For instance, a simple majority voting rule may not suffice for all situations, especially, for high-risk proposals that request huge amounts of funds.

Second, a secure and sustainable *treasury funding mechanism*. In addition to contributions from block rewards (i.e., taxation of miners' rewards), the treasury system should accommodate other funding means such as voluntary donations, or other external funding sources. This option is particularly useful when the tax from block rewards becomes small (as a result of decrease in block rewards) or as a result of money supply limit being reached and only transaction fees make up block rewards.

Third, *thorough stakeholder participation and community-driven* treasury. Game-theoretically efficient *incentive structure / reward mechanism* further drives increased stakeholder participation in treasury process, and also helps ensure that incentives do not lead to hyper-inflation which can diminish cryptocurrency value.

Fourth, *blockchain and stakeholders' security and privacy.* For instance, an adversary who carries out Sybil attacks (by distributing his stake into multiple addresses each with smaller stakes) should gain no advantage by so doing, and the vote of stakeholders should be weighted relative to their stake in the system. Additionally, participation in treasury activity should not compromise the security and privacy of participants.

Finally, other desirable treasury system properties include: treasury refund/recall mechanism, project spending/milestone monitoring scheme, on-chain consensus and history verification for all proposals, etc.

We now discuss the main sources of development funding for cryptocurrencies (or their treasury system).

III. Funding Sources

Funding is a critical tool necessary for the development and maintenance of any real-world cryptocurrency. The major sources of development funding on blockchain systems include Initial Coin Offerings (ICOs), donations (charity), taxations, venture capitalists (investor funding), and patron organisations. Today, cryptocurrencies largely rely on one (or a combination) of the above-listed sources for development funding and maintenance.

A. Initial Coin Offerings (ICOs)

ICO is a means of crowd-funding done by issuing some cryptocoins to investors, or other individuals, in exchange for other cryptocurrencies (usually Bitcoin or Ethereum) or a fiat currency. Typically, most ICOs are deployed as smart contracts that receive funds and distribute equivalent amount of the new or underlying cryptocurrency to the investors at a later date [4]. Technologies such as the ERC20 which facilitate easy development of ICOs have enabled increase in the number of ICOs in the cryptocurrency community. Usually, investors

buy these tokens in expectation that their value may rise if project/company offering the ICO is successful in the future. ICOs represent a good way to raise reasonable amount of money to support cryptocurrency development within a short period of time. For instance, projects such as Basic Attention Token and Aragon [5], [6] were able to respectively raise 35 million USD and 25 million USD in 30 seconds and 15 minutes.

Due to the successes recorded by early ICOs, there have been a rise in number of ICOs for cryptocurrencies and other blockchain-based technologies [7]. According to Cointelegraph, approximately 4 billion USD (fiat currency equivalent) was raised in 2017 alone. While ICOs are good, there are a number of gray issues associated with the legality of ICOs. For example, are ICO-tokens utility tokens or financial security? Unfortunately, some ICOs have been used in Ponzi schemes and financial scams. Moreover, recently there have been an apparent decline in the rate of successful ICOs, perhaps due to an increase in the number of speculative projects carrying out ICOs.

Evidently, ICOs are valuable for initial development or starting out a project due to the amount of funds that can be raised in a short span of time. However, the uncertainties surrounding the amount of funds that can be raised at any given time make them unsuitable for funding treasury. Furthermore, they are incompatible with the methodical planning and reliable funding that is expected of decentralised cryptocurrency treasury systems. In other words, an obvious drawback is that ICOs are not suitable for long-term planning of cryptocurrency maintenance and development. Therefore, ICOs do not represent a sustainable development funding mechanism for cryptocurrencies.

B. Donations

Donations, perhaps, is the oldest and most common means of cryptocurrency development funding. "Developers/founders" of a cryptocurrency rely on donations from charity e.g., from the public, stakeholders, or other third parties, for cryptocurrency development funding. Although, donations represent an alternative funding mechanism to ICOs, they are not without their own pitfalls. For instance, Bitcoin through its foundation- The Bitcoin Foundation (whose goal is to increase global acceptance of Bitcoin) - have developed via reliance on donations and membership registration fees, however, there have been instances where development activities have been threatened because of low availability of funds. For instance, in 2015, Olivier Janssens (who later became a board member of the Foundation) published a note on the Bitcoin Foundation forum where he stated that the Foundation was seriously struggling with funds. Moreover, BitcoinCore, an open source endeavour responsible for the maintenance of the Bitcoin client [8], also runs a sponsorship program - the Bitcoin Core Sponsorship Programme - through which top companies and industry players can contribute to the development of the cryptocurrency.

For the Monero (XMR) cryptocurrency, developers or proposers (planning to execute cryptocurrency development projects) discuss details of their proposals (including the amount of funds needed) on the "getmonero forum" and seek donations from other community members who see value in the proposals and their contribution to the overall growth of the Monero blockchain.

Although, donations are useful for cryptocurrency development funding, solely, they are not suitable for long-term methodical planning and sustainability of cryptocurrencies. Planning is difficult if funding is only available through donations. Meticulous planning for blockchain development activities is impractical under the donations model due to uncertainties about the amount of funds that will be available at any period of time. Furthermore, donations could introduce centralisation in the system. For instance, "popular donors" (not malicious) may take advantage of the model to influence decisions in the system to their favour. In contrast, a malicious adversary or donor may try to influence the system in ways that are detrimental to the sustainability and growth of the system. For instance, this may be done to cripple the system due to the adversary holding a large stake in an altcoin or competitor cryptocurrency.

C. Taxations

Taxation is an alternative development funding source found on existing cryptocurrencies such as Dash, ZenCash, ZCash, etc. By design, a fraction of block rewards (payment for finding new block) is taken and contributed to a decentralised treasury, or the coin company (investors/founders of the cryptocurrency), or some other bodies providing services to the cryptocurrency. For instance, 10% of miners' rewards on the Dash blockchain is contributed to a central pool, from which developers and other community members can request for funds for proposals that will advance the Dash blockchain. For ZCash, 10% of the 21 million ZEC (that will be mined on the network) represents tax (aka "Founders Rewards") that will be distributed among founders, investors, employees, and advisors.

Taxation, perhaps, is the most sustainable of all cryptocurrency development funding sources because it is a blockchain sustenance mechanism derived from activities on the blockchain. Furthermore, it lends itself to methodical planning which is necessary for disintermediation protocols such as cryptocurrencies. Therefore, taxation which is obtainable from miners' rewards (and possibly transaction fees) represent a good treasury fund source. However, additional funding schemes may be required because of the decreasing miners' reward which is a common feature of most cryptocurrencies. Accordingly, a hybrid treasury funding source, such as one that combines taxation with donations or minting (to supplement the shortage from diminishing miners' reward) represents a more robust and sustainable blockchain funding source.

D. Minting

Minting can be described as a process that creates new coins in a cryptocurrency. For example, this is referred to as coinbase

transaction in the Bitcoin blockchain. Basically, this is the means by which proposers of new blocks get rewarded. The miner or node proposing this block gets some new coins for being the first to correctly solve a computational puzzle (proof-of-work) or for being the leader of a committee responsible for proposing a new block (proof-of-stake). Similarly, a related approach can be used for rewarding community members (or cryptocurrency stakeholders) who propose to, and carry out projects that will advance the growth of the blockchain. In other words, members who propose to execute tasks that support cryptocurrency development can be funded by minting only the amount of coins needed and awarding same to them, to enable them carry out the projects.

Although minting provides stable funding for cryptocurrency development, if not well researched and implemented, it is susceptible to abuse by proposers who are only interested in taking funds from the system because of the " seemingly unlimited" availability of funds supply. Clearly, there is need for thorough economic and game-theoretic analysis to determine an optimum amount of coins that should be minted (for funding projects in the system), and the number of proposals that should be funded at any particular time. This analysis is also necessary to determine the overall inflation impact and implications for long-term growth and value of the cryptocurrency.

E. Patron Organisations

Apart from ICOs, taxations and donations, patron organisations also provide services to support blockchain development. For instance, Bitpay contributes to Bitcoin development by funding wages of some Bitcoin Core developers. Furthermore, industrial organisations can also contribute human resources and services to the growth of a cryptocurrency. For instance, in addition to providing funding to Bitcoin Core, BitStream also contribute human resources to the Bitcoin cryptocurrency e.g., developers contributing to Bitcoin Core software. An obvious drawback is that these organisations tend to wield ample influence in decision-making on the development direction of cryptocurrencies they support. Usually, these decisions tend to occur in a centralised manner, and centralised sustenance mechanisms that do not equally represent the interests of all stakeholders are not appropriate for blockchains.

Conclusively, each of the above-listed blockchain development funding sources, individually does not serve as a secure, methodical and decentralised planning, funding source for decentralised blockchain-based cryptocurrencies' treasury system.

Next, we discuss the models of treasury systems for blockchain technologies. Although the proposed ontology for treasury models is motivated by current solutions found in existing cryptocurrencies, the classification also covers possible new treasury systems that could potentially be adopted by other cryptocurrencies.

IV. Treasury Models

A key motivation for classifying treasury system models is to identify similarities, basic properties, strengths and weaknesses of the diverse groups, with a view to determining their applicability to particular blockchain systems. A major overarching attribute used in the classification of treasury systems is the source of development funding for projects, as well as the input and contribution of community members of the cryptocurrency ecosystem (especially, people who hold stake in the system).

Concretely, we identify three main models of treasury systems:

- Open-System Treasury: This class consists of systems where source of blockchain development funding are external to the system, e.g, Donations, Patron organisations, industry, founders' resources, etc. Additionally, participation in treasury activities such as decision-making, proposal submission, proposal review, and project execution, etc., are open to other members of the cryptocurrency, rather than the cryptocurrency founders, developers and company only.
- Closed-System Treasury: Under this category, all fund sources are local to the system, i.e., within/from the cryptocurrency. e.g, minting, taxation, and donations from stakeholders of the cryptocurrency. Typically, decision-making and cryptocurrency development processes are organised in a centralised manner (e.g., by some organisation) void of input from the general cryptocurrency ecosystem.
- Hybrid-System Treasury: This category of treasury systems represents a combination of the features of the closed and open-treasury systems. Under Hybrid-System treasury, cryptocurrency development funding sources comprise funds from within the cryptocurrency, and from sources external to the system.

Following from the identified treasury models, we now discuss sub-classes of treasury systems.

- **Taxation-Community-Controlled (TCC)**
  Taxation is the primary source of project funding on TCC treasury systems. The funds can be obtained by taxing miners' block rewards or block transaction fees or a combination of both. The Dash governance system is a classic example of a treasury system within the TCC class because it relies on taxations of 10% of block rewards for funding treasury (or fund pool).
  Within this class of treasury system, project funding decisions are reached through the use of community-inclusive mechanisms such as voting. In other words, funding decisions are made in a decentralised manner (which prevents excessive centralisation of powers in the hands of a few members). A variety of voting systems and rules can be adopted for decision-making such as liquid democracy, preferential voting, plurality voting, etc.
- **Taxation-Organisation-Controlled (TOC)**
  TOC is very similar to TCC in terms of treasury funding source. However, unlike TCC, decisions on how to use funds within the treasury are made in a centralised manner. Typically, an organisation or group of individuals

(usually company founders or investors) are responsible for making funding decisions, with little or no input from other members of the cryptocurrency ecosystem or cryptocurrency stakeholders.

- **Donation-Community-Controlled (DCC)**
  Under DCC, the major source of cryptocurrency development funding comes from donations. This donation can be obtained from community members, patron or charitable organisations with interest in the development of a particular blockchain. For instance, Bitcoin Core receives donations from individuals and corporate organisations, for carrying out activities that support the continued existence and growth of the Bitcoin cryptocurrency.
  Similar to TCC, usage of funds within this treasury class is decentralised. Funding decisions for proposals are made through the use of community-inclusive mechanisms, thereby supporting collaborative decision making.
- **Donation-Organisation-Controlled (DOC)**
  Within this group of treasury system, funding available for cryptocurrency development are sourced from donations. That is, like DCC, DOC treasury systems are also funded from donations received from charities and corporate bodies or community members. For example, proposers of projects that support the Monero cryptocurrency source for funding from donations made by other community members.
  Unlike DCC, DOC treasury decisions are made similarly to that of TOC, i.e., centralised funding decision-making.
- **Hybrid-Community-Controlled (HCC)**
  As the name suggests, within the HCC class funding source is hybrid. Therefore, HCC treasury systems are funded from a combination of sources such as taxation, minting and donation.
  Similar to other community controlled treasury system, HCC treasury system make use of decentralised decision making mechanisms to reach funding decisions and community members of the cryptocurrency are major participants in the treasury process.
- **Hybrid-Organisation-Controlled (HOC)**
  The source of funding for this class of treasury system is similar to the HCC class explained above. However, a major difference between the HCC class of treasury system and the HOC class is the funding decision making process. Within HCC treasury systems, funding decisions are made in a centralised manner. In other words, the community members or holders of stake in the cryptocurrency wield (little or) no power in the decision making process on how funds are used. Typically, an organisation responsible for the blockchain or cryptocurrency makes all the decision regarding usage of funds within the HOC class of treasury systems

We now examine existing treasury systems in real-world cryptocurrencies by discussing their features (funding source, decision-making and community participation), strengths and potential drawbacks, etc.

V. Case Study: Dash Governance System

The Dash governance system (DGS) [9] also referred to as Dash governance by blockchain (DGBB) is the pioneer treasury implementation for cryptocurrency development funding on any real-world cryptocurrency [10]. The DGS allows regular users on the Dash network to participate in the development process of the Dash cryptocurrency by allowing them submit project proposals (for advancing the cryptocurrency) to the network. A subset of "special" nodes known as Masternodes then vote to decide what proposals receive funding. Every voting cycle (approximately one month), winning proposals are voted for and funded from the accrued resources in the blockchain treasury. 10% of all block rewards within each monthly voting period is contributed towards the blockchain treasury, from which proposals are then funded.

A. Proposals and Submissions

Projects willing to support the Dash cryptocurrency request for funds through proposals by submitting a special transaction (that burns some Dash to prevent DoS attack) on the network [10]. Proposals include name, URL to detailed proposal, date (start and end date for funding request), payment address (if proposal is successful at voting), and the amount of funds requested.

Every node on the network verify the validity of proposal transactions (GOVERNANCE_OBJECT_PROPOSAL) they have seen before adding them to their local "storage" because the proposals are not stored on the Dash blockchain. Following submission, proposers are expected to publicise their submissions to other users (specifically Masternodes who vote) of the Dash community. There are third-party tools and websites that support campaigning, tracking and voting for proposals. For instance, www.dashcentral.org, http://dashmasternode.org/masternode-tools/, https://dashvotetracker.com/, etc.

B. Voting and Rules

The DGS has direct democracy as its system of decision-making. That is, voters on the DGS vote directly on proposals in the system using the Dash wallet or other third-party tools or websites. Only Masternodes can vote on the DGS and they can either vote "YES", "NO", or "ABSTAIN" implying "for", "against" or "neutral" respectively. Voting is done via a special transaction that identifies the Masternode as well as the hash of the proposal that is being voted on.

Similar to proposal submission, every node on the network checks to confirm the validity of the votes before adding to their internal storage (because like the proposals, the votes are also not stored on the blockchain).

In order to be considered for funding at the end of voting (in the payment stage), winning proposals are decided upon via a fuzzy threshold voting scheme where the absolute amount of votes for a winning project must be greater than a given threshold. Specifically, for Dash governance system,

$$V_{\mathsf{votes}} = (V_{\mathsf{yes}} - V_{\mathsf{no}}) \geq 0.1 * |\text{master nodes}|$$

That is, only proposals with V_{votes} are eligible for funding.

All eligible proposals are then ranked in a descending order according to the amount of net votes they receive and are funded accordingly until the available budget is exhausted. Note that, once budget is expended, other eligible proposals are discarded. Therefore, only top-ranked proposals that fit within the available budget are funded in an automated process that requires synchronisation of the proposal rankings among masternodes and communication on the network. As earlier mentioned, the total budget for any voting period is gotten from taxation of miners' block rewards, and is calculated as follows: $\mathsf{Budget} = (\mathsf{Block\ reward} * 0.1) * 16616\ \mathsf{blocks}$.

C. Discussion

DGS employ off-chain systems in the decision-making process. A potential issue arises as a result of reliance on data (voting and proposal) which are not stored on the blockchain. Reliance on off-chain data could make system susceptible to validation attacks leading to forks on the blockchain.

Moreover, voting on the DGS is not private, as a result, voters can be subjected to coercion from a powerful adversary. Currently, the DGS does not support proxy voting (delegation) or liquid democracy. Liquid democracy allows members of the community take advantage of experts within a community. This is in addition to the scaling advantage it provides to the system. That is, when the system grows and there are enormous amounts of proposals to vote for, it will be practically impossible for (non-technical) members of the community to thoroughly evaluate the merits of all submitted proposals. Therefore, by relying on experts through vote delegation, they can easily be more confident of their voting decision.

Participation in the DGS is currently not incentivised, and this might perhaps explain the low level of Masternode (stakeholder) participation generally experienced on DGS decision making. Finally, additional funding sources for the DGS treasury may be necessary as sole reliance on taxation may not be sufficient for future budgeting, considering the fact that miners' reward decreases by about 7% annually on the Dash network.

VI. Case Study: ZCash Treasury

ZCash Electronic Coin Company is the organisation responsible for building the Zcash cryptocurrency. Zcash is a privacy-centric proof of work mining-based cryptocurrency that utilises zk-snarks as its fundamental building block and was founded by the Zero Electric Coin Company [11]. The company serves the interests of founders, investors and developers of the Zcash coin. 20% of all block mining rewards are paid to the company under a scheme termed Founder's rewards. Next, we explore ZCash's approach to treasury.

A. Zcash Foundation

Recently, Zcash community members can propose projects for the zcash cryptocurrency through the Zcash foundation. Particularly, the Zcash foundation through its GitHub Grant Proposal Page [12] requests community members to submit proposals that fall within the foundation's defined scope, as well as support the overall mission and vision of the foundation. The Zcash foundation has a board responsible for its projects. Only 5 members voted in the Q4-2017 round of budget approval that approved 300 ZEC (approximately $\$80,000$) as the amount available for community-driven projects. Nonetheless, the board has the power to fund projects in excess of this approved amount at the board's discretion.

B. Proposal and Submissions

Community members with proposals wishing to be considered for funding need first submit an informal detailed description of their proposals (on GitHub). Following this, based on comments, critiques, suggestions and feedback from other community members, proposal owners submit a revised formal version of their initial proposals (on GitHub as well). A fixed committee of 5 reviewers (aka Zcash Foundation Grant Review Committee appointed by Zcash foundation then considers all submitted proposals and decide on the winning proposals (that receive funding) based on comments and the proposals (or by making additional consultations where necessary).

Proposal submissions are expected to contain information about the following [12]: Motivation and overview, technical approach, team background and qualification, plan, security considerations, schedule, budget and justification. The details provided under each of the listed sections are the basis upon which comments, critiques, and suggestions are raised before a final proposal submission is made.

Final formal proposal submissions are to be made via attachments to the original (informal) submissions on the "Zcash Foundation Grants: Call for Proposals". In summary, the submission process involves users submitting their proposals, and community members providing comments, and suggestions for improvements. Proposal files are issues (on the Zcash foundation dedicated GitHub repository) which contains details about the proposals.

C. Funding/Treasury Period, Payment and Monitoring

Typically, a funding cycle is a period of about three months. During the first month, calls for proposals are released and filing deadlines for initial submissions are approximately one month from the date of call for proposals. Following this, discussions and comments and critiquing of submissions are then expected to take place. Final submissions (with possible corrections and improvements from discussions and feedbacks) are then expected to be submitted approximately twenty-one days from the initial submissions. Thereafter, the Zcash Foundation Grant Review Committee review the proposals and provide funding decisions (which also requires the approval of the Zcash Foundation Board) in approximately one month. Therefore, the Zcash Foundation Grant runs a quarterly treasury period.

Payment is made in a single lump sum in the ZEC equivalent of the fiat currency requested in an approved proposal. As a means of ensuring transparency and future evaluations,

proposers of funded projects are required to provide progress reports six months after receiving funding.

D. Funded Proposals

In October 2016, the first funded project was a contest (Zcash Open Source Miner Challenge), operated by Least-Authority.com (a company that supports Zcash Electric Coin Company), to support projects that would encourage wide and open source mining of the ZEC in order to further strengthen the Zcash cryptocurrency. $\$30,000$ was paid in rewards to the top 5 winning projects selected by a panel of 3 judges.

The first set of of funding made by the Zcash Foundation (from revenues obtained from the Founder's rewards) was the award of 33 ZEC each to three recipients under the "Test Transaction Awards". This was an award made to three vibrant members of the Zcash community who have consistently developed tools and solutions that support Zcash. Following the award, announcement about the launch of the Zcash Foundation Grant program was made to encourage other community members to participate in the development of the cryptocurrency whilst taking advantage of available funding.

Although, the process raised awareness about the Zcash Foundation Grant scheme, the community was not a part of the decision making process in selecting the deserving members. Similarly, the community also played no part in the process of selecting the winning proposals of the Zcash Open Miner Challenge.

E. Discussion

Clearly, the Zcash model of treasury does not scale for a cryptocurrency with a huge number of proposals to consider. When the Zcash system grows and there are hundreds of proposal submissions, it is practically infeasible for each member of the Foundation Grant Review Committee to scrupulously review each proposal to determine its credibility and utility. Moreover, relying on a select number of reviewers appointed by a board (that grants final approval and also determines the amount of funds available for funding proposals) is not representative of a decentralised, open and inclusive system that blockchain systems (cryptocurrencies) represent. Clearly, a better and alternative approach would be to accommodate a larger number of community members (or possibly all willing members) in the decision-making process.

Having, a 5 member committee examine all proposals on a decentralised blockchain system is clearly problematic, particularly considering that the members of the committee can also submit proposals of their own. For example, in the last funding round, one of the members was unavoidably absent, thereby limiting the team strength to 4. Some proposals were reviewed by only 3 reviewers due to conflict of interest by one of the review team members who also submitted a proposal. Note that although the Zcash Calls for Proposals states that Review committee members must exclude themselves from the discussion of their own proposals, there are still subtle ways in which a committee member can still influence their proposals towards getting funded. For instance, a committee member who has submitted a proposal and has knowledge of the approved budget for proposals, can deliberately down-vote or negatively review other projects under consideration, such that total budget request of all approved proposals is less than the available budget. Thereby, increasing the chances for the acceptance of the member's proposal.

Furthermore, while the feedback process of the initial submission is desirable and helps the overall quality of proposals submitted to the system, only a limited amount of members from the large Zcash or cryptocurrency community participate in this process. Definitely, a system that encourages participation among all community members, such as delegative democracy (a collaborative decision making mechanism), would represent an improvement over the approach deployed in the Zcash Foundation Grant process. Another significant drawback of the funding mechanism of the Zcash Foundation Grant system is the non-use of the Zcash blockchain at any point in the decision-making process. Funding decisions on a blockchain-based cryptocurrency should leverage the facilities the blockchain can provide to improve the decision-making process. For, instance, secure time-stamping of final proposals, commitment(hashing) of proposal submissions, voting in the decision making process, tamper-proof "locking" of voting and funding decisions, etc.

Moreover, at any point in future, it is not particularly clear how much money would be available for funding proposals. In other words, at any particular time in the system, the amount of community-driven projects or proposals is solely dependent on the approved budget by Foundation Board. Although, the Zcash Foundation Board is empowered to make discretionary approvals above a budget for any particular quarter, the uncertainty about available budget may thus inhibit the amount of development proposals that the community can contribute to the overall development of the cryptocurrency. Therefore, an alternative solution, such as "decentralised treasury pool" represents a better solution for the system.

In conclusion, because the system is relatively new, it is expected that the system will evolve with time and some of the issues raised will be addressed. For instance, there are plans to implement some changes to the system, e.g., the establishment of "Working Groups" for monitoring volunteers/proposers. Furthermore, information on the Zcash Foundation Grant GitHub page also corroborates the suggestion that there are plans to evolve the system into an "open-community review process".

VII. Case Study: Ethereum Foundation

In the Ethereum blockchain, the bulk of discussions and analyses revolve around governance system rather than treasury system. It is important to note that a governance system is not the same as a treasury system, although, both systems support long-term sustainability of blockchain technologies. Most importantly, a treasury system handles and ensures regular funding and decision-making on fund usage, a governance system is mainly concerned with general blockchain and protocol rules such as soft-forks and hard-forks. A governance

system determines how and when changes are made to a blockchain's core.

Similar to the Bitcoin Foundation, the Ethereum Foundation is a not-for-profit Swiss that supports Ethereum through research, development and education [13]. Like the Bitcoin Foundation, the Ethereum foundation also relies on donations as its primary source of funding for Ethereum development and research. Basically, the foundation uses donations to support "general" Ethereum development activities. However, donors can specify specific projects for which their donations can be used for (provided the foundation supports such projects).

Although, the Ethereum blockchain does not have a treasury system, it supports development projects through grants to support research that would improve blockchains. For example, the programs referred to as subsidy programs was established to support projects on sharding and layer-two protocols that would improve blockchain scalability. Teams, researchers, developers, who do relevant work in this area can apply for support through a process described as "flexible to accommodate various needs of different applicants". The Ethereum core leadership is responsible for deciding what proposals are funded, with funding amounts of $\$50,000$ up to $\$1$ million. Clearly, this encourages open and community-wide participation, however, the core leadership wields much power in the decision-making process.

Critics of decentralised governance argue that adaptation of blockchain protocols to changes is slow on systems with decentralised governance due to the minimum requirements for approval being high. They argue that decentralisation constitutes the major point of arguments against existing off-chain or traditional blockchain governance model. Critics further argue that a side-effect of decentralised on-chain governance is the ability of a rich minority (with very substantial amount of stake) to have over-bearing influence on decision-making via a voting process.

Other highlighted criticisms or suggested factors that hinder on-chain voting governance are low participation (or voter turnout) and unequal wealth distribution. Within Ethereum, for instance, Ethereum Improvement Proposal (EIP) 186 Carbonvote, with approximately 2.7 million ETH voting had less than 20% voter turnout. About 11% is the highest voter turnout of any current proposal on the DAO with about $23,606$ unique Ethereum addresses holding tokens (aka DTH - DAO Token Holders). However, low-voter turn-out is not peculiar to blockchain voting. According to FairVote, established democracies such as the United Kingdom and United States also experience low voter turnout. For instance, only about 60% of eligible voters participated in the 2016 US national elections. Similarly, the 2015 UK elections recorded about 66.6% voter turnout.

However, the problem of low voter incentive and low voter turnout can be addressed through clever incentives engineering, by rewarding participants who take part in elections. Furthermore, novel voting mechanisms such as liquid democracy mitigate some of the well-known raised issues that affect traditional voting schemes. For instance, these issues are addressed by delegative/liquid democracy where users effectively assign their voting powers to other (better qualified) members of the voting community. Members who receive delegation usually possess more subject-matter expertise and knowledge, and are renowned within the ecosystem.

VIII. Conclusion

We highlight the sustainability of funding for blockchain platforms. We examine various sources of blockchain funding and categorise treasury system models. Treasury systems are relatively novel within blockchain research, and cryptocurrencies that deploy treasury systems, e.g., Dash cryptocurrency, have benefited from its adoption.

However, a number of issues continue to affect improved adoption and success of pioneer treasury systems. These include inadequate design analysis, security, privacy and game-theoretic analysis of the systems before they were developed and deployed. It is evident from the systems reviewed that they were created ad-hoc and changes (not necessarily backed by research evidence) were made as the systems mature. Little or no analytical proofs of security and overall security goals and requirements of these systems are provided.

Finally, despite being an interesting solution to sustainable blockchain funding , treasury systems require careful design and analysis to avoid issues that will hinder their utility. Notably, utmost consideration should be given to source of treasury funds, management, decision-making (e.g., voting rule and systems such as liquid democracy, receipt-free voting), partitionary budgeting, usability, security and privacy, incentives for stakeholders, game-theoretic analysis, cryptocurrency inflation and blockchain (resource) utilisation.

References

[1] B. Zhang, R. Oliynykov, and H. Balogun, "A treasury system for cryptocurrencies: Enabling better collaborative intelligence," *IACR Cryptology ePrint Archive*, vol. 2018, p. 435, 2018.

[2] D. Kaidalov, L. Kovalchuk, A. Nastenko, M. Rodinko, O. Shevtsov, and R. Oliynykov. (2017) Ethereum classic treasury system proposal. IOHK RESEARCH REPORT.

[3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21*, 2015, pp. 104–121.

[4] BitcoinMagazine. What is an ico? bitcoin magazine. [Online]. Available: https://bitcoinmagazine.com/guides/what-ico/

[5] B. A. Token. introducing blockchain-based digital advertising. [Online]. Available: https://basicattentiontoken.org/

[6] Aragon, "unstoppable organizations. create value without borders or intermediaries." [Online]. Available: https://aragon.org/

[7] ICOAlert. Ico alert - the only complete list of icos, token sales, and crowdsales. calendar of active and upcoming initial coin offerings. [Online]. Available: https://www.icoalert.com/

[8] BitcoinCore. Announcing the bitcoin core sponsorship programme. [Online]. Available: https://bitcoincore.org/en/2016/04/04/announcing_sponsorship_programme/

[9] DASH. Dash is digital cash. https://www.dash.org/.

[10] D. Kaidalov, A. Nastenko, O. Shevtsov, M. Rodinko, L. Kovalchuk, and R. Oliynykov. (2016) A review of the dash governance system:analysis and suggestions for improvement. IOHK RESEARCH REPORT.

[11] ZCash. Zcash - all coins are created equal. https://z.cash/.

[12] ZcashFoundation. Zcash proposals submission. https://github.com/ZcashFoundation/GrantProposals-2017Q4/blob/master/README.md.

[13] Ethereum Blockchain App Platform. https://www.ethereum.org/.