

BOScoin White Paper 2.0

2018. 11. 01.

Disclaimer

Abstract

Foreword

1. Introduction: Background

1.1 Understanding the Current Economic Model

Distribution Failures caused by corporate structures

Centralized financial decision-making process

Developments in information technology reduce the need for human labor

The three problems and a direction for a new economic system

1.2 Alternatives to the Current Economic System

Cryptocurrency

Commons Movement

Impact Investment

1.3 Analysis of Alternatives and a New Direction

Money and commerce as a Commons movement

The current problems of the crypto economy and our proposal

2. Proposal

2.1. Public Financing

Definition and meaning

Reverse ICO Partner Program

2.2. Congress Voting

Background

Definition

Homomorphic Encryption

Membership

Voting

Requirements

Voting Preparation : Getting a Ballot Stamp

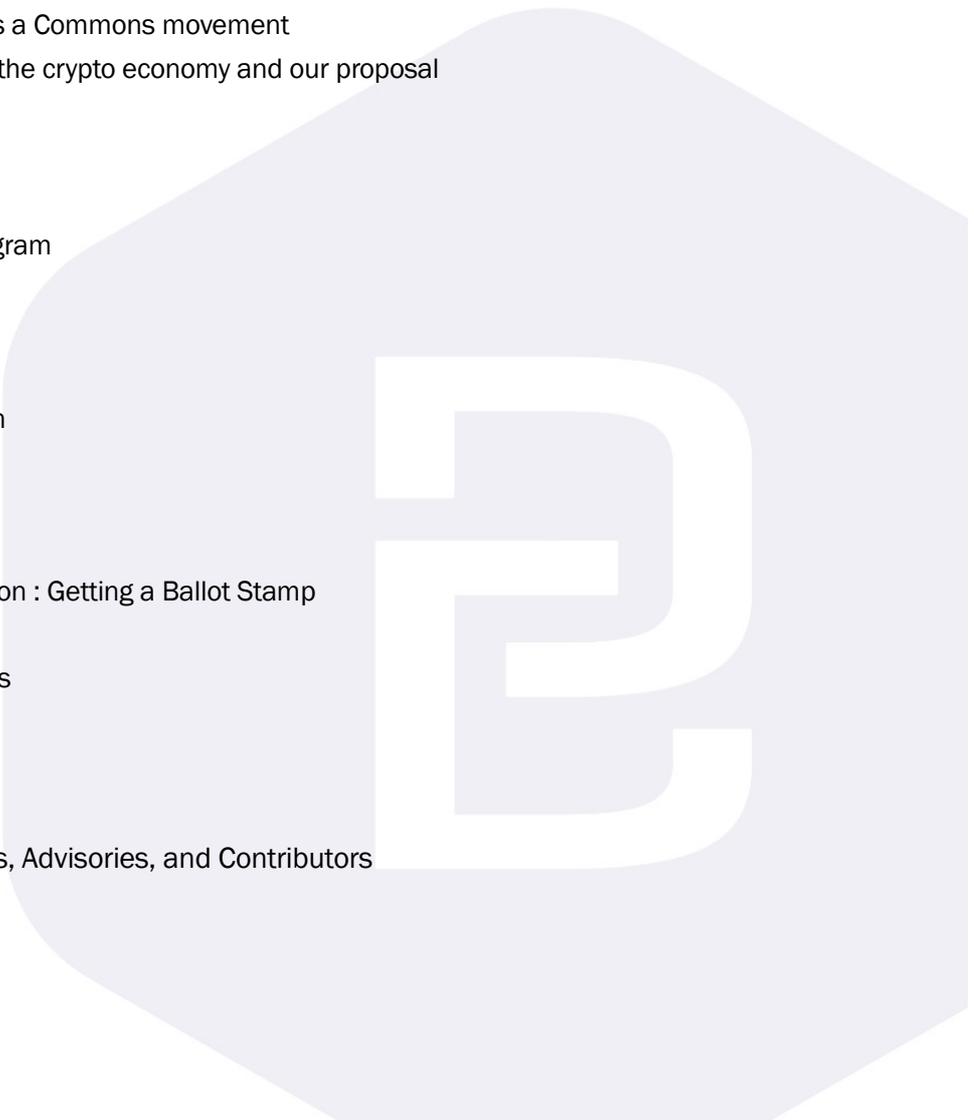
Casting votes

Tallying the votes

3. Conclusion

Reference

BOScoin White Paper 2.0 Writers, Advisories, and Contributors



Disclaimer

This document is 'BOScoin White Paper 2.0', a summary of the ecosystem BOScoin constitutes and plans to constitute. This White Paper purports to present only future plans and related information and does not guarantee execution of the plans. Any technical innovations described in this document are under development and not yet completely applied, unless explicitly indicated. BlockchainOS does not provide nor guarantee any successful development and implementation of technical innovations nor any result of activity. Information presented in this document is referenced from sources believed to be reliable, however, there can be no assurance as to the accuracy, completeness, or adequacy of such included information.

BlockchainOS team (BOS team) does not approve nor guarantee the value of BOScoin. BOS team does not provide nor guarantee offers of any retrievable investment as well. To the maximum extent permitted by the applicable laws, regulations and rules, BOS team, authors of this document, advisories, and any third party involved in BOScoin project shall not be liable for any indirect, special, incidental, consequential, or other losses of any kind. Investors shall be liable for their investment arising out of, or in connection with, any acceptance of, or reliance on this White Paper. Investment should be made depending on your own knowledge, investigation, evaluation, and judgement. If you are in any doubt as to the actions to take, you should consult with your legal, financial, tax or other professional advisors.

This White Paper is available only from <https://boscoin.io/>. Any copies or duplicates of any part of this document without the corporate identification may be made only by specific prior written permission by BOS team. All contents herein may not be used or reproduced without the prior written consent of the BOS team. Distribution of this document may be restricted in some nations by their laws, regulations and rules. The act of possessing this document constitutes an agreement to the aforementioned terms.

Abstract

The BlockchainOS team (BOS team) submits the “White Paper” — a complimentary to the first white paper. The breadth of current discourse and business expansion around the blockchain and cryptocurrency market calls for new strategies. BOScoin’s new project builds a global system of finance. This community driven credit creation system aims to shock the existing paradigm with refreshing technological and socio-economic implications.

The current capitalist system has led an era of unprecedented affluence for the past 50 years. Since the 2008 global financial crisis, however, capitalism seems to have reached its limits. As Piketty concisely formulated in “Capital in the Twenty-First Century”, the intensification of economic inequality in a corporate system, the loss of jobs with technological development, dropping consumption, the alienation of financial sovereignty, etc. will render current society untenable. This has encouraged us to focus on three alternatives for a new economic vision: Cryptocurrency, the Commons movement, and Impact investment. By combining these three alternatives with blockchain technology, humanity can move beyond shareholder capitalism, which concentrates wealth to a few shareholders. A funding model called Public Financing (PF) can generate credit through mass participation and utilize democratic decision-making processes. This is an effective way to utilize value created by the community. The Commons movement was able to transcend the limits of property laws without denying the core principles of capitalism. Likewise, BOS team wants to transcend capitalism’s limits in the most capitalist way — without denying its core principles and merits. PF is BOScoin's vision; this model differs from other ICOs and is BOS team’s core competitive strategy in the cryptocurrency market.

PF creates credit, not through decisions made by a central bank or government, but through the collective consensus of individuals who use and trade real credit. BOScoin has already introduced a governance system called the Congress Network to give its participants decision-making powers. The BOScoin community can propose, review, and vote on new token issuance through the Congress Network. The community as a whole has financial sovereignty, rather than it being given to a concentrated few. The community members determine the size, volume, and base price of issuance, as well as the terms of its usage. The community’s decision will be executed by Trust Contracts in BOScoin. Real economic assets acquired through the issuance of BOScoins will be used by the community as commons, and thus PF will remain “public”.

When problems arise in a community, it is important that members express their opinions and participate. The conventional corporate system of allocating one share per dollar value or a Proof-of-stake (PoS) system and a Delegated Proof of Stake system (DPoS) in some Blockchain projects, however, allow those with more dollars or stake to exert more influence, dominate the system, and eventually create greater inequality. BOS team aims to realize an anonymous voting system which enables one person / one vote; to accomplish this, we need to verify personal identification. BOS team aims to develop the Congress Voting system based on homomorphic encryption technology. This technique can overcome

vulnerabilities such as key capture and data leaks. Homomorphic encryption operates directly on the encrypted data without accessing the encrypted key. By using this encryption, BOS team is trying to create a technology that allows only one identity per person, while at the same time allowing completely anonymous voting on the network.

Our goal of “hacking capitalism in the most capitalist way” will overcome the limitations of the system through the explosive potential of the crypto economy and the Commons movement. PF and Congress Voting will be an important stepping stone for that goal. The contents that we could not cover in this White Paper, crypto-economy model BOScoin plans to constitute and Generic Trust Third Party (GTTP) as an element of the model, will be described in the next revised edition.

Foreword

We started writing the BOScoin White Paper 2.0 to outline the vision of the BOS team and BOScoin beyond the first white paper. White Paper 1.0 defined BOScoin as an alternative model to overcome the limitations of Ethereum. It introduced the Congress Network as a means of solving the technological and governance problems of the Trust Contracts. The Trust Contracts itself resolve the security issues faced by smart contracts and mFBAs (FBAs which accept open membership). An economic model called the Commons Budget was introduced to fund the BOScoin ecosystem into the future. However, we re-evaluated the market and our business development after the ICO and decided that a complement to the existing strategy was needed. The core of our complementary strategy is Public Financing, a counterpoint to the current ICO crypto economy, and Congress Voting realizing one person / one vote.

This White Paper focuses on the problem that the BOS team wants to solve and our solution — “Public Financing”. As the paper will further elucidate, PF will be executed by voting on the Congress Network. We intend to introduce Congress Voting based on the homomorphic encryption developed in conjunction with Korea Smart Authentication Corp (KoSAC). We will organize White Paper 2.0 around these two topics. In the revised version of this White Paper, we will propose a new concept called a Generic Trust Third Party (GTTP), which is a link between the BOSNet and external data.

BOS team is a spiritual descendant of the Open Source movement and its culture. We work with the belief that blockchain technology can transform the world. By working on the latest white paper, BOS team members revitalize our relentless vision. What is the objective of BOS team? In response to this question, project leader Yezune gave this answer at a Dallas Meetup: “In the spirit of the GNU Declaration and the Creative Commons movement, we want to hack capitalism in the most capitalist way”. BOS team is not trying to create a token platform that simply uses a blockchain, nor a pseudo currency for a specific purpose. We want to organize and create a de facto global currency and credit creation system, one that is trusted by the global community to successfully replace the current one.

Let's take a closer look at the issues that the BOS team is trying to solve.

1. Introduction: Background

The world is currently experiencing the most affluent era since the beginning of civilization. This affluence comes from the increase in productivity, not only from technological developments, but also from credit creation by the capitalist system. This system is able to generate credit at levels unlike any other society in the past. The end of the gold standard in 1971 introduced fiat currencies worldwide and gave birth to this credit generation mechanism. By overcoming several economic crises, which were portrayed as mere glitches, the capitalist economic system was believed to be invincible. However, this confidence was shaken during the 2008 global financial crisis.

The current capitalist system fails at distributing wealth. This indicates that the capitalist system's very existence is endangered, because it continues to break down its own consumption-based ecosystem. While skewed distribution causes several market failures, technological developments (particularly in information technology) reduce the need for labor. This, in turn, lowers labor earnings and quality of labor. How can the capitalist system be maintained if workers cannot consume due to such technological developments? If it cannot be maintained, what are the alternatives? These are questions that BOS team will address through BOScoin project.

In the following section, we will examine in detail the problems of capitalism and analyze various alternatives which tried to overcome these problems. Such analyses of the alternatives will shed light on BOScoin's new direction. We will then propose a new crypto economy to overcome current economic problems.

1.1 Understanding the Current Economic Model

Distribution Failures caused by corporate structures

Following the Industrial Revolution, the capitalist system has, despite some difficulties, experienced a general, proportional growth in income and productivity. This increase in income gave birth to many middle-class consumers with significant purchasing power. The economy continued to grow, backed by the flourishing middle class. The middle class in the 1980s and 2000s, however, saw little growth in income, even while the economy was experiencing solid growth. Because income did not grow for the working class in developed countries, their consumption was maintained through taking on more low-interest, consumer debt. They were able to consume all goods and services through financing. This was called the "financialization of the economy", a trend that has since continued worldwide. Through this mechanism, the financial services sector grew exponentially, and for a while, the economy seemed to be booming. A precarious situation took hold during this time; capitalists and people with money accumulated a great deal of wealth through capital income, while the majority of the people fell further into debt in order to sustain their consumer activity. The current iteration of the capitalist system (so-called "neoliberalism"), based on the "financialization of the economy", has created more fundamental

problems than the capitalist systems of the past. The 2008 subprime mortgage crisis was a symbolic event that shed light on these problems.

There are many reasons for the failure of wealth distribution, but the most significant cause of such structural failure was the systemic focus on maximizing shareholder profit. A corporation is established and funded through the issuance of stock. Its primary interests are aligned with the distribution of profits to its shareholders. That is why most corporations try to minimize production costs and maximize consumer prices. They, therefore, seek an increase in the productivity per unit of labor; this means cutting labor costs. For the past 400 years — since the first recorded incorporation — society has certainly benefited from the innovations driven by corporations. However, the wealth generated by this improved productivity is being returned to a few shareholders, and not distributed back to the workers, who actually consume the produce goods and services. The corporate system is not only failing to distribute wealth, but also accelerating the economic downfall of the workers and consumers. In recent years, as information technology has become critical, global platform-based companies have emerged in the form of multinational corporations. These companies are now able to concentrate wealth on a global scale, as opposed to ones previously limited to a jurisdiction (Piketty and Ganser, 2015).

Centralized financial decision-making process

In a capitalist system, finance plays a crucial role in credit creation. However, we accept the inability to participate in the financial decision-making process as natural. Given the fact that the basis of finance is the agglomeration of small credits from numerous ordinary people, why should financial decisions be left to a few financial institutions? A few people control the whole financial decision-making process — and subsequently, its profits. The problem with this structure is that, when the structure fails, the ordinary people — who didn't make the financial decisions — are held accountable. The set of decisions that led to the Lehman Brothers bankruptcy is a perfect example. These were made by a small cadre of financiers, but the burden of these decisions was shared by society itself — which was the source of credit. Another example is how banks create credit through commercial loans; these are also judged and enforced by a few financiers. The sentence engraved in the Genesis block of Bitcoin, “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” (Times, 2003, January), pinpointed the phenomenon that the public is deprived of its financial sovereignty.

Of course, one could participate in the economy as a shareholder of a corporation. Under the current financial system, however, most people are not given the opportunity to participate as shareholders. Take, for example, the current start-up ecosystem, which is structured to be high risk but has the potential to generate high returns through M&As and IPOs. Start-ups grow through venture capital investment. As it grows further, more capital is invested through private equity funds and investment banks. Based on these funds, a start-up can attain global platform status such as Google and Facebook, and eventually be listed on a stock exchange. Only then is the public allowed to have a piece of the pie. Before being placed on an exchange, investment is made solely by a few venture capitalist, private equity fund managers, and investment bankers. Yes, there is high investment risk, but the public are outright denied access to the potential for great capital gains.

As the market for P2P loans and crowdfunding, as well as FinTech in general, began to grow in 2016, major countries such as the United States set individual investment limits for P2P loans and crowdfunding. The opportunity for individuals to take the risk of investment and reap high returns on that investment was taken away in the name of “investor protection”. On the one hand, the state has a duty to protect the individual, but on the other, these are unreasonable regulations over the public’s financial decisions. There are diverse tools to encourage well-informed investments, and still allow opportunities. For example, Russia recently set a maximum dollar amount to participate in an ICO for the general public and requires individuals take a course at a recognized institution to qualify for an increase in the amount of investment beyond the maximum. Even in the ICO market, there are similar attempts, such as individual investment ceilings, to prevent public participation. Thus, it can be argued that under any capitalist and liberal economic orders, the ordinary worker and citizen has no “financial sovereignty”.

Developments in information technology reduce the need for human labor

In the industrial era, the key factors of production were land, capital, and labor. With the development of industrialization, management and technology have grown ever more significant, and today, they have become key factors of production. The changes during 1980s and 2000s was significant, because of huge developments in technology. In contrast to the past, when technology had complemented and enhanced human productivity (Brynjolfsson and Saunder, 2009), automation today replaces labor across the entire economy; such displacement of workers by technology may exacerbate the gap between returns to capital and returns to labor. (Brynjolfsson, and McAfee, 2014).

As witnessed by stock valuations of modern global platform corporations (such as Amazon, Google, Facebook, Uber, Airbnb, etc), the information goods and technology industry, which utilizes information as the key factor of production, is becoming increasingly influential (Cusumano, 2017_1; Cusumano 2017_2). Companies that produce physical products also use information technology to enhance their commodities. For example, Nike is enhancing their products by presenting the commodity with healthcare data. This trend is predicted to continue. Corporations will use such technologies to increase shareholders' capital gains and replace labor. Moreover, a corporation that does not do so will be left behind the competition.

Intermediary platform-based IT corporations scale from the effects of positive externalities, i.e., information goods. For example, when a user on the Amazon website purchases a digital camera, a piece of clothing, or a book, their choice is recorded and used to assist other Amazon users’ choices. In a shareholder capitalist economy, most of the wealth created through such information goods is taken by the enterprise and subsequently by its few shareholders. At the same time, these IT innovations damage preexisting industries and jobs. Amazon’s disruption to the US retail industry has been so effective that it has caused the bankruptcy of many smaller independent brick and mortar retailers. During this process, Amazon creates only a few highly skilled IT jobs. Paradoxically, consumers who enabled the growth of Amazon are losing their jobs because of it. New techniques related to Artificial Intelligence and Big Data will only accelerate this tendency; this trend is here to stay.

In short, information goods and technology have become far more important factors of production than the conventional factors such as land, capital, and labor. Information goods and technology are easily duplicated and have little marginal cost in the production process. Because of these attributes, information technology continues to improve productivity and reduce the need for labor. Information technology has the tendency to remove human labor as soon as a return on investment is possible. Where labor remains are areas with no return on investment — often the lowest paying jobs. Moreover, once information technology develops further and has captured all easy returns on the investment, the process will repeat itself in low wage jobs. IT platform companies provide services to enhance user experience, but such innovations reduce the need for labor and disrupt existing industries. This perspective offers a whole new dimension to the economic crises we are experiencing.

The three problems and a direction for a new economic system

We believe that a “new economic system” should be able to solve the three problems above. In other words, it is necessary not only to utilize the power of capital’s credit generation, but also to 1) overcome the problems of shareholder capitalism and provide a way for everyone to participate in the market, 2) enable those who provide credit for the economy to participate in its financial decisions, and 3) define a production system as a common resource if the production requires or utilizes consumer activity but does not benefit them.

Academics have proposed that a global standard on capital taxation and basic income be introduced to overcome the fundamental problems of capitalism. These proposals ask for bold and pragmatic political decision-making. However, other approaches — alternatives that do not require political decisions — are already here. Let's take a look at those approaches.

1.2 Alternatives to the Current Economic System

There are many alternatives to the current economic system, but we herein reviewed ones that inspired us to create our new vision: Cryptocurrency, Commons movement and Impact investment.

Cryptocurrency

In 2017, interest in the cryptocurrency market spiked worldwide. The economic system based on cryptography called cryptocurrency is partially becoming an alternative economic system. Most crypto projects are 1) decentralized through blockchain technology, 2) structured to compensate ecosystem participants through cryptocurrency (token economy) and 3) unlike existing investment schemes; ICOs (Initial Coin Offering) make it easy for anyone to become an investor. These features could potentially overcome the problems of shareholder capitalism, so cryptocurrencies are emerging as an alternative to the corporate system. These three characteristics correspond to our conditions for a “new economic system” discussed above — low barrier for participation, collective decision-making, and sharing the means of production. With due optimism, the cryptocurrency market grew explosively in 2017. In the past,

start-ups emerged under the investment of Venture Capital (VC). Now, there exist many startups who launch ICOs, and many VCs choose to invest in these ICO-based startups.

BOScoin introduced the Congress Network to reinforce participants' decision-making power, but neither BOScoin nor most cryptocurrencies sufficiently satisfied the three conditions of a “new economic system”. The sharing of the means of production was often not even considered. There is a movement, however, that maintains that a system of production created by the global community is a common resource and must provide access to everyone. This is called the Commons movement.

Commons Movement

The budget introduced in BOScoin White Paper 1.0 is a Commons Budget, not a common budget. The Commons Budget did not yet have a clear definition nor an operation strategy in place, but it was created in the spirit of the Commons movement. Commons refer to the cultural and natural resources available to all members of society, including natural elements such as air, water, and earth. These resources are not privately but jointly owned, and the Commons is managed by a community for personal and collective interests. Amongst these movements, there were attempts to organize information goods and technology as common property of the collective society. Prominent examples of such movements are GNU and the Creative Commons.

If information goods and technology are a large part of the added value of a product, then the following two questions should be addressed. First, should companies monopolize information goods and technology while accumulating wealth created through them? Furthermore, when the importance of IT to added value rises, the lack of jobs destroys the consumer market, and the entire economy is in a depression, should the added value created through information goods and technology be shared with the community? The Commons movement, which interprets the information technology and production systems as “commons”, can be an important step towards a working utility system under joint ownership.

If a community agrees that a particular resource is commons, the wealth produced using the commons ought to be shared by the community. This is a fundamental and effective alternative to the vicious cycle of a dying consumer base and dropping labor income. We will analyze the Commons movement in 1.3 and present our proposal to make this philosophy successful.

Impact Investment

“Impact investment” seeks appropriate returns and social value. While conventional investments focus on economic and financial performance, impact investments refer to investments that goes beyond and take account of social and environmental implications. It is an attempt to solve social problems through business — recognizing that it is difficult to solve social problems through public budgets alone. For example, in 2012, Goldman Sachs invested \$9.6 million in a project to lower the youth recidivism rate in New York City. There are other active investments into similar types of projects. Impact investment is also emerging as a trend in Korea. For example, VC firms such as Korean Social Investment and Yellow

Dog have been active in impact investing. There are also real estate investment and management companies such as OOGround, whose mission is to turn their buildings into independent platforms for social problem-solving while creating value and profit.

Impact investment is a good way for the community to secure the commons, but if driven by a selected few, it is certainly not the most efficient solution to the problems of the current economic system. However, it is clear that impact investments can increase social value.

1.3 Analysis of Alternatives and a New Direction

We have seen that the cryptocurrency and Commons movement present solutions for a new economic system. In Section 1.3, we will analyze the limitations of the current Commons movement and the crypto economy and discuss how to combine the advantages of these two alternatives.

Money and commerce as a Commons movement

Good intentions and practical usefulness are two independent measures. The Commons movement seeks to expand the communal P2P production method; but can this approach achieve the ideals of the Commons movement?

If the Commons movement wants to be bigger than the state and the market, then the Commons movement has to compete in the market on a state or global scale. For example, suppose a cooperative platform were created to solve the problems caused by Uber. Could this platform survive the competition with Uber? Can P2P production systems compete with products made by robots? We dare say, it won't be easy. Small scale producers will find it difficult to play catch up with the might of economies of scale.

Of course, communal P2P production is effective in certain areas. There are two informative success stories from the Commons movement: GNU and Wikipedia. The two projects had these things in common. 1) Both projects had clearly defined actors and avid contributors from the start, 2) these projects would have been impossible without large scale collaboration, and 3) they were structured to give contributors not only reputation – the primary incentive – but also economic incentives based on that reputation. This resulted in products with quality that were comparable to those of ordinary capitalist companies. So how did these commonalities create success? The first commonality – to have clearly defined actors and contributors – is a condition, not a method for success. The third commonality – how they provided reputation as economic incentives – is also not a big enough motive for the participants. We believe that the fundamental mechanism by which these two projects succeeded was that they mobilized large-scale collaboration, to a scale that the existing capitalist companies could not replicate. This implies that in order to succeed, the Commons movement must enable collaboration between more and diverse individuals than the existing capitalist enterprises can. It is unlikely that all spheres of society will be subject to the Commons movement (at least until the Commons occupies a dominant axis of society).

This is because not all areas are best suited for large scale collaboration. It is also essential to have trustworthy, stable tools to ensure that everyone can participate with confidence.

So, we ask ourselves, in what areas can the Commons movement be most effective in solving capitalism's problems? We see finance as the ideal candidate for the Commons movement. As we have discussed, if we cannot fundamentally solve issues around capital and finance under capitalism, the affluence of present is unsustainable. Historically, particularly for the credit cooperatives in the financial sector, there was large scale collaboration amongst ordinary citizens. However, the lack of technology to maintain trust made it difficult to organize global large-scale collaborations such as GNU and Wikipedia. However, blockchain and crypto economies will be able to build trust amongst citizens, resulting in large-scale global collaboration. In this way, we can generate greater credit than the financial institutions. Furthermore, we believe that it will be possible to create credit at a large scale based on the crypto economy and to commonize those means of production. BOScoin has already embraced the Commons concept by introducing the Commons Budget. However, we believe that the methodology presented in White Paper 1.0 was insufficient in presenting this goal. We will now discuss and complement this gap by reviewing the current state of the crypto economy.

The current problems of the crypto economy and our proposal

The limitations of the current crypto economy in terms of technology are clear: slow processing speed, an unsafe smart contract development environment that leads to frequent hacking incidents, software code that holds contracts illegible to the public, etc. However, the technical problems of cryptocurrencies are expected to be solved in the foreseeable future. In the first white paper, we presented an alternative to these technical limitations through mFBA and Trust Contracts. We believe that the technical strategy of White Paper 1.0 remains valid, and it remains in development. Thus, this white paper will examine the strategies and policies of the current cryptocurrency market from a socioeconomic point of view rather than the technical and analyze the problems.

1) Price volatility due to scarcity from predefined limitations on volume. The large volatility of cryptocurrency prices comes in part from the growth of the market, but more from the expected scarcity of the predefined total issuance volume. Since the 2008 financial crisis, central banks have recklessly issued fiat currencies (quantitative easing), and Bitcoin was an active response to the decline in the value of fiat currency. Bitcoin was developed with a predefined total issuance plan and a decentralized monetary system. It has become an alternative to the existing fiat currencies by those in the cryptocurrency community. Cryptocurrency has started attracting attention through one particular mechanism: Scarcity increases the value of cryptocurrency, participants increase with the increase in value, and the cycle repeats (the "scarcity mechanism"). Moreover, Ethereum expanded the scope of the blockchain applications in 2016, consequently, the number and capitalization of cryptocurrency projects worldwide has increased significantly. The scarcity mechanism works as an investment incentive for participating in the cryptocurrency ecosystem, but it causes large fluctuations in crypto prices. This volatility of cryptographic currencies is a barrier to a means of monetary function. If the price goes up, one party will want to keep the cryptocurrency and if the price goes down, the other party will be reluctant

to receive them. In order to overcome this problem, various attempts — such as making a value-stabilized token pegged to a fiat currency — have been made, but they have not found fundamental solutions. The volatility issue complicates economic ecosystems even with a single cryptocurrency, and it becomes even more complicated when multiple cryptocurrencies are used simultaneously. Let's look at this problem through the Dapp-ICO strategy of platform cryptocurrencies.

2) **Fragmentation of the monetary space by ICOs.** As Ethereum provides the ability to issue tokens for Dapps, numerous ERC20-based ICOs have taken place. Besides, Ethereum recently introduced DAICO, a fix for the DAO after the hacking incident. Ethereum's strategy is to position itself as a token publishing platform. Other consensus layer platforms, even the ones trying to outperform Ethereum are using similar Dapp strategies. This strategy is effective for the initial platform expansion; most consensus layer networks are not capable of doing everything, but they are effective at attracting a variety of projects through economic incentives. BOScoin also once agreed with this strategy and applied it in White Paper 1.0.

However, we believe that the Dapp-ICO strategy is likely to reduce the money space of the crypto platform by fragmenting the users and merchants. Money is conceptually similar to a platform, in that it only becomes valuable when there is widespread usage — by consumers, holders, and investors. Currently, the Dapp-ICO strategy fragments the money space even if it uses the same crypto network resource. Although it is not inconvenient to occasionally use the exchange as an investor, it is very inconvenient for the consumer to spend various cryptocurrencies for everyday use. Currently, most cryptocurrency holders will not complain about the emergence of various cryptocurrencies, because they tend to view cryptocurrency as a digital asset. In the future, however, we anticipate that the fragmentation of the money space caused by the Dapp-ICO strategy will be a major obstacle for cryptocurrency's rise to the status of fiat currencies. This Dapp-ICO strategy seems favorable in the short term, but it is not comparable to the status of fiat currency.

3) **A fragmented credit creation system.** In order to prevent a fragmented monetary space, BOScoin once pushed for Dapp development through the Commons Budget. After meeting many companies for collaboration, however, we found that what they wanted was to create credit through an ICO more than to use BOScoin platform itself. We also found out that the platform may be a secondary component for a certain industry. Furthermore, the scale of credit they were looking for was too large to fit the Commons Budget. (The details of the Commons Budget and its usage will be presented later in the next version of White Paper 2.0) Existing legal currencies are issued by a central bank and credit is created by the commercial banks' fractional reserve banking. Thus, commercial banks have a large-scale credit creation mechanism that creates additional credit based on created credit. This fiat-based credit creation system is the core of financial capitalism. Currently, the crypto economy does not have such a credit creation system; ICOs create credit at first, but there is no continuous cycle. It is also difficult for a consensus layer to transfer the credit generated by a Dapp-ICO to another Dapp-ICO. In other words, the crypto economy is unlikely to surpass the capitalist credit creation system. To expand the crypto economy and move beyond the existing capitalist credit system, it is necessary to replace the Dapp-ICO strategy.

4) **The Problem of Centralization.** Most cryptocurrencies are networked by economic incentives. Bitcoin was famed for being decentralized at the beginning, but the whole network is under the control of those with majority hash power. Low fee transactions were constantly being placed in a situation where confirmations were erratic and nodes having to pay high fees to process a timely transaction. The situation was in stark contrast to the expectations of crypto experts who claimed transaction fees would be lowered with decentralization. The PoS or DPoS method is also expected to cause centralization problems similar to PoW. EOS project unfortunately confirmed this speculation. A network started to become centralized once the consensus process depends on economic incentives. This is not what we want in a cryptocurrency economy. Moreover, a cryptocurrency without a governance system faces a very difficult situation in resolving the centralization problem. The centralization problem is something even BOScoin, which has a governance structure, must effectively overcome. (The solution to this problem will be covered in the next version of the White Paper 2.0)

2. Proposal

The contents of the introduction are summarized as follows. In the current capitalist system, information goods and technology are important. Thus, labor earnings decrease, and the wealth is not distributed. This collapses the consumption base which capitalism depends. We need a system to solve the distribution problem, and the current crypto economy is the closest thing to a workable alternative. However, the Dapp-ICO strategy of the current crypto economy is likely to produce fragmented credit generation systems that may not solve the capitalist problem the BOS team intends to solve.

Public Financing. In order to solve the problem of fragmented credit creation systems by the Dapp-ICO strategy, we propose Public Financing (PF). PF is a way for individuals who use and trade real credit to make collective decisions to create credit. Rather than be dictated by a central bank or government, the community creates its own credit. Unlike other crypto platforms, BOScoin can offer PF because it has a governance system called the Congress Network. In capitalism, the institutionalized financial system holds most capital and most decision-making powers; most members of the system obediently follow the decisions made by others. It is also difficult to withdraw from the system. On the other hand, many cryptocurrencies, including BOScoin, are community currencies. If a currency does not reflect the voices of its members, the community will wither and die. A cryptocurrency can grow into a community money if justified by community consensus. Thus, a cryptocurrency should be able to offer a governance structure which reflects a majority of community. However, the Congress Network proposed in White Paper 1.0 allowed those who hold many nodes – more wealth – to have a bigger influence on community decision-making. To solve this problem, we are implementing a system of one person, one vote. The system of one person/ one vote may not be the best method to the problem of plutocracy but the most appropriate governance system for the time being. However, it is impossible to introduce the one person, one vote principle without requiring identification – this in turn jeopardizes privacy and freedom of expression. This goes against the general ethos of the blockchain. At the time of writing White Paper 1.0, we were unable to find a solution to this challenge, and the Congress Network's decision-making process remained unanswered. We reviewed this problem with KoSAC and looked at the possibility of creating a form of Congress Voting using homomorphic encryption. This is covered in detail in section 2.2.

2.1. Public Financing

Background

So far, we have described the background for introducing PF. In summary, we assessed that the crypto economy is, among the many alternatives to the current economic system, the most effective in utilizing credit creation mechanisms and solving distribution problems. However, the Dapp-ICO strategy of the current cryptographic token economy is not an appropriate alternative to the capitalist system because it segregates and fragments the money space.

Definition and meaning

PF means the BOScoin community issuing additional BOScoins as a credit-generating means of acquiring various assets of the real economy. The credit is generated from the community, not invested from a third party outside the community. The community itself suggests, reviews, and votes on additional issuance through the Congress Network. This decision is implemented through BOScoin's Trust Contracts. We define this process as Public Financing (PF). The assets and their added value received by the community through PF will not be distributed to each member of the community. The community utilizes and manages the assets and their added value through decisions made by the Congress Network.

The difference from the earlier proposal with the Commons Budget is: First, in addition to predefined issuance plans, the community issues additional coins through collective decision-making. Second, if the Commons Budget was conceptually similar to cost, PF should be seen as similar to investment. Third, as BOScoin is issued for investment in PF, the BOScoin community assets (the commons) increases in value to correspond with the issued volume. Finally, the Commons Budget was a model that does not consider utilization, but PF is designed with utilization at its core, and it must be implemented with that logic in mind; because without plans for future profit, there is no incentive for members to enforce PF within BOSnet.

The term "Public Financing" was created in contrast to Project Financing – the pinnacle of financial capitalism – and it is “public” in two respects.

First, the community members have the power – financial sovereignty – to make financial decisions. Here, the meaning of “public” is, not merely being invested in the public good, but closer to money being created by community consensus. Unlike for Project Financing, which is run by conventional financial institutions, the will of the community and its decisions create the credit for Public Financing. This solves the long-standing problem of “financial sovereignty”, which was examined in the introduction. Community consensus is possible because BOScoin has a governance system called the Congress Network.

Second, wealth produced by the secured real economic assets – the commons – will be considered as a community resource, from an economic perspective. Public Financing is “public” in that commons are secured through PF and the wealth created by those commons will be used for the BOScoin community. We believe that this can solve the fundamental problem of how capital and technology displaces labor income.

A PF proposal submitted by community to the Congress Network will be likely to include the purpose and expectations of the project, the size and condition of the issuance, utilization methods, as well as the reinvestment plans for a sustainable economic system. Each PF proposal will describe a concrete investment plan; however, the plan shall not include lending of money or something analogous to loan. If proposers to be included in the BOScoin network need financial support out of necessity, support shall be made free of interest. PF is BOScoin's vision, identity, and competitive strategy in the crypto market. It is also a mechanism for building an ecosystem for the Generic Trust Third Party (GTTP), a participant in

the BOScoin Network, which will be introduced in the next version of the White Paper 2.0.

In order to gain real PF experience, we plan to pilot a PF of reasonable scale and create a realistic plan. The pilot project will provide the community with a detailed process as well as data to improve the quality of decision-making before starting the Congress Network voting process. The pilot project is executed as a Reverse ICO Partner Program (RIPP) project.

Reverse ICO Partner Program

PF can be classified into several categories in accordance with its purpose: SME (Small and Medium Enterprise) PF for investment, Reward PF for community reward, Infra & System PF for building BOScoin infrastructure. Among these categories, SME PF needs to be conducted based on verification of target company's business model (BM), capability, and viability of generating synergy with BOScoin. We developed the Reverse ICO Partner Program (RIPP) to fulfill the verification objectives. RIPP will include Reverse-ICO process in which the target companies' competence can be verified. Depending on the result of Reverse-ICO, the company can be included in the BOScoin community by Congress Voting.

2.2. Congress Voting

Background

Blockchain is a protocol technology, built to be decentralized, immutable, trustless, and nonpartisan. Blockchain was thus celebrated as “governance via infrastructure”.(Sclavounis O., 2017) But even in blockchain projects, human roles exist. The creation and management of the system is done by various stakeholders in the community, which can be seen as the “governance of infrastructure”.(De Filippi, P. & Loveluck, B., 2016) BOScoin's ability to self-evolve is driven by the “people”; here, “self-evolution” consists of collective discussion and decision-making.

Every blockchain community has two layers of governance (Myungsan Jun, 2018). The consensus on the blockchain ledger operates on the principle of direct democracy. All nodes are free to participate equally, to confirm and agree on a transaction. Whether the agreement will be made by the 51% or the 67% is a matter of taste. The key idea is that all participating nodes are given equal rights and opportunities to reach a consensus. On the second layer of governance, however, early crypto projects had little to no formal mechanisms of decision-making process. If any, the mechanisms were mostly developed off the blockchain. Blockchain has its foundations in the logic of power (computational “hashpower”). Since mining is a business that is more profitable at scale, the natural logic of computational monopoly inevitably resulted in large mining operators grabbing most power and profit.(Ehram F., 2017) Other members, such as users and developers, were excluded from sharing the benefit.

The problem is not just with centralization. When the system degrades in quality or reduces the benefits to its members, members have no choice but to escape the network (either by moving to another project or carrying out a hard fork), which leads to a reduction in network effects.(Albert O. Hirschman.

1970) If all participating members have a channel to participate and make changes to increase their profits, the community will retain more members. It is also helpful for the development of the community to better understand the problem and to provide more input and solutions to problems. An effective governance system can better include and amplify the voices of its network participants.(Duncan L., 2017)

Crypto projects have recognized this and have begun to introduce various mechanisms such as Master Node voting, DGBB (decentralized governance blockchain budget), (Wiecko Robert., 2018) and equity-based voting systems. This effort has added a complementary decentralized layer to the “governance of infrastructure”. However, such a system is a plutocracy, in which those with more resources exert greater political influence. As a few wealthy individuals dominate the system, the community is likely to shift towards a model which increasingly benefits the rich. This creates a self-reinforcing system with increasing inequality of wealth and results in ordinary members becoming increasingly alienated from the value they create.

If we think that everyone on the network should be equally representative, the network must identify each individual. Without this process, it is vulnerable to a Sybil attack. Sybil attacks are attacks that create multiple false identities to wield undue influence on a P2P network. However, when collecting personal identification information, user privacy is violated. If there is no solution that can accommodate a user’s real existence without sacrificing their privacy and freedom, applying same values to the “governance of infrastructure” will remain impossible and the promises of the blockchain will grind to a halt.

Definition

BOSnet's decentralized and democratic “governance of infrastructure” will be realized through a platform we call the Congress Network. The Congress Network will be BOSnet’s fully functioning democratic decision-making body. The network will introduce a state-of-the-art encryption solution that identifies participants, ensures full anonymity, and prevents Sybil attacks. The network undergoes several levels of decision-making to maximize the wisdom of the crowd(Surowiecki J., 2005) and to compile it in the most legitimate manner, best reflecting diverse and independent opinions. Decentralization will occur on all levels of agenda setting, proposal submission, facilitation of discussion, and voting. While implementing Congress Voting on BOSnet, personal data shall be processed as described in this document and in compliance with applicable data protection laws.

Homomorphic Encryption

A complete homomorphic encryption, or homomorphic encryption, is a form of encryption originally conceived by Rivest, Adleman, and Dertouzos in 1978 and first implemented by Craig Gentry in 2009. Homomorphic cryptography differs from conventional cryptosystems in that it can operate directly on encrypted data without requiring access to the private key.(Homomorphic Encryption Standardization homepage, 2018) On the contrary, existing encryption techniques either require the private keys to be stored in the server where computations are performed, or that the data is converted from encrypted to plain-text. This causes vulnerability from a lost key or the plain-text data being leaked.

An asymmetric ciphertext

$E = (\text{KeyGen}, \text{Encrypt}, \text{Decrypt})$

can be said to be homomorphic if the following operations are possible:

Running “+” arithmetic operations on a message (other operations such as multiplication are possible)

Deriving a new ciphertext “s” by running “+” algorithms on the public key “pk” and ciphertexts “c1” and “c2”

This is accurate when all messages “m1”, “m2” return “d = m1 + m2”.

$(pk, sk) \leftarrow \text{KeyGen}(); c1 \leftarrow \text{Encrypt}(pk, m1); c2 \leftarrow \text{Encrypt}(pk, m2);$
 $f(c1, m2) = \text{Encrypt}\{f(m1, m2)\}$ (Bernhard D., Warinschi B., 2014)

Membership

In order to participate in the Congress Network, one must first obtain a Congress membership. Anyone can become a member of the parliament. Nationality and gender are not important. Anyone in the BOScoin community should find it very easy to contribute to BOSnet. Also, just as importantly as accessibility, Sybil attacks must be prevented by ensuring each identity involved in governance is unique. This does not mean, however, that it is necessary to know the full identity of everyone who participates in the system. All we need to know is that an identity belongs to a real person, who is a single, unique member of the network. Our goal is to minimize the requirements of personal information – maximize privacy – and at the same time ensure identity uniqueness. The identity account will be formed on the blockchain, and the user will get a token to prove that the owner is a unique member of the Congress Network. The account is given a public name called the ID_A.

In the short term, proof of identification such as passports will be used, but in the long term, members can certify their physical presence and uniqueness with biometric technologies such as iris scanning. The biggest advantage of this is that it is possible to match “1 to n” without using personal information such as names, state registration numbers, and addresses. (B. Thiyaneswaran, S. padma., 2012) Identity verification data is written on a biometric information repository of the Trusted Third Party (TTP) and a homomorphic hash algorithm is applied to make identity tracing impossible in the repository. All new identity verification data can then be compared to the existing database for the same or substantially similar data. If an onboarding request results in a match with the existing data, the request is rejected. The identity information is stored in a database off the blockchain and will be utilized as centralized cloud service. Although this requires a certain degree of trust in the third party, it has the advantage of scalability, and as all data is kept encrypted at all times, it can be easily secured. In addition, third-party biometric information storage services are not themselves involved in blockchain transactions or decision-making processes, so BOSnet or the Congress Network do not rely on this TTP. (Zyskind, Nathan, Pentland, 2016) Aforementioned personal information shall not be stored in blockchain and not be used in combination with account information to identify individual.

Voting

To process the vote, a voting program (public address ID_v) is created for the agenda. Each member

(ID_A) is entitled to one vote on the issue (ID_V) and is issued a single Ballot Stamp.

Requirements

1. Eligibility: System must be able to see if the voter is eligible.
2. Privacy: No one except the voter should know who voted for what. That is, it should be impossible to link a voter to a result.
3. Unforgeability: It should not be possible to forge ballots, results, or change the agenda.
4. Uncoercibility: It should not be possible to coerce or buy votes.
5. Singularity: One person has one vote. If changing one's vote is allowed during the voting period, only the last vote is counted.
6. Completeness: A valid ballot must be counted. Invalid ballots should not be counted. Results must be accurately tabulated.
7. Fairness: Voting should not be affected by the votes of others. In other words, partial counts should not affect the entire process.
8. Verifiability: Voters must be able to verify that their votes are properly reflected in the results and that all votes were fairly cast (Fujioka A., Okamoto T., Ohta K., 1993), (Çetinkaya O., Doganaksoy A., 2007)

Voting Preparation: Getting a Ballot Stamp

After the registration process, members will receive an individual wallet linked to the account module and voting program (1. Eligibility guaranteed). Personal wallets generate a one-time PKI key. ID_A confirms the voter's eligibility as confirmed during registration.

Then, members can apply for a ballot. At the time of application, a random value is sent to the voter. The voter then homomorphically encrypts it with a private key and sends it to the voting program. The voting program generates a ballot stamp based on Encrypt (RE) using homomorphic computation.

$$\text{Encrypt}(\text{Ballot Stamp}) = f\{\text{ID}_A, \text{ID}_V, \text{Encrypt}(R_E), R_A\}$$

This ballot is created in a trustworthy environment, and moreover, the voting program that generates this value can neither read the data nor associate it with any individual (2. Privacy guaranteed). The Ballot Stamp is created in the public domain, but only the voter holding the private key can use it.

Additional processes eliminate the latency between the ballot creation request and vote – creating even more privacy for the voter.

Casting votes

When a ballot is delivered to a member, the member uses his or her private key to decipher the ballot, makes a decision, and returns the ballot and decision through encrypted channels to the voting program. Since the plain-text ballot is known only to the member, a member could arbitrarily create multiple ballots and vote multiple times, and the voting program couldn't tell the difference. To avoid this and to verify that the owner of the keys signed the Ballot Stamp, the voting program sends the ballot in the form of a tag value.

$$\text{Tag} = f\{\text{sk}, \text{Encrypt}(\text{BallotStamp})\}$$

The value of “sk” is known only to the voting program, and only those who have a key to “Encrypt (BallotStamp)” can figure out the secret value. “XOR” operations or a “Blind Signature” method can be utilized for “f”, which is public. Since it is a homomorphic operation, the following examples are also possible.

$$\text{Encrypt}(\text{BallotStamp}) * sk1 + sk2 = \text{Encrypt}(\text{BallotStamp} * sk1 + sk2)$$

The member figures out the value of “sk” and sends it to the voting program along with the ballot and decision. If “sk” is correct, the voting program will save “BallotStamp”, member decision, and “sk” for future verification (3. Unforgeability guaranteed). The “sk” value can be publicized by hash before it is computed with “BallotStamp”. This will confirm the completeness of the voting program for the future.

Members can apply for a “BallotStamp” multiple times, but the system creates a “BallotStamp” with the same value each time. In other words, the user can vote several times with the same ballot stamp within the voting period; as new information comes out during the voting period, voters should be free to change their decisions. This also limits the possibility of coercion that can occur in remote voting. (4. Uncoercibility guaranteed)

Tallying the votes

At the end of the voting period, the system stores the vote results. The date and time of each vote is retained, and if the same ballot is duplicated, only the last vote counts as the final result (5. Singularity guaranteed). This process and the results are verifiable; the results are recorded on the blockchain and no valid votes are lost (6. Completeness guaranteed). Since the counting is done after the voting is completed, partial counts that may affect the vote are not disclosed (7. Fairness guaranteed).

When the result is aggregated, they are stored on the blockchain. Since members know their plain-text voting stamp, members can confirm that their votes have been taken into consideration (8. Verifiability guaranteed).

Through this process, our protocol meets all the requirements described above.

3. Conclusion

The famous economist John Maynard Keynes once said, "The difficulty lies not so much in developing new ideas as in escaping from old ones."

How difficult is it to change the perception that only central banks and existing financial institutions can generate credit? What if a crypto platform had a better credit-generating system than the current financial capitalist system? Cryptocurrency has been criticized as not being "real money" based on the argument that it is not a suitable medium of exchange, method of payment, or a store of value (due to its volatility). Besides, existing cryptocurrencies are not as good at generating credit as fiat currencies. To overcome this, BOScoin intends to introduce a credit generation system called the Public Financing (PF) system, armed with a governance structure called the Congress Network; a departure from current ICO models.

In addition, the real economic assets (wealth) secured by the credit created through the PF will be regarded as commons and utilized according to consensus. We believe that PF can solve the fundamental problem of capitalism.

In order for PF to succeed, the Congress Network must identify individuals. In order to prevent privacy violations during the process of individual identification, we plan to use homomorphic encryption for Congress Voting. This will also stop false identities from creating undue influence on the vote and prevent Sybil attacks. The process allows one person, one vote instead of creating wealth-proportional voting rights. This means that the community as a whole can participate with peace of mind and maximize the share of diverse knowledge and opinions. The Congress Network acts as a decentralized, democratic decision-making body.

In the next version, we will be explaining concepts not addressed in this White Paper. It will include the BOScoin economic model including the GTTP concept which links between BOSNet with external data. We will shift away from old ideas and propose new ones that hack capitalism in the most capitalist way. We recognize that every historic achievement was an "impossible dream" until it was accomplished. Marx, whose 200th birthday was celebrated in 2018, may seem anachronistic. However, his thoughts are constantly revisited as the various critical failings of the capitalist system surface. Although the development of capitalism has brought significant economic largesse, it has failed to solve the problems of inequality, alienated labor, and distribution.

The BOScoin project, which will lay the foundation for a new crypto economy, will contribute to innovations that will fundamentally change the world. This project aims to build a social trust system linking technological innovation to social innovation. Some global trends can be put on hold but are irreversible. The blockchain and crypto economy is one of these trends. We join this movement to participate in revolutionizing society as we know it.

Reference

- Piketty, T. Capital in the Twenty-First Century. Belknap Press, 2017.
- Brynjolfsson, E., and McAfee, A. The Second Machine Age: Work Progress, and Prosperity in a Time of Brilliant Technologies. W.W. Norton and Company, 2014.
- Brynjolfsson, E., and Saunders, A. Wired for Innovation: How Information Technology is Reshaping the Economy. The MIT Press, 2009. Cusumano, M.A. "The sharing economy meets reality," Communications of the ACM, 61 (1): 26-28, 2017. Cusumano, M.A. "Amazon and whole foods; follow the strategy (and the money)," Communications of the ACM, 60 (10): 24-26, 2017.

Congress Voting

- Myungsan Jun (2018) Blockchain Government: A next form of infrastructure for the twenty-first century. CreateSpace Independent Publishing Platform June 15, 2018 (<https://boscoin.io/blockchain-government-free-download/>)
- Slavounis O. (2017) Understanding Public Blockchain Governance. Oxford Internet Institute. Retrieved March 18, 2018 from <https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/>
- De Filippi, P. & Loveluck, B. (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review, 5(3). Retrieved March 18, 2018 from <https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure>
- Ehsam F. (2017) Blockchain Governance: Programming our future. Retrieved March 18, 2018 from <https://medium.com/@FEhsam/blockchain-governance-programming-our-future-c3bfe30f2d74>
- Albert O. Hirschman. 1970. Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States. Cambridge, MA: Harvard University Press. Retrieved March 18, 2018
- Duncan L. (2017) Thoughts on Governance and Network Effects. Medium. Retrieved March 18, 2018 from <https://blog.aragon.one/thoughts-on-governance-and-network-effects-f40fda3e3f98>
- Wiecko Robert. (2018) Understanding the Governance and Budget System. Dash Official Documentation. Retrieved March 18, 2018 from <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/8585240/Understanding+the+Governance+and+Budget+System>
- Surowiecki J. (2005) The Wisdom of Crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations. Anchor. Retrieved March 18, 2018
- Homomorphic Encryption Standardization homepage, Retrieved March 18, 2018 from <http://homomorphicencryption.org/introduction/>
- Bernhard D., Warinschi B. (2014) Cryptographic Voting – A Gentle Introduction. In: Aldini A., Lopez J., Martinelli F. (eds) Foundations of Security Analysis and Design VII. Lecture Notes in Computer Science, vol 8604. Springer, Cham, Retrieved March 18, 2018 from https://link.springer.com/chapter/10.1007/978-3-319-10082-1_7 [10] B. Thiyaneswaran, S. padma. (2012) Iris Recognition Using left and right Iris feature of the Human Eye for Bio-metric Security system. IJCA, vol 50 No. 152. Retrieved March 18, 2018 from http://www.gjimt.ac.in/wp-content/uploads/2017/11/Vijay-Kumar-Sinha_Enhancing-Iris-Security-by-Detection-of-Fake-Iris_Paper.pdf [11] Zyskind, Nathan, Pentland (2016) Decentralizing Privacy: Using Blockchain to Protect Personal Data. Retrieved March 18, 2018 from <https://enigma.co/ZNP15.pdf>
- Fujioka A., Okamoto T., Ohta K. (1993) A practical secret voting scheme for large scale elections. In: Seberry J.,

- Zheng Y. (eds) *Advances in Cryptology – AUSCRYPT '92. AUSCRYPT 1992. Lecture Notes in Computer Science*, vol 718. Springer, Berlin, Heidelberg. Retrieved March 18, 2018
from https://link.springer.com/chapter/10.1007/3-540-57220-1_66
- Çetinkaya O., Doganaksoy A. (2007) A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network, *Availability Reliability and Security 2007. ARES 2007. The Second International Conference on*, pp. 432-442, 10–13 April 2007. Retrieved March 18, 2018
from <http://ieeexplore.ieee.org/document/4159833/>

BOscoin White Paper 2.0 Writers, Advisories, and Contributors

Writer

Jonghyun Kim: CSO at BlockchainOS / Editor in Chief of WP2.0 / Concept Creator and Writer of Public Financing part

Myungsan Jun: CGO at BlockchainOS / Writer of Congress voting part

Kibong Moon: CEO at KoSAC / Writer of Congress voting

Hawon Han: Researcher at KoSAC / Writer of Congress voting

Advisory

Yezune Choi : CEO at BlockchainOS / Advisory Committee on WP2.0

Minhyo Bae : CTO at BlockchainOS / Advisory Committee on WP2.0

Joonkoo Kang : CTO at KoSAC / Advisory Committee on Congress voting

Kibae Kim : Researcher at ARIST (BlockchainOS Research Center) / Advisory Committee on Public Financing

Contributor

Soonkuk Kang : BlockchainOS Developer / Advisory Committee on WP2.0

Joonseouk Lee : Former Developer at BlockchainOS / Advisory Committee on WP2.0

Taekwon Jung : Former Researcher at ARIST (BlockchainOS Research Center) / Advisory Committee on WP2.0

Jaeoh Kim: PF Manager at BlockchainOS / Editor on WP2.0

Hojung Park: PF Manager at BlockchainOS / Editor on WP2.0 (English)

Gyuchoel Choi: PF Manager at BlockchainOS / Editor on WP2.0

Korean Editor

Joonsoo Kim Lee

English Translation

Seungwook Yeo

English Editor

Scott Matheina: Community Manager at BlockchainOS

