Proposed Classification of Blockchains Based on Authority and Incentive Dimensions

Hitoshi Okada*, Shigeichiro Yamasaki**, Vanessa Bracamonte*

* National Institute of Informatics, Japan

** Kindai University, Japan

okada@nii.ac.jp, yamasaki@fuk.kindai.ac.jp, vbracamonte@nii.ac.jp

Abstract— **The potential of blockchain technology has received attention in the area of FinTech —the combination of finance and technology. Blockchain technology was first introduced as the technology behind the Bitcoin decentralized virtual currency, but there is the expectation that its characteristics of accurate and irreversible data transfer in a decentralized P2P network could make other applications possible. Although a precise definition of blockchain technology has not yet been given, it is important to consider how to classify different blockchain systems in order to better understand their potential and limitations. The goal of this paper is to add to the discussion on blockchain technology by proposing a classification based on two dimensions external to the system: (1) existence of an authority (*without an authority* and *under an authority*) and (2) incentive to participate in the blockchain (*market-based* and *non-market-based*). The combination of these elements results in four types of blockchains. We define these dimensions and describe the characteristics of the blockchain systems belonging to each classification.**

Keywords— **Blockchain technology, Virtual currency, Bitcoin**

I. Introduction

Systems based on blockchain technology —or simply, blockchains— have characteristics of accurate and irreversible data transfer in a decentralized P2P network. Focusing on these characteristics, several government ministries and agencies in Japan have established research groups to discuss the potential of blockchain technology.

For example, in February 2016 the Ministry of Economy, Trade and Industry of Japan held a workshop on the application of blockchain technology to industry and released a report in March of the same year [1]. In April 2016, the Bank of Japan established the FinTech Center [2] and in the same month organized a FinTech workshop to examine the potential of blockchain technology, with the participation of experts from the fields of information technology, law and economy. In a similar way, many organizations are considering the potential application of blockchain technology, not only for implementing virtual currency systems, but also for use as core technology in the financial sector —in Fintech— and for use in other industry fields.

In general, virtual currencies can be classified into three types, in relation to the issuers: (1) centralized virtual currencies that have issuers; (2) e-precious metals, where the administrator issues the currency based on the reserve of precious metals, and (3) decentralized virtual currencies, which do not have specific issuers [10]. Conceptually, Bitcoin —the first blockchain system— is a decentralized virtual currency that has the following characteristics: it is an alternative means of payment that does not have the mandatory circulation of legal tender; it is versatile —its use is not limited by location—; and it has an open-loop configuration that does not place a limitation on the recipients of the payment [9]. Bitcoin implements different technical components collectively called "blockchain technology" as a mechanism to achieve an irreversible record of transactions of its currency without the existence of a trusted third party.

However, blockchain technology itself has not yet been clearly defined. One approach is to take Bitcoin as a starting point and consider its three main technical components [3]: transactions and scripts, consensus protocol, and communication network. Understanding the characteristics of the Bitcoin system is a useful approach to understanding blockchain technology and its potential. However, the same characteristics are not shared by all blockchain systems: although several altcoins —alternative coins— are based on or have a similar implementation to Bitcoin, other systems that are considered blockchains differ in the specifics of one or all technical components.

Because of this situation, there is interest in the standardization of blockchain technology. For example, in June 2016 the W3C organized a workshop to consider whether there are aspects of the blockchain technology which could be standardized [4]. In August 2016, IEEE announced the establishment of special interest group on blockchain technology, focused on standards and education about the technology [5]. Recently, a proposal from Standards Australia for a new technical committee [6] was voted on and accepted by the ISO member countries, and on October 2016 the ISO/TC 307 Blockchain and electronic distributed ledger technologies was established [7]. Similarly, other standards organizations are also considering how to approach this issue [8].

In addition to definition, there is also the issue of classification of blockchains. In this matter, there have been some proposals: a report by the UK Government Office for Science [11] provides a classification of blockchains —or distributed ledgers— based on permission regarding the use and maintenance of the integrity of the ledger. According to the report, blockchains are classified into: (1) “unpermissioned”, which anyone can use and maintain; (2) permissioned public, which anyone can use, but only trusted nodes can maintain; and (3) permissioned private, which can be only used and maintained by their owner. This type of classification based on permission for read and maintenance functions is widely used.

Another classifications considers the source of control for the permission of read and maintenance functions in the system: (1) public blockchains, where anyone can read or maintain; (2) consortium blockchains, which are under the control of a financial consortium responsible for maintenance functions and where read function may or may not be restricted; and (3) fully private blockchains, where only one entity controls the maintenance of the blockchain, although read permissions may or may not be granted [12]. This classification is limited to either the consortium or private models of control, and in the case of the latter it is considered that blockchain technology may not be the best solution.

In this paper, we take a general perspective and propose a classification of blockchains based on two external dimensions: existence of an authority and incentive to participate.

II. Dimensions of Classification

A. Existence of an authority

The Bitcoin system does not require a third party to validate transactions. Correctness is not ensured by any particular node; the requirement is that the majority of computational power in the network is controlled by honest nodes [13]. In blockchain systems similar to Bitcoin there is no need of an authority to certify the trustworthiness of a particular node or to restrict participation in any way.

On the other hand, there are blockchain systems where a trusted authority exists who has a certain degree of control over the blockchain. This control can and often manifests in the ability to grant or deny participation in the system: in some cases permission may be required to join the network at any level; in others, certain functions may be restricted and others not. For example, any node may be able to read the transactions, but only nodes that had been granted permission by the authority would be able to validate or add transactions to the record. Although some nodes in such systems may not need permission, this does not change the fact that the authority exists. And this authority could potentially exercise other types of control.

The difference between blockchains like Bitcoin and these latter type of blockchains resides in whether a trusted authority who can enforce rules exists or not. Taking this difference in consideration, we define “blockchains without an authority” as blockchains where an authority does not exist. On the other hand, we define “blockchains under an authority” as blockchains where a trusted authority exists and has power over the system.

A blockchain under an authority centralizes power in a trusted third party that can decide who to grant permission to participate in the system and for which functions. In order to make this decision, the authority has to authenticate users that wish to participate to the system. As a consequence, the identity of authorized nodes can be verified.

In contrast, in a blockchain without an authority there is no third party to grant or deny permission to participate in the system, or to authenticate participants. All participants are pseudonymous and their identity cannot be directly verified, although further analysis may reveal them [3].

B. Incentive to participate

Research on the success of the Bitcoin system has identified the economic incentives it provides as one reason for its continuance [3]. Bitcoin miners compete to create new blocks; if they succeed they can receive new bitcoins. This new currency is the reward for the role they play in the continuance of the system. For blockchain systems that have a virtual currency, this is considered to be the main economic incentive needed for participation —although miners also receive transaction fees.

However, at the current stage of blockchain technology adoption, the virtual currency that the participants of the system receive as new currency and fees is not an incentive by itself. This incentive depends an external factor: the existence of a market around the blockchain system.

The new currency reward works as an incentive because there is currently a market with a price mechanism surrounding Bitcoin and other similar systems, which will take this currency and convert it into fiat at an attractive exchange rate. Currently, speculation on the potential of these blockchain systems in the future is part of the reason why they have developed a market price.

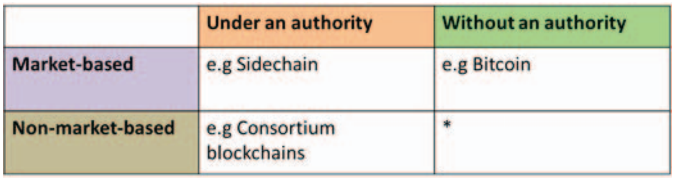
The establishment of a market for the blockchain can be contingent on many factors, such as whether the blockchain has a transferrable currency or asset, and whether or not a market can be formed without restrictions on the transfer or exchange of that currency. The liquidity or potential of the currency to function as money can also depend on the regulations that may or may not be placed on it.

If the market for buying and selling the virtual currency is established, then the price of the virtual currency can be formed. Whether there is a market that will accept the currency, and the fungibility and liquidity of that currency, are important requirements for the continuance of the system. We consider that a blockchain is market-based when market price is the main incentive for continuing participation in the system.

On the other hand, when the main incentive is other than the market price, we consider them in general as non-market based. The reasons why a market is not formed around a blockchain system can include the possibility that the blockchain does not have not an associated virtual currency. In these cases, non-market based incentives may be varied; technological or ideological reasons, fear of missing out, or continuance based on contracts or other legal obligations.

III. Blockchain Classification

The combination of the dimensions of authority and incentive results in four types of blockchains (Figure 1):



	Under an authority	Without an authority
Market-based	e.g Sidechain	e.g Bitcoin
Non-market-based	e.g Consortium blockchains	*

Figure 1 Dimensions of classification

A. Blockchains without an authority and market-based

The characteristics of not having an authority and being market-based may not be mutually necessary conditions, but they form an ideal relationship. The reason is that in a blockchain which does not receive regulation from any authority, it is necessary to have an established market that will form a price and that will receive the coinbase reward — the new virtual currency issued for mining— to incentivize the participation of mining nodes in the system.

This is particularly relevant for blockchains that implement a consensus protocol similar to that of Bitcoin. The Bitcoin system implements a mechanism based on computational complexity to ensure the accuracy of the records even if a trusted third party does not exist. In this consensus mechanism, nodes compete to find the answer to a computational puzzle [3]; the larger the computational power they hold, the more their probability of becoming the winner increases. The winner receives the coinbase reward.

The fact that a large number of general nodes from all over the world participate in mining and finding the correct answer to the computational problem means that they leave proof that a large number of computation devices —including high-performance computers— have put in a large calculation effort. However, this proof of work (POW) based consensus requires large amounts of energy and is therefore costly. This makes the fungibility of the currency important: miners rely on the price of the virtual currency to cover costs and obtain profit. If there is a market with a demand for the virtual currency and this currency has a price, then there is an incentive to produce it and to support the continuance of the system.

B. Blockchains under an authority and market-based

This type of blockchains can take advantage of the market price to incentivize the participation of numerous nodes and increase its security; at the same time, the authority can introduce a degree of control over the system. A market for circulating the currency or the coinbase reward can also be established for blockchains under an authority, as it is established for blockchains without an authority such as Bitcoin.

The main incentive is that the currency has a value and fungibility for nodes to want to join, but the characteristics of the system under an authority play an important role too. The trusted authority and additional blockchain characteristics unique to the system have to offer an additional benefits that will differentiate sufficiently from a blockchain without authority.

Sidechains [16] pegged to Bitcoin —or other blockchains that have an established market— are also one example of this type of blockchain system. Although an authority exists, a free market can still be established around the blockchain system; authorized nodes from the sidechain exist along the general Bitcoin nodes. Only the authorized nodes are given certain privileges by the authority, and they could play a special role as nodes that issue assets or as audit nodes. On the other hand, the general nodes can join the competition for the creation of new currency, with the incentive provided by the market price. If a POW consensus protocol is used, the existence of general nodes would introduce computational complexity for mining and contribute to finding the solution. The participation of more general nodes would increase the decentralization and the resistance to tampering.

C. Blockchains under an authority and non-market-based

In a non-market based blockchain there needs to be a compelling alternative incentive to join and remain in the system. Without a market surrounding it —without a price mechanism— it would be preferable for consensus to be based on some other grounds besides POW or similarly costly algorithms. Rather, it is more sensible to take an approach based on other methods of agreement between the parties that are more energy efficient compared to POW consensus. In this case, the authority can facilitate the implementation of these alternative methods by exerting control over participation in the system.

Consortium blockchains are one example of this type of blockchain systems. A consortium refers to an alliance of companies formed for a certain purpose; only limited members are able to participate as nodes. General nodes cannot participate in the system. When a consortium sets up a blockchain, it limits the participants only to those nodes that have been recognized by the authority; in this case it is not necessary or practical to rely on the competitive mining of the participating companies. A technical approach could provide a solution by implementing an appropriate algorithm instead, such as practical byzantine fault tolerance (PBFT) [14] or two-phase commit variants [15]. Another option is a legal approach that solves the problem by means of prohibiting dishonest acts through a contractual relationship. The participating companies that set up a consortium blockchain could agree on the contents of a legal relationship based on a contract. In such cases, a rational method would be to determine the order for validating the blocks in advance and validate the block by turns, using a rotation method.

However, whether such protocols can still be classified as part of blockchain technology is debatable, and they have not been tested as extensively as the Bitcoin protocol in real world settings. The consensus protocol based on POW —Nakamoto consensus [3]— used by the Bitcoin system has proved to be stable in practice since its inception, although the possibility of different types of attack still exist [3]. The same cannot be said for the closed environment of consortium blockchains, which could present weaknesses in time. Whether an optimum algorithm can be devised, which can maintain the capabilities of a blockchain even without an established market and under an authority, depends on the direction of future proofs of concept.

On one hand, these mechanisms can be more energy efficient in terms of computation. In addition, the benefit of using a blockchain for the validation of records by multiple entities in a consortium could increase confidence in those records [11]. This is true if the participants have sufficient incentive to act honestly. However, the limited participation in consortium blockchains can bring problems concerning the possibility of fraud by collusion between nodes —the Byzantine Generals problem. It is rare that an alliance of companies participating in a consortium would continue for a long time without changing its members; it is possible that there could be dishonest acts caused by the transition of participants.

Moreover, it would be necessary to change the authority settings when the participating companies changed; this would mean that a small number of privileged nodes could hold a greater authority of using blockchain technology in the first place. Less powerful entities could be at disadvantage. A rule of the majority could mean that without appropriate regulation, the majority could set rules to their own advantage. In addition, there may be ways of obscuring operation depending on the setup and making it difficult to know if there has been mismanagement. If such a disadvantageous situation were to develop, only the contract would remain to incentivize organizations to remain. Closed systems such as these would be highly dependent on such contracts and regulations, and some degree of transparency would have to be introduced, through regulators or observers.

D. Blockchains without an authority and non-market based

Without a market to provide the incentive of price of the currency, and without an authority to enforce and administrate participation in the system through contracts, the long term continuance of a blockchain becomes complicated. Therefore, this last type of blockchains are perhaps difficult to contemplate.

In its early years Bitcoin could have fit this classification. At its inception, Bitcoin did not have a market and bitcoins did not have an exchange rate with fiat. Continuance of the system was achieved partly by the ideological principles of its early adopters. However, in the end a market formed around bitcoin and a price was established. It is likely that a more efficient consensus protocol would be able to reduce the energy consumption of nodes, in turn reducing the barrier for entry to the system. However, without the monetary incentive and without the possibility of enforcing regulations, incentivizing participation would remain a challenge, although ideological, social or ethical considerations can play a part as incentives.

IV. CONCLUSIONS

Blockchain technology has received much attention for its potential on areas such as Fintech. Although the exact definition of blockchain technology remains a challenge, in this paper we have made an attempt to classify it based on two external dimensions: existence of an authority (without an authority or under an authority) and incentive to participate in the blockchain (market-based or non-market-based). The combination of these elements describes four types of blockchains, with different characteristics.

One limitation of the proposed classification is that market-based incentive is taken as a discrete factor —it exists or it does not— rather than a continuous one. In reality, the price of the currency of a blockchain is variable. In the case of Bitcoin, for example, the currency did not initially have a market for its exchange with fiat; the price for bitcoins developed over time. Here we do not identify at which exact point the price is sufficient as to become the main incentive.

There is currently no established theory with respect to the dimensions of analysis for blockchains; there is the possibility that other classifications from a different point of view may offer a superior explanation. This paper is presented as an opportunity to discuss the benefits and limitations of blockchains through a proposed classification. There are still many outstanding challenges and new technologies are always in flux; different classifications may appear depending on the evolution of the technology and future implementations, and new dimensions of analysis will be proposed. In this way, the technical characteristics of blockchains will gradually become clearer through repeated examination.

REFERENCES

[1] METI, “Survey on Blockchain Technologies and Related Services FY2015 Report,” Japan, Apr. 2016.

[2] Bank of Japan, “Establishment of the ‘FinTech Center,’” Apr-2016. [Online]. Available: https://www.boj.or.jp/en/announcements/release_2016/rel160401a.htm/. [Accessed: 12-Sep-2016].

[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 *IEEE Symposium on Security and Privacy*, 2015, pp. 104–121.

[4] W3C, “Blockchains and the Web Report,” Jun-2016. [Online]. Available: https://www.w3.org/2016/04/blockchain-workshop/report.html. [Accessed: 29-Oct-2016].

[5] IEEE, “Getting Linked to the Blockchain,” *The Institute*, Aug-2016. [Online]. Available: http://theinstitute.ieee.org/technology-topics/computing/getting-linked-to-the-blockchain. [Accessed: 24-Aug-2016].

[6] ISO, “ISO TSP 258 (Blockchain and Electronic Distributed Ledger Technologies).” Apr-2016.

[7] MEXT, “The ISO Will Start Discussion on International Standardization of Blockchain Technologies,” Oct-2016. [Online]. Available: http://www.meti.go.jp/english/press/2016/1007_05.html. [Accessed: 29-Oct-2016].

[8] M. del Castillo, “Double Standards: The Coming Push for Blockchain Interoperability,” *CoinDesk*, Oct-2016. [Online]. Available: http://www.coindesk.com/double-standards-the-push-for-blockchain-interoperability-could-get-messy/. [Accessed: 14-Oct-2016].

[9] H. Okada, I. Takahashi, and S. Yamasaki, *Kasō tsūka: gijutsu hōritsu seido (Virtual currency: technology, law, institutions)*. Tokyo: Toyo Keizai Inc., 2015.

[10] FinCEN, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” USA, Mar. 2013.

[11] Government Office for Science, “Distributed Ledger Technology: beyond block chain,” UK, Dec. 2015.

[12] V. Buterin, “On Public and Private Blockchains,” 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. [Accessed: 03-Oct-2016].

[13] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *www.bitcoin.org*. p. 9, 2008.

[14] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” in *Proceedings of the Symposium on Operating System Design and Implementation*, 1999, pp. 1–14.

[15] G. Danezis and S. Meiklejohn, “Centrally Banked Cryptocurrencies,” *arXiv*, no. February, pp. 1–16, 2015.

[16] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, “Enabling Blockchain Innovations with Pegged Sidechains,” 2014.

Hitoshi Okada is an Associate Professor at the National Institute of Informatics (NII), Japan. He got his Bachelor of Public Law (LLB) and Bachelor of Private Law (LLB) from the University of Tokyo, Japan. He completed his MA at the Osaka School of International Public Policy (OSIPP) at Osaka University, Japan. He got his Ph.D. in International Public Policy from Osaka University, Japan. His current research topic is the consumers' acceptance of IT enabled services, especially the electronic commerce services and the virtual currency systems.

Shigeichiro Yamasaki was born in Fukuoka, Japan 1957. He received the Ph.D. degree in information science from Kyushu University Graduate School and Faculty of Information Science and Electrical Engineering. He is a Professor of Kindai University.

Vanessa Bracamonte is a postdoctoral researcher at the National Institute of Informatics, Japan. She received her PhD in Informatics from SOKENDAI (The Graduate University for Advanced Studies, Japan) and holds a BSc in Informatics from Pontificia Universidad Catolica del Peru. She has previously worked as an analyst and project manager in the development of electronic commerce stores. Her research interests include trust and risk in information technology, virtual currency and consumer behavior in electronic commerce.