# Blockchain: A Pipe Dream or a Dream to Come True

Sooyoung Song*

*Preliminary*

June 12th, 2021

Korea Money & Finance Association

Haevich hotel, Jeju

* Corresponding author. Department of Finance, College of Business and Economics, Chung-Ang University. Address: Heuksog-ro 84. Dongjak-gu, Seoul, South Korea 06974. Email: sosong61@cau.ac.kr, sosong61@gmail.com. Phone: 82-2-820-5518, 82-10-3036-5645.

Previously a draft version of the current paper was presented at the *Policy Symposium on Blockchain* sponsored by the Korean Finance Association in April 2018. Usual disclaimers are applied. Since this paper is preliminary and incomplete, do not quote without permission.

Abstract

Since the frenzy of Initial Coin Offering had propelled the Bitcoin price at $18,640 in December 18, 2017, we witnessed again the unprecedented surge of the Bitcoin price at 62,926.56 on April 15th 2021. As of May 24th 2021, the price has been dropped as low as $34,259.55. Despite the extreme fluctuation of value, the backbone technology of crypto currency, Blockchain, comes in the fore such that the portent benefit from distributed ledger technology is readily acknowledged in some arenas of economic transaction. Wide adoption and frequent use of Blockchain technology, nevertheless, *a priori* requires the sustainability of consensus among users. To that purpose, most of the research in the blockchain economics by far seems to focus on the deterrence mechanism from the *ex post* moral hazard such as double spending, deviation from the chain, manipulation, and so on. Above all, immutability, though allegedly, guarantees the credibility of the record in the distributed ledger because the stored record is free of posterior fabrication. Immutability not only reduces the transaction cost since no monitoring is needed, but also works as a catalyst to maintain the consensus since no incentive for deviation. This paper, however, claims immutability is just a necessary condition but *not* sufficient condition for the consensus *at all*. Validity of information *ex ante* is imperative for the consensus sustainability. Information cannot be immaculate just because it is recorded in a block and appended to a chain. Information may turn out to be *not true* later on or some people even may have motive to record distorted information. Thus some records surely needs correction at any moment. As the incentives and motives are the key features in shaping the feature of economy under the information asymmetry, the quality of information loaded on the blockchain should vary with the users of different motives. Thus the sustainability of consensus could be undermined to the extent of *falsehood* of information, i.e. *adverse selection*. Even though the *ex post* fabrication, *moral hazard*, is blocked perfectly due to the immutability, the flawed information needs to be corrected. Then, the central authority is indispensable, which would rather facilitate the adoption and foster innovative use of blockchain technology. Thus, the efficacy of Blockchain protocol requires the following criteria; Cost efficiency (moderate seignorage), Immutability (censor free information), and Resilience (rectifiable data).

Keywords: Blockchain protocols, Consensus, Individual incentive

JEL Codes: G23, G38, and E44

# I. Introduction

## 1. Bitcoin: A Crypto currency under the BlockChain

From an enthusiastically hailed technology which entails huge innovation within the economy, the block-chain technology seems to lose the power of momentum since the price of crypto-currency price, particularly bitcoin, has been plunged from the 19,086 US$ on the 16th December 2017[1]. Since the inception, bitcoin behind the blockchain technology has been traded with the unprecedented premium as a virtual currency which could achieve a status of portent replacement of government issued currency. Initially the blockchain technology is exploited to feed on the frenzy of crypto currency such as bitcoin etherium ripple etc. through the Initial Coin Offering.

At the moment of inception, the rules of usage protocol incorporated with blockchain seem to be developed and applied by computer scientists or engineers without interventions from economists, lawyers, and regulators. Thus bitcoin, the first incarnation of self-*invented* trust without the need of central authority; allegedly core spirit of blockchain technology, cannot help but reveal its own weakness when the usage is expanded into wider social context, for example, as a currency despite the proclaimed technical prowess. When the rule of bitcoin usage is studied under the lens of economists, its limit has become clear. Also, if not coincidentally, the price of bitcoin fell steeper than it soars. To that regard, Tirole (Financial Times November 30th, 2017), among many others, warns the risk of bitcoin such that it is a pure bubble because its value is derived only from the expectation of future use by others. But he alluded the distributed ledger technology behind bitcoin could be a welcome innovation with useful applications e.g. automatic execution of smart contracts.

Observing the unprecedented high volatility of price and perceiving the danger of ingrained anonymity associated with money laundering or drug dealing, people began to feel the suspicion about the bitcoin in lieu of security and stability which are crucial features for an entity to be used as a currency. A viable currency should fulfill tasks as a medium of exchange, a store of value and a unit of value measure in an economy. As the prospect of Initial Coin Offering craze is dwindling, due to the tightening governmental

[1] https://www.coindesk.com/price/

regulation and increased wariness, the excitement over the crypto currency is somewhat weakened. Another Nobel laureate Krugman (*New York Times*, Juky 31st, 2018) ascertains that the crypto currency goes astray in light of transaction cost reduction, which is the exactly opposite of direction of evolution of medium of exchange, i.e. money. Thus it is right moment to turn around the direction of development of innovation underpinning blockchain technology other than crypto currency.

Despite the unsatisfactory outcome in an effort to replace the central bank issued currency with the crypto currency, for example, bitcoin etc., the blockchain technology is adopted to create innovations in insurance, finance, legal services etc. around the several countries. For example, insurance is quite active in developing *peer to peer insurance*, *parametric insurance* (low frequency high intensity trigger), *micro insurance* (low income people groupwise insurance for low income people), and *land registry* in Sweden, *property registry* in Georgia, *automated escrow* service with Smart contract, *ownership transfer* in stock transaction, *online voting* and so on. Among them the impact of blockchain technology on Finance is salient such that the mitigation of trust cost manifests itself in several ways within financial system.

2. Blockchain usage

As the blockchain technology is a way to record a transaction such as exchange, contract, ownership, identity, and data via connecting and creating an immutable time-stamped public ledger (Davidson et. al. 2018), it may allow us to replace the intermediary or central authority needed to assure the completion of transaction. The economic utilization of blockchain technology is apparently in the nascent stage but notably is extended to the arena of politics, in which it is adopted to replace the monitoring of ballot count that demands quite a substantial cost on the government. The very feature of blockchain technology which entails the decentralized, distributed and fabrication-free ledger record could fit well with the ballot counting process in the most political voting process.

In the meantime, the most imminent areas to be adopted are the incumbent financial sectors such that the blockchain technologies could implement automatic trigger process across the institutions and widen financial access via implementing new ways to intermediate funds, assess the real-time value and manage the risk. And yet the

infrastructure underpinning the technology is underdeveloped as was the case for the spread of internet innovation, which was accomplished through the software enhancement, computing power upgrade, and communication network expansion.

With the ever explosive public consciousness over the past years, let alone the crypto currency that the blockchain technology underpins, the blockchain hype has spawned several investment projects for a couple of years but have not delivered yet the fruitful outcome. To our disillusionment, the blockchain has been changing itself so as to become usable in finance, which is much less than what it was supposed to change everything. Thus, in the practical business as well as academic fields, two diverging views flow side by side such that some alludes the blockchain technology a pipe dream, belief system or crypto skeptic on the one hand and others claim

Overall the blockchin technology is believed to have a real portent to be a catalyst to invoke a change in the world of finance but it is too early to argue it will change economy and everything (Casey et al 2018). As recently as Abadi and Brunnermeier (2018) focus on the economic role of ledger in record keeping, to some devotees, Blockchains, a particular type of Distributed Ledger Technology (DLT) , could be as effectual as the invention of double entry book-keepings in fourteen-century *Banco-di-Medici* in Italy. But they point out the clear limitation which postulates the tradeoff features inherently present in the ledgers, which are correctness, cost efficiency and decentralization.

In this paper, regardless of diverse or sometimes conflicting definition and description blockchain technology so far, a definition of blockchain technology offered in Cong and He (2018) is adopted. Cong and He (2018) propose two arenas of research on blockchain: one is mechanism that generates and maintain consensus, the other is economic outcome that blockchain functionality provides. Albeit the diverse and huge impacts are anticipated for firm structure, industrial organization, corporate governance, or legal edifice, the blockchain-invented ledger mechanism should or could assure us of the reliability, first of all, before the widespread adoption and consequential use of blockchain functionality. Thus the crucial aspect of blockchain technology lies in the mechanism of how to nurture and sustain the consensus among participants. As is agreed on, consensus enables agents with divergent perspectives and incentives to engage in transactions in efficient way as if the truth persists, which has profound implications on the functioning

of society, including ethics, contracting, and legal enforcement, among others. Thus it is natural to focus on the issue of persistency of truth in light of information asymmetry.

## 3. Blockchain with Information asymmetry

Information asymmetry entails a loss of efficiency and consequential transfer of surplus that are borne by the party who would like to distinguish herself in the form of cross subsidy or costly signal. Thus, of interest are whether the consensus is sustained under the protocol incorporated in the blockchain technology in the face of incentive problem to exploit the environments of information asymmetry.

As the blocks are created and linked to the chain as an information storage appended to build up an auditable database, they are equivalent to the contracts as long as they are to be used for economic transaction. Then they are inevitably subject to the incentive problem. The advocates of distributed ledger technology, however, claim that the immutability feature could eliminate an incentive to fabricate, manipulate, or violate the contract later on due to the immense costs incurred. That is, as the contracts are recorded on all the blocks appended and linked to formulate a chain, the cost becomes too large to manipulate. In the parlance of information asymmetry literature, the agent is deterred from the pursuit of undesirable behavior with which the contract incurs more cost to the agent. This construct in relation with the blockchain technology conforms to the moral hazard model, which entails hidden behavior occurring after the contract becomes effective. Therefore when the blockchain technology advances the immutability as a way to assure of the persistency of truth, it deserves examination of whether the feature guarantees the elimination of hidden behavior even though the protocol *technically* enables the alleged security and immutability of ledger to assure of trust among participants.

As the blockchain system relies on the distributed ledger technology, it is noteworthy that the distributed ledger implies the diffused information and in conflict with *privacy*. Transparency may give rise to the unintended revelation of private information to be exploited otherwise protected from misuse or abuse. To the extent of the distributed ledger system relies on the diffusion of information, the inherent tension between privacy and transparency is inevitably increased. To overcome this conflict, zero-knowledge proofs are devised and implemented but is in the pilot stage (Narula et. al., 2018).

Furthermore the transparency, allegedly realized via the distributed information through the ledgers, does not *necessarily* assure of the quality of information *ex ante*. According to the literature of blockchain technology dated back to when the merkle tree (Merkle 1988) is contrived, the merkle tree can detect the fake or altered block and verify the information stored within the block. Then, we still need a criteria assessed against the truthfulness of information. Despite the truthful criterion is available, the quality of information conveyed in the block may turn out to be wrong even after the block is appended to build up a long blockchain. Hence the adverse selection is unavoidable at the time of contract offering. The information conveyed in the block was a truthful one at the time of blockchain formation given the available criteria at the time of contract. Then, if the criterion turns out to be a wrong one later, the blcokchain may not maintain the consensus. Within the construct of distributed ledger system, the more robust data verification is, the wider sharing of information is required. This personal incentive conflict becomes salient in the transparency and privacy as to the medical records particularly for the insurance industry. When each participant's node had access to only a subset of data, the balance between transparency and privacy musters a fundamental question against the viability of the system for such uses once its core and defining feature is restrained.[2]

The recent analysis and discussion of blockchain technology largely focuses on the core functionality of blockchain which lies in *a posteriori* maintenance of consensus among the participating agents whether it is achieved through *a priori* communication and commitment or not. In spite of the moral hazard or adverse selection, which are presumably postulated due to either the information asymmetry or the incompleteness of contract, the blockchain technology based system may or can retain the trust worthiness, resilience, and cost efficiency. That is, can it survive the individual incentive to exploit the engaged transaction through persuasion, pretense, deception, misrepresentation, falsehood, and hypocrisy because of the envy, anxiety, anger, jealousy, sympathy, and so on, when honesty surely is not the characteristic that prevails in our economy.

---

[2] See Not There Yet': Bank of Canada Experiments with Blockchain Wholesale Payment System,"by Maureen Gillis and Alexandru Trusca, CyberLex, June 20th, 2017,

The rest of paper is as follows. The evolutionary change of blockchain technology into the several different shapes from the conventional definition of blcokchain is expounded. Then a new trilemma model for the ledger to be useful is set forth and analyzed under the presence of individual partipant's incentive to pursue his own benefit at then expense of others. Potential arenas for the usefulness of the blcokchain technology are considered and policy implication is discussed in light of regulation. Then, conclusion follows.

## II. Literature on the Blockchain definition

As the public consciousness is clearly enhanced due to the overhyped phenomena of bitcoin price change, blockchain technology was already conceived, developed, adopted and used among the computer science researchers working on the operational algorithm of distributed network, for example, software company computer network or internet (Narayanan and Clark 2017). They are fully aware of the consensus problem latent in the distributed network system, aka byzantine paradox.

Arguably, the first incarnation of blockchain technology is bitcoin (Perry 2018). The first use of distributed consensus mechanism is proposed in the bitcoin through which the self-interested participants are compensated for validation of the transaction. With the use of bitcoin, the participants can be convinced of, without any further confirmation, the updated history of transaction recorded in the block. The consensus algorithm developed to validate the records in the distributed ledger, that is, blockchain is the proof-of work protocol which entails computational cost incurred to the miners engaged in competition. Since then the applications of blockchain has flourished platform financing through initial coin offerings as well as plethora of smart contracts featuring payments triggered by tamper-proof consensus. As a result, blockchain is delivered as an innovative and clearly defined technology when we observe countless blockchain explainers in text, audio, and video around the web.

Contrary to our notion, however, there is no universally accepted definition of a Blockchain (Jeffries, 2018). To our surprise, there is widespread disagreement over which qualities are essential in order to call something a blockchain. In an effort to develop a blockchain terminology standard for the International Standards Organization, *Victoria*

*Lemieux* in Jeffries (2018) points out that

> "*In general, if the transactions are gathered together in blocks, and it is blocks that are secured on the chain using cryptography, and it is designed to be tamper-resistant and produce immutable records, the system qualifies as a blockchain. That said, in general usage, blockchain is often a term that encompasses a broad range of distributed ledgers, even if transactions are not organized into blocks*."

From the legal perspective, the Walch (2017) is concerned about the messy implication delivered along with the definition of blockchain when Arizona's Electronic Transactions Act was amended in 2017 to clarify that it covers transactions done on a blockchain as a legislature in the state of Arizona.

> *"Blockchain technology means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth."*

Walch singles out the words particularly *immutable* and *uncensored truth* which are totally independent of the blockchain technology. First, no censorship does not guarantee the truth of data at all. Inaccurate data, such as a wrong diagnosis on a medical record, can still be validated and remain uncensored in a blockchain as long as the anonymous users maintaining the network, who may include miners, developers, or villains, want it to be. Secondly, the immutability, if ever, forbid the users from correcting her own data when the data are inaccurately recorded. Thus, it is necessary for the users to delete the data in effect without interrupting the remaining correct data.

Three crucial components in blockchain technology are *hash pointer* which links blocks with chain, *timestamp* which secures proof of document time like a dashboard cameras, and *transaction data* which are suitable for recording of events, medical records and records management activities such as identity, transaction processing, provenance, and traceability. When these three components are combined to produce a chain a ledger, the chain must be trusted among the participants. Conventionally the participants involved with the transactions are assured of the trust on the ledger by the central authority such

as government, intermediary, and central counterparty. However, with Blockchains, the participants rely on specific protocol that secures the consensus without the central authority on the distributed ledger. Until now, the salient protocol is the proof-of-work used in the bitcoin whereas the proof-of-stake and the proof-of-concept are adopted and used in a certain arenas.

## III. Consensus maintenance mechanism with Permissionless Blockchain

In order to facilitate the remote commercial transactions between the economic agents, the agents are assured of the quality of information recorded in the ledger before it is transferred. That validation should be obtained under the consensus free of distortion. Historically, the participants relies on the central authority, e.g. the state or its delegates in order to reach a consensus among them. But the agreed upon trust could be betrayed by the central authority by accidental misfeasance or by intentional malfeasance. Thus the distributed ledger technology, permissionless blockchain, is developed to overcome the aforementioned mishap or distortion by the dispersed records through the network.

For the distributed ledger technology to be successfully adopted to the practical economy, it is quite crucial for the individual block holders to keep an incentive to maintain a single designated blockchain when the blocks are mined, validated and connected into a blockchain. As mentioned earlier, the central authority could validate the block to be connected to the chain under the consensus among the participants. Under the distributed ledger construct without the central authority, among the validation protocols so far considered to be practical are the following three processes: proof-of-work, proof-of-stake, and proof-of-concept.

### 3.1. Proof-of-work

Already introduced in the bitcoin offering in 2008, the proof of work is currently the most widely known protocol in the blockchain technology. In Nakamoto (2008) he contrives proof-of-work protocol in order to randomize the validation among the participants rather than majority voting, because the majority voting would be susceptible to the potential monopolization of mining blocks. Consequently, the upwardly ratcheted cost of mining block is integrated within the process.

In line with Nakamoto (2008), Biais, Bisière, Bouvard and Cassamata (2018) demonstrate the features of strategic equilibria that the blockchain protocol of proof-of-work entails under a framework of coordination game, upon which the blockchain is built as a decentralized recording commercial transactions and asset ownership. In conclusion, the presence of information delay and software upgrade could lead to the multiple equilibrium strategies in creation and retention of blockchains among the participants. They demonstrate that coordination motives could lead to creation of new blockchain, i.e. *hard fork* whereas the continuous production of a robust consensus is the key to the success of blockchain. This could jeopardize the stability and immutability of transaction history recorded in the blockchain if vested interests entails multiple active blockchains, i.e. coexistence of several blockchains. As is the case in the coordination game, the prior communication cannot assure of the coordination among the participants.

Another aspect of concern is derived from the inherent incentive mechanism built in to avoid the emergence of governing entity. Initially the mining cost was cheap but the computing facility of mining incurs the negative externality over the expansion of blockchain, even 300 kwh consumption of electricity on average for the bitcoin transaction. This substantial externality in lieu of excessive computing capacity and consequential green-house effect due to the consumption of electricity leads to the alternative protocol, proof-of-stake.

### 3.2. Proof-of-Stake

Though ingeniously devised, Proof of work protocol has neither effectively nor efficiently fulfilled designated task eventually. It has been adopted for a mechanism to maintain the consensus among the bitcoin users but in practice we have even observed emergence of different blockchains and their persistence. These occurrences reassure the caveats of protocols which were demonstrated theoretically in the study that the proof-of-work protocols are susceptible to the individual's incentive to keep vested interests or to delay the information dissemination in order to exploit the coordination failure. In addition the proof of work generates endogenously negative externality because of the ever increasing mining cost. Thus an alternative mechanism, proof of stake is considered and elucidated whether it could overcome the hurdles invoked in the proof of work.

In hopes of devising a non-exorbitant permissionless blockchain, the proof of stake entails

the removal of competition and random selection of stakeholder who is endowed with the right to get the block and update the blockchain. Therefore the larger stakeholder is the more likely to be selected, who incurs more cost with the delayed update of blockchain. Despite the lack of competition, the larger stakeholders are incentivized to maintain the consensus via updating the blockchain since it could reduce the risk of delay. However, the developer is reluctant to adopt the PoS since it is subject to the Nothing-at-stake problem.

A participant without any stake in the incumbent blockchain, though with least odd, can be selected to get an offer the right to update the blockchain, i.e. he lacks incentive to attach a new block to the incumbent blockchain since he has no stake. Saleh (2018) claims that, via restricting updating ability to large stake-holders with the modest level of reward for the sustained consensus, the permissionless blockchian is viable without the central authority.

Ingenious as Saleh's idea looks, his scheme, however, inevitably leads to the monopolistic status of a stakeholder eventually. Once the stake surpasses 50% of blocks, a single majority stakeholder could make the worst of his unfettered authority to *not* update the incumbent blockchain but create a new one while threatening the remaining dispersed stakeholders to pay for the reward, actually ransom, who have kept valuable records of transaction in the incumbent blockchain.

This sort of threat could be a real and substantive one even at lower than 50% of stakes. We have observed often the significant damage incurred on the corporations due to the moral hazard committed by CEO in spite of the small ownership. Hence, the protocol, PoS, has its own defect to be a sustainable and credible mechanism for consensus, because it is evidently susceptible to the individual's incentive at the expense of minority stakeholders.

### 3.3. Proof-of-Concept

Other than the two previous protocols, the proof-of-concept rather attracts the interests of fintech related industries as well as crypto currency related arenas. A renowned fintech firm, R3 has conducted the development of international payment systems together with twenty two biggest banks including several central banks worldwide. Despite a number

of pilots and proof-of-concepts of the blockchain technology, the verdict is well illustrated in the report that the blockchain is not yet mature enough to take over the role of world's largest payment system.

According to the report by Lynsey Barber in City A.M. on 26th October 2017, analysts at the investment bank Berenberg partnership, claim that there are currently only two large disruptive blockchain successes: cryptocurrencies, and initial coin offerings (ICOs) so far, even though they identified promising areas of blockchain use in the future were insurance, supply chain, and logistics and energy markets. Thus the proof-of-concept is still needs progress even at the pilot stage of application.

Once hailed technology faces difficulties in implementation at the pilot stage, particularly in banking arenas such as settlements and clearing, trade finance, securities and interbank payments. This calls for the modification or evolution of blockchain technology to be implemented properly within the surrounding environment. Consequential adaptation of blockchain technology to the needs and requirements of banking and capital markets leads to the fundamental change of attributes e.g. from distributed ledger to shared ledger.

3.4. Yet elusive protocols are with Blockchain

Recently the technology is modified into a chain without individually autonomously validated block, operating in a permissioned environment, with a centrally authorized database of recorded transaction. As a shared data base, the blockchain is expected to process the payment, settle the transaction, and update (clear) itself in real time under the computer algorithm without the verification of third party. Eventual validation of performance still needs a central authority who is in charge of maintaining the consensus among the participants in order to take care of the unexpected faulty situation.

The blockchain technology hype may have spawned many intriguing projects but ends up with no substance in light of economic progress let alone the productivity paradox. Walch (2018) exemplify how a misconception of a simple use of hash tag among the less technical observers becomes a source of plethora of overhyped adoption attempts of blockchain technology at the national level.[3] This prospect is quite different from the

[3] Dave Birch (2017) claims the argument that the Estonian national identity scheme uses

landscape with which the enthusiastic advocates predict blockchain technology would bring us.

## IV. Can a Blockchain be the Ledger of last resort?

Popular consciousness about the blockchain obviously started with the frenzy of bitcoin. Bitcoin, an incarnation of blockchain technology, converts the secure ledger for recording all previous payments transactions in a currency to be used for a trade. Thus bitcoin blockchain works as if it were a bank note with a long list of transaction records used as a medium of exchange.[4]

Although many central banks are looking into issuing digital currencies, the conclusion of many of the biggest - including the European Central Bank, the US Federal Reserve and the Bank of Japan - has so far been that blockchain technology is not yet mature enough to power the world's biggest payment systems. German bank Berenberg last week wrote in a report that blockchain was an "overhyped technology" that faced important

---

a blockchain is totally a myth. Even if many arguments in the similar vein have been advanced, taken for granted and circulated as if a true one in the news, speeches, and articles by the practitioners and academicians, Estonian electronic identity system relies on the use of hashes to protect the integrity of data in the Estonian system, which was launched in 2002 quite earlier than the publication of Nakamoto (2008).

[4] As far dated back as in 10th century in Tang Dynasty of China, a promissory note labelled as Jiaozi (交子: literally 'A Thing for Exchange') was issued by the private merchant enterprises and commonly used among the merchants for a large denomination payment and settlement of trade. In 1024, the succeeding Song Dynasty government takes over the issuance of Jiaozi converted to the standard government notes with smaller and fixed denominations. The notes contain the records of coin equivalent amount owed, issuer name of merchant, serial numbers, and stamped with six different inks and multiple seals like a form of registered security to combat the counterfeiting. Due to the inflation caused by over-issuance of Jiaozi relative to the copper reserve to finance a war expense against Jin dynasty, a new paper currency Huizi (会子: literally 'A Thing for Assemblage') was officially issued by the Ministry of Revenue in 1160. Then Jiaozi has remained in circulation along with Huizi until 1256 when the leftover of Jiaozi is replaced with Huizi. Huizi was replaced by the Jiaochao (交鈔: literally 'A Copy for Exchange') under the following Yuan Dynasty. Jiaocho is neither backed nor exchanged for the reserve silver so that it is deemed the first genuine fiat money. Paper currencies are used under the Ming Dynasty until 1450 when the paper currency is banned due to the inevitable hyperinflation. Since then, Sycee (細絲: Fine Silk), privately minted silver or gold ingot currency, is used along with coin and Cowrie Shell for the local exchange until the collapse of Qing Dynasty.

challenges, pointing out that there had so far been very few success stories, despite a huge number of pilots and "proofs of concept" of the technology.[5]

Though the bitcoin clearly fell short of the devotees' aspiration to replace the incumbent currency despite a few futile attempt, the blockchain technology became the focus of popular attraction with its ability to store and execute computer programs on it. It had given rise to several applications such as smart contracts enabling payments triggered by tamper-proof consensus on contingent outcomes emerged in various forms in business and financial services e.g. insurance, escrow service etc.

Regardless of the genuine definition of blockchain technology, the current paper sheds light on whether the blockchain mechanism can generate and maintain a sustainable consensus for the products in whatever forms such as identity, property rights, registry, currency, token, medical record, legal documents, food stamp, financial instruments (e.g. securities, bank notes, derivatives, insurance policies). Hence blockchain technology encompasses several features that interact with dispersed record keepers. Blockchain related technologies so far developed are purported to keep the ledger with *trustworthy information*, *immutable data*, and *efficient maintenance* so as to facilitate and deliver economic transaction free of delayed validation, costly verification, and ephemeral consensus.

Blockchain innovation is aimed to enhance the economic transaction in finance, trading, verification, certification, such as remittance, payment, clearing. These environments lend us a model of blockchain innovation under a setup of adverse selection

### 4.1. A Simple Adverse Selection Model

Recent pilot tests in relation to the blockchain technology are mostly focused on the enhancement of service qualities and operational efficiency in lieu of promptitude of response and execution. Once hailed as a comparable harbinger of the previous industrial revolution, the blockchain technology, at the current stage, looks an innovative technology that improves the performance of institutions, assets in place though it has not

---

[5] See Lynsey Barber (26th October 2017) 'Is blockchain overhyped? Analysts at investment bank Berenberg thinks so' *http://www.cityam.com/274646/blockchain-overhyped-analysts-investment-bank-berenberg*.

materialized yet the outcome. As is entitled in the Geneva reports on the world economy 21 (Casey et. al. 2018), the impact of blockchain technology is alluded as a catalyst for change in lieu of performance enhancement of the existing assets or institutions, which is succinctly coherently addressed in the following model.

In an economy, there are two participants, consumers (users) and suppliers. The consumers generate and enjoy the benefit from the contracts, services, and information derived from the existing institutions and assets in place, which are supplied by the suppliers. The institutions or assets in place comprise a system which is supplied by the private firms, the public organizations, and the government at the cost of lump sum investment $I$.

Upon the use of system, the consumers can generate the total surplus benefit $R$ in the case of successful fulfillment and 0 in the case of failure in the future. With successful fulfillment, the consumers can enjoy the net benefit of $R_c$ when the residual, $R - R_c$, is paid back to the supplier to compensate the lump sum investment[6]. But in the case of failure, both consumers and suppliers end up with 0. Thus, the consumers are assumed to be subject to the limited obligation as much as the limited liability of shareholders. Also, the consumers and suppliers are risk neutral such that both are assumed to be an expected net benefit (or social surplus) maximizer. Discount rate is normalized to be zero.

The consumers are one of the two types: *good* or *bad*. Both types are assumed to make efforts to fulfill the obligation deliberately when they are engaged in the use of the system such as contract issuance, remittance, payment, settlement and clearing, insurance and so on. They, however, are destined to different probability of fulfillment due to the contrasting motives, or inherently different traits, or unexpected mutation of features. Thus a consumer can be of good feature with probability of $\alpha$ and of bad one with $1-\alpha$ or equivalently a society is consisted with good consumers and bad ones with the corresponding share of $\alpha$ and $1-\alpha$ respectively.

A good consumer fulfills her obligation with probability $p$ whereas a bad consumer has probability of fulfillment with $q$ assumed to be smaller than $p$. Facing the asymmetric

[6] This payback can be interpreted either as taxation if the system is supplied by the government or as fee if by the private firms.

information as to the consumer types, the suppliers of the system cannot tell the good $p$-type consumer apart from the bad $q$-type one at the time of decision making in investment. Hence the supplier cannot but rely on the expected probability of positive net benefit at investment decision as follows.

$$m = \alpha\, p + (1-\alpha)\, q$$

The expected net benefit of the good consumers is assumed to be always positive such that $0 < pR - I$ where $0 \leq q < p \leq 1$. The good consumers can bring about the positive net benefit i.e. social surplus through the use of existing system but due to the presence of bad consumers, the two subcases are possible, which should be treated separately;

$qR < I < pR$ where the bad consumer's net benefit is negative

$I < qR < pR$ where both types' net benefit is positive.

4.1.1. Symmetric Information

If the types are known and identified by the supplier, the supplier can set the fees or taxes separately such that the benefit for the consumers are $R^G{}_c$ and $R^B{}_c$ for good type and bad type respectively. In order to induce the investment, the suppliers compete with each other to reach the zero profit or satisfy *non*–negative deficit for the government.

$$p(R - R^G{}_c) = I$$

If $qR < I$, the suppliers do not allow the bad consumers to participate and use the system. If the bad consumers insist on the participation, the supplier must set up the negative benefit for the bad consumer $R^B{}_c < 0$ because the supplier is subject to the zero profit constraint, that is, if $q(R - R^B{}_c) = I$, then $qR^B{}_c = qR - I < 0$. So the negative benefit implies higher fees or higher tax for the bad consumers and consequently the bad consumers are effectively deterred from using the system.

If $qR > I$, the suppliers set up the net benefit for the bad consumers $q(R - R^B{}_c) = I$ where $R^B{}_c > 0$. Then it is clear that $R^G{}_c > R^B{}_c > 0$. Thus both types of consumers come into and use the system to generate the positive social surplus.

If bad consumers are identified, they are effectively banned from using the system and the expected net benefit is $pR - I$ and the investment for the system is always launched

without hesitation. However, under the asymmetric information, the supplier should weigh the expected benefit against the investment such that $mR - I > 0$.

4.1.2. Asymmetric Information

If the suppliers cannot tell apart the good types from the bad types, the menu of contract offered under the symmetric information is not robust, since the bad consumer could easily pretend to be a good consumer and receive the net benefit higher than his true type net benefit. Under the limited liability condition in the case of failure, whatever benefit share $R_c$ for the consumer is offered, the bad consumer is better off not to reveal his type because the expected net benefit for the bad consumer is always increased when he mimics the good one. As the benefit share for the consumer is *non–negative* $R_c \geq 0$, the supplier's expected net benefit is therefore on average:

$$\{\alpha\, p + (1-\alpha)\, q\}(R - R_c) - I = m\,(R - R_c) - I$$

*No investment*: If $mR < I$, which can occur only when $qR - I < 0$, no investment is made at the first hand. Let $\alpha^*$ denote the portion of good consumers out of the population which makes the investment equal to the expected benefit of system in place $m^*R - I = 0$. Then,

$$\alpha^*\,(pR - I) + (1-\alpha^*)\,(qR - I) = 0$$

Thus, if $\alpha < \alpha^*$, the expected total net benefit, *present value* of investment, is negative.

$$\alpha\,(pR - I) + (1-\alpha)\,(qR - I) < \alpha^*\,(pR - I) + (1-\alpha^*)\,(qR - I)$$

$$mR - I < 0$$

If the good consumers' share in the population is too low, the investment cannot be made and the economy is subject to the under investment. Therefore the good consumers suffered from the lost net benefit otherwise available to them. The sufficient condition for the investment is $mR \geq I$ or equivalently $\alpha \geq \alpha^*$ for the institutions or assets in place to operate continuously within the economy.

*Investment and Institutions in place*: if $mR \geq I$, the suppliers set up the net benefit $R_c$ to the consumers so that they break even on average.

$$m\,(R - R_c) = I$$

Both types participate in the system and eligible for the net benefit reward $R_c$ since the

supplier cannot distinguish the consumers. The expected net benefit for the consumers are $pR_c$ for the good type and $qR_c$ for the bad type respectively.

$$\alpha \{ (p R - I) - pR_c \} + (1- \alpha) \{ (q R - I ) - qR_c \} = 0$$

Under the breakeven condition, a unique case is when the expected net benefit for the good type is less than her contribution; $p R_c < p R - I$ and the reward for the bad type exceeds his contribution; $q R_c > q R - I$. Thus the cross subsidization is realized even though the supplier ends up with the loss at the use of bad customers such that $q(R - R_c) - I < 0$.

Of interest is the loss incurred by the asymmetric information, *adverse selection*. Two subcases are considered

*Bad types with positive contribution,* $qR > I$ : If both types contribute the total benefit of the system, that is, $pR > I$ and $qR > I$ , then there is no net loss of total benefit despite the cross–subsidization through the transfer of benefit from the good types to the bad types. But from an individual point of view, the adverse selection cost is borne by the good type as follows. The total surplus with both types in an economy is $mR$, or the net total surplus is $mR - I$.

$$m R = \{\alpha p + (1- \alpha) q\} R = [1- (1- \alpha) \frac{\Delta p}{p}] p R \text{ where } \Delta p = p-q.$$

*Bad Types with Negative Contribution,* $qR < I$ : As the net loss of total surplus occurs when the bad type consumer's contribution is negative, $q R - I < 0$ but still $q R_c > q R - I$ . This implies overinvestment at the expense of reduced total surplus, which is *pareto* inferior allocation. Then the inefficiency cost of *adverse selection* is measured as follows.

$$(1- \alpha) \frac{\Delta p}{p}$$

In lieu of Morris and Shin (2002), decentralized decision making in market environments cannot be relied on to rule out inefficient outcomes, so that there may be room for policies that mitigate the inefficiencies. Agents overreact to public information, and hence any

unwarranted public news or mistaken disclosure may cause great damage. A growing part of the economy may be starting to act like a financial market, with all that implies—like the potential for bubbles and panics as is the case for the bitcoin. One could argue that far from making the economy more stable, the rapid responses of today's investors make their investment in the exotic software vulnerable to the kind of self-fulfilling optimism and pessimism that used to be prevalent only for investment in paper assets. As the digitalization continues, the heightened sensitivities of the financial market extended to the digital assets could magnify any noise in the public information to such a large extent that public information ends up by causing more harm than good. If the information provider anticipates this effect, then the consequence of the heightened sensitivities of the market is to push it into reducing the precision of the public signal through the flawed information loaded in the blockchains.

### 4.2. Ground for the Jury's Verdict

Despite portent use of blockchain technology to the benefit of economy, enthusiasts for cryptocurrency and/or blockchain, the concept that underlies it, continue to pay huge sums for digital tokens, e.g. Bitcoin, Etherium, Dogecoin, and so son. Like a self-fulfilling prophecy, the rising prices keep drawing new investors. This must be a Ponzi scheme that goes on as long as Bernie Madoff ran his scam fund for two decades and might have gone even longer without financial crisis in 2008. To be a long-running Ponzi scheme, the crypto currency needs narrative that convince the crypto boosters as well as others with arcane terminology and revolutionary new technology. However, blockchain is pretty old idea that has yet to find compelling uses. Also, there is libertarian assertions that buttress the belief in the crypto currency. Considering the durability of gold as a highly valued asset, I think the crypto currency could live on for a long period. However, the fact that blockchain technology could achieve any meaningful economic role to the benefit of people, is totally irrelevant to the longevity of crypto currency achieving the similar status gold holds.

As the blockchain technology is of use and value, it should contribute common good, otherwise, the benefits go to an individual at the expense of society. Particularly, though the total surplus of benefit for the society is worth pursuing in the utilization of

blockchain technology, as the current model suggests, the good type people cannot but bear the burden of subsidization cost.

Nakamoto (2008) argues that the blockchain protocol (proof-of-work) ensure the stable consensus of the block chain, *i.e*. a single chain as long as the miners attach its own current block to the most recently solved block, which is dubbed as the *Longest Chain Rule*. According to the folk theorem that persists among the Blockchain advocates, without friction, the information is disseminated instantaneously in the network and then a single *longest* blockchain is assumed to prevail. Miners, however, may discard the last block and could chain his block to the previously solved block. Then, a fork chain starts.

## V. Overcoming the Huddle

Trillemma has been proposed by Abadi and Brunnermeier (2018). Three crucial features that determine the feasibility of consensus are cost efficiency (seignorage should not be too burdensome), immutability (free of censorship) resilience (rectifiable).

### 5.1. Dilemma of DLT

Anonymity and Decentralization may lead to coordination failure and externalities. Private blockchains can restore coordination and internalize externalities, which muster a centralized authority. We, nevertheless, may still face the counter incentive for a larger than 51% stakeholder (either with monopoly or under collusion) to create a fork and destroy the extant chain at the expense of minority stakeholder despite the random assignment of block appending. Presumably the very benevolent dictator over the blockchain is necessary to assure a single block chain under full consensus. His study reminds the oligopolistic collusion which could assure the consensus, but which freeriding incentive is *non trivial*.

### 5. 2. Why is the Distributed Ledger Technology hailed so far?

Many beneficiaries are well-to-do individuals or Fortune 500 companies. User driven innovation in 1970s. Open source software development in 90s. Resurrection of Aborted Ideology *A Free-market monetary system* with Anonymity and Decentrality

> Hayek (Gold and Monetary Conference 10 Nov. 1977) "*discovered that I had opened a possibility which in two thousand years no single economist had ever studied. There were quite a number of people who have since taken up and we have devoted a great deal of study and analysis to this possibility.*"

He allegedly claim that *A free-market monetary system* in which the competitive system drive out the bad money, achieve the neutrality of money against the inflation, and attenuate fluctuation of business cycle, which was lucidly criticized by Sraffa (1932) and Kaldor (1942). Davidson et. al. (2018) argues that the emergence of DLT lead to *Institutional Evolution to the Capitalism* which entails DAO (Distributed Autonomous Organization) or DCO (Decentralized Collaborative Organization) as a new order of Economic Institutions of Capitalism. If a government is believed to behave reasonably only if it is forced to do so, an individual can never behave more reasonably than forced to do so. Central Authority Institution such as Fed, ECB etc. has performed quite well in the aftermath of the *Great Recession* since 2008.

5.4. Tradeoff *between* Speed *and* Verifiability with the Blockchain

1. As the *cryptographic* verification slows down the transaction, a single globally distributed blockchain e.g. Etherium would never be useful for the financial industry who needs faster and more efficient process particularly in the algorithmic trading.

2. Blockchain could not readily replace an *incumbent* universal protocol such as TCP-IP or HTML until the remote future.

3. Contrary to the optimistic notion, the *financing* activities are severely hampered by the lack of central authority, because the use of blockchain is equivalent to the pledge of 100% cash collateral for every financial transaction. To that regard, the liquidity services are contracted rather than expanded to the extent of which the non-secured short-term loans such as CP are not viable. Then this sort of *feature* (or *bug*) could affect the P2P online lending as well as the shadow banking.

New Trilemma

Cost Efficiency: Net cost reduction matters

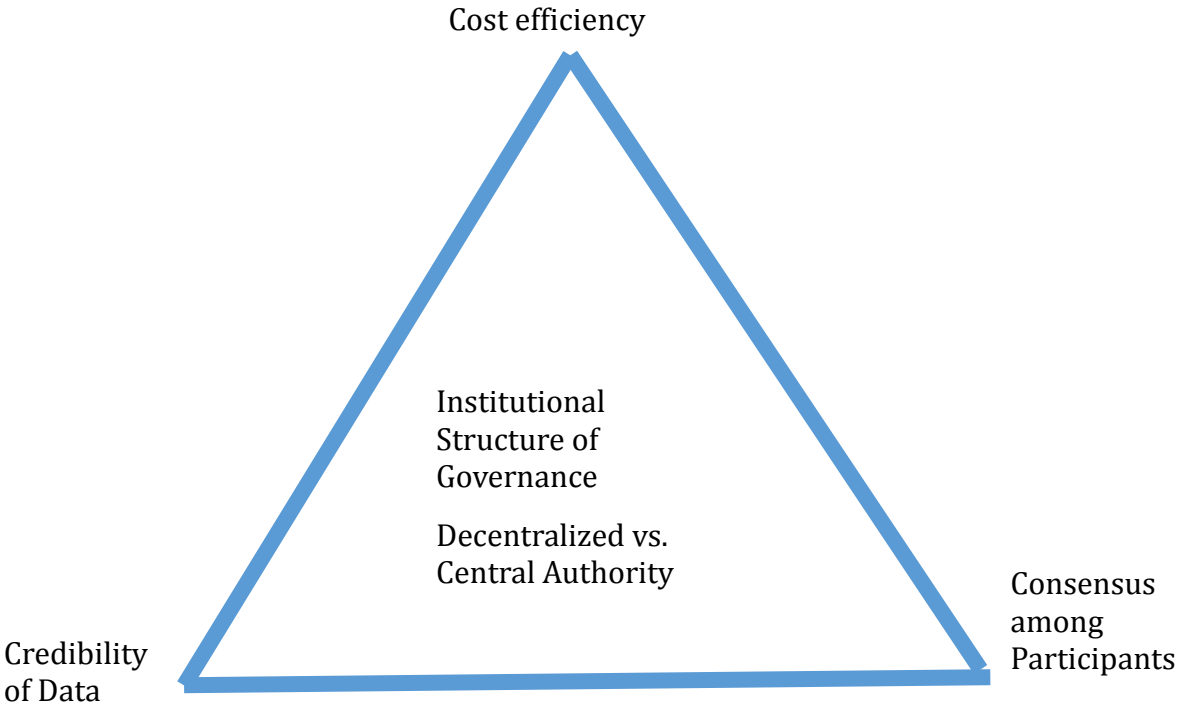
Cost of trust, rent extraction, vs. cost of latency, capacity constraints, and consuming resources, Privacy, Switching

Credibility of Data (information): Truthful Data or Information

Trade-off Status: Immutability vs Corrigibility

Consensus Maintenance : Participants

Security and safety vs. Privacy




DLT should be assessed against the Centralized or Intermediated Ledger in light of the three aspect, which determines the destiny of Blockchain.

VI. Conclusion

Enhanced transparency does neither necessarily alter the freeriding incentives nor deter the deviators' incentives to create a hardfork. Large blockholders (coincidentally *blockholders* in lieu of corporate governance are in parallel with the large stakeholders in

a Blockchain) face a strong counter incentive despite the maintaining consensus incentive.

Liquidity is frozen and disappear within the economy once the crisis starts and spreads out to the less informed investors. Immaculate transfer from the enhanced transparency to the improved liquidity and efficiency is a far-fectched allegation with an overhyped technology. Prospect for the Private Blcokchain looks compromising but that of Public looks unpromising so far.

Krugman (27 March 2018)

> W*hatever you think is the ultimate cause of an economic phenomenon, your story about how that phenomenon happens has to include an explanation of how peoples' incentives change.*
>
> E*conomics is about what people do, and stories about macrobehavior should always include an explanation of the micromotives that make people change what they do.*
>
> I*ncentives and motives are still key.* – New York Times –

If a government is believed to behave reasonably only if it is forced to do so, an individual can never behave more reasonably than forced to do so.

Neither *Howard Roark* in the Fountainhead nor *John Galt* in the Atlas Shrugged can be free of incentive and motive as an individual.

References

Abadi, Joseph and Markus Brunnermeier, 2018 “Blockchain Economics” *June 18*, working paper mimeo

Biais, Bruno, Christophe Bisière, Matthieu Bouvard, and Catherine Cassamatta, 2018 “The blockchain folk theorem” Working Paper, TSM-research.

Birch, Dave. 2017, ‘Estonia, fake news and digital identity’, *Consult Hyperion* (Mar. 20), http://www.chyp.com/estonia-fake-news and-digital-identity/

Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015) Bitcoin: economics, technology, and governance, *Journal of Economic Perspectives* 29, 213–238.

Casey, Michael, Jonah Crane, Gary Gensler, Simon Johnson and Neha Narula (2018) “The Impact of Blockchain Technology on Finance: A Catalyst for Change”, The 21st Geneva reports on the world economy, *July*, International Center for Monetary and Banking Studies (ICMB) and Centre for Economic Policy Research (CEPR)

Catalini C., and J. Gans, 2017 “Some simple economics of blockchain” Working paper

Cong, Lin William, and Zhiguo He, 2018, Blockchain disruption and smart contracts, May 22. *Conditionally Accepted, Review of Financial Studies*.

Davidson, S., De Filippi, P., & Potts, J. (2018) “Blockchains and the economic institutions of capitalism”, *Journal of Institutional Economics*, 1-20.

Gillis, Maureen and Alexandru Trusca, 2017. “‘Not There Yet': Bank of Canada Experiments with Blockchain Wholesale Payment System,”, June 20th, 2017, https://www.mccarthy.ca/en/insights/blogs/snipits/not-there-yet-bank-canada-experiments-blockchain-wholesale-payment-system

Gerard, David. 2017 ‘Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts’, Paperback – July 24, 2017.

Gupta, Sanjeev, Michael Keen, Alpa Shah, and Geneviève Verdier (2017) “Digital Revolutions in Public Finance”, *International Monetary Fund*.

Jeffries, Adrianne (2018), "Blockchain is meaningless", The Verge, 7 March

Kaldor, Nicholas 1942, “Professor Hayek and the Concertina-Effect” *Economica*, New Series, Vol. 9, No. 36 (Nov., 1942), pp. 359-382.

Merkle, Ralph. C. (1988). "A Digital Signature Based on a Conventional Encryption Function". Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science. 293. p. 369.

Morris, Stephen, and Hyun Song Shin. 2002. "Social Value of Public Information." American Economic Review, 92 (5): 1521-1534.

Morris, Stephen and Shin, Hyunsong. (2003). Global Games: Theory and Applications. In M. Dewatripont, L. Hansen, & S. Turnovsky (Eds.), Advances in Economics and Econometrics: Theory and Applications, Eighth World Congress (Econometric Society Monographs, pp. 56-114). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511610240.004.

Narula, N., W. Vasquez, and M. Virza (2018), "zkLedger: Privacy-Preserving Auditing for Distributed Ledgers", 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), USENIX Association.

Perry, J Steven, 2018, “What is blockchain? A primer on distributed ledger technology” The developer Works Blog, IBM. *Updated* March 19, 2018

Raskin M., and D. Yermack, 2016, “Digital Currencies, Decentralized Ledgers, and the Future of Central Banking” NBER Working Paper No. 22238.

Tirole, Jean, 2006, “The theory of corporate finance” *Princeton University Press*.

Tirole Jean, 2017 “There are many reasons to be cautious about bitcoin” Financial Times November 30.

Saleh, F (2018), “Blockchain without Waste: Proof-of-Stake”, working paper.

Sraffa, Piero 1932, “Dr. Hayek on Money and Capital Source” The Economic Journal, Vol. 42, No. 165, pp. 42-53

Walch, Angela 2017 “Blockchain’s Treacherous Vocabulary: One More Challenge for Regulators” Journal of Internet Law, Aug. Vol. 21 (2), 9-16

Yermack, D., 2017, “Corporate Governance and Blockchains” , *Review of Finance*, 21(1), 7-31.

Philippon, Thomas, 2018, “The Fin Tech Opportunities”, March *NYU* Working Paper.

Philippon, Thomas 2015, “Has the US Finance Industry Become Less Efficient? On the

Theory and Measurement of Financial Intermediation", *American Economic Review*, 105 (4) 1408–1438.