Asian Journal of Advances in Research

Volume 7, Issue 1, Page 587-599, 2024; Article no.AJOAIR.4254

A Novel Centralized Blockchain and Cryptocurrency for E-Governance

Om Prakash [a++*]

[a] *SMS Lucknow, India.*

Author's contribution

The sole author designed, analysed, interpreted and prepared the manuscript.

Article Information

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://prh.mbimph.com/review-history/4254

Short Communication

Received: 18/08/2024
Accepted: 22/10/2024
Published: 29/10/2024

ABSTRACT

The work undertaken in this research seeks to solve the problem of the lack of state of art Civil Law and legislation, which till now is rather unavailable. A proposed solution is a need of new legislation that offers coherent as well as thwartwise answers to address a proper and upright use of crypto-currencies. It is proposed that the legislators and lawmakers must aim to provide rules essential for achieving meticulous and explicit policies & goals with reference to virtual assets like cryptos. This research work also highlights some shortcomings in using existing legal concepts when it comes to regulating cryptocurrencies. Furthermore, in practice, the current legislative arrangement is rather unable to achieve the required enhancements to regulate crypto-currencies by just utilizing traditional concepts as used to regulate fiat currencies. It is also shown that the current work in this paper is actually in-line with the present corpus of literature, claiming that current suggestion to regulate crypto-currencies would not inhibit the required development and promoting blockchain and cryptocurrency technologies. However, this has to be developed and grown within the right legal framework.

[++] *Professor Management;*
**Corresponding author: Email: omprakash@smslucknow.ac.in;*

Cite as: *Prakash, Om. 2024. "A Novel Centralized Blockchain and Cryptocurrency for E-Governance". Asian Journal of Advances in Research 7 (1):587-99. https://jasianresearch.com/index.php/AJOAIR/article/view/486.*

Keywords: Crypto-currencies; bitcoin; economic regulation; civil law.

1. INTRODUCTION

The traditional laws are not yet ready to generate a coherent and transversal response to regulate crypto-currencies and, in general, virtual goods. The restrictive regulatory responses that seek to avoid their misuse should be punctual and minimum necessary to comply with strictly defined policy objectives. Many countries, including India, have not yet developed the appropriate conceptual categories to regulate such a new phenomenon. Furthermore, from a practical as well as financial standpoint, crypto-currencies are yet to achieve necessary importance for justifying regulatory efforts as in the case of fiat currencies. This argument joins other voices that have warned with suggestions to regulate crypto-currencies, rather than inhibiting their development [1]. The concern that motivates this article is that in order to regulate Bitcoin, for example, the most popular crypto-currency, one ends up clumsily regulating the local Bitcoin exchanges or new applications of Blockchain, which is the technology that enables Bitcoin [2]. Although in this article the attempt is not to address the problem of disruption and competition that has been the focus in countries like Chile, like the battle between crypto-currency intermediaries and traditional commercial banking, the attempt is rather to illustrate why crypto-currencies are a challenge for traditional law that it goes far beyond its potential criminal uses or the difficulties it presents for monetary regulation (Álvarez, Bignon, Walras and Menger (2011).

The development of the argument is based on the review of the concept of virtual currencies to distinguish them from other forms of electronic money. Crypto-currencies are revolutionary and therefore it is necessary to distinguish them from it. Crypto-currencies and virtual currencies not only share the characteristic of being digital, but both were designed to emulate the scarcity that exists in the real world. This is essential to understand the phenomenon to be regulated. In this regard, the operation of crypto-currencies are also illustrated to bring forth the aspects in which they represent something totally new for which many of our legal institutions are not adapted (Ametrano, 2016). If the law serves to attribute responsibilities or give certainty to the parties in a transaction, crypto-currencies have programmed in a way that could render many of the legal institutions that seek compliance or regulate the behavior of intermediaries useless. From an economic point of view, crypto-currencies are different from traditional currencies, and regulating them by thinking about traditional currencies, without distinguishing between them, is a mistake. Relying on history, operations and the economy of crypto-currencies, it may be seen that the legal system may adapt a cautious approach to its regulation, especially if it seeks restrictive objectives, such as protecting investors and consumers, or preventing commission of crimes. In this paper, therefore, suggestions of a cautious regulatory approach and with specific responses to remedy imminent problems are recommended. One may not have a clear idea of how crypto-currencies will interact with deliberative humans in this new way of generating and transferring wealth. So, to protect investors and consumers, or prevent the commission of crimes it is essential to adopt cautious regulatory approach and with specific responses to remedy imminent problems [3].

2. LITERATURE REVIEW

Crypto-currencies and other forms of digital money: Crypto-currencies are files, bits with data - such as the popular PDF or MP3 - seeking to achieve every function as fulfilled by fiat currency, though with the use of internet as medium of transmission. Before delving into the concept, its economic conception and its legal categorization, it is useful to distinguish crypto-currencies from other similar concepts that invite confusion. In the order discussed, these are: i) digital money, ii) electronic money, iii) virtual currencies and, finally, iv) crypto-currencies [4].

Digital money or digital currency is the generic name for any intangible that is used as a means of digital paymen [5]. This should be understood as opposed to the concepts of physical money, metallic or paper money. Digital money is the genre that includes all the other categories: electronic money, virtual currencies and crypto-currencies [6], Simonetti Rojas, 2017; Tucker, [7]. The concept, although too broad to be legally categorized, is of interest to economists because it includes different means of payment that could have an impact on the general price level (Babaioff, Dobzinski, Oren, Zohar, 2012). Incipient studies in macroeconomics consider that digital money is a variable that should be considered in monetary theory, especially if it

functions as a mechanism for the expansion of bank credit [8-10].

Electronic money, also known as emoney, is an electronic means of payment that eventually "obliges in" or gives "the right to" money in current or circulating use and that bears its name [11,12]. The European Central Bank defines it as "an electronic deposit of monetary value [contained] in a technological device [software or hardware] that can be widely used to make payments to entities other than its issuer." 1 The United States has had legislation regulating electronic transactions and, therefore, electronic money since 1978 (Electronic Fund Transfer Act).

What distinguishes electronic money from other forms of digital money is that it requires a "contractual infrastructure" that assigns responsibilities between the parties and contains mechanisms to convert it into current money, even if these are not used in practice (Khan, 2008). The obligations generated by electronic money are analogous to those generated by transactions of documents representing money (Khan, 2008; Halaburda and Sarvary, 2016; Rogers, 2005: 1,257-1,262). With Paypal, for example, you can pay in dollars for a sale on the internet. But Paypal relies on credit cards and the contracts that support them and that assign responsibilities between the parties. This operation is not radically different from how a credit note or a check that is drawn against a checking account works. As Gans and Halaburda [13] point out, electronic money is the "digital layer" of current money [14].

Virtual currencies are unregulated digital currencies that serve as a means of payment on the internet (European Central Bank, 2012: 13). It is important not to confuse them with representative commodity mechanisms. The latter would become the "digital layer" of money based on commodities (commodity money). Virtual currencies have their own denomination and have no correspondence in the physical world. They are not traded under the assumption that they are convertible into current money, even though secondary markets regularly allow such conversion [15]. Their usefulness as a means of payment - their main function - is determined by what can be purchased directly with them [13]. Loyalty programs in flight miles are a type of virtual currency of growing popularity [15,16]. Miles and virtual currencies are so similar when used as means of payment that many airlines are exploring transforming their miles into crypto-currencies [17].

Finally, crypto-currencies are a type of virtual currency with particular characteristics that allow them to have a universal and more widespread application. What makes them special is that they minimize the potential value problems associated with virtual worlds in which the same scarcity rules as the real world do not operate. They are also special because they work without intermediaries to validate transactions and, additionally, because in the most popular versions they are decentralized [18]. Crypto-currencies are issued and change hands in a decentralized way using cryptography to maintain fidelity, in addition to registration technologies or accounting books that are maintained and updated by thousands of computers independently to verify that there are no duplicate uses [19,20]. Given these special characteristics, crypto-currencies aspire to have the same functions as electronic money and, therefore, current money (Halaburda and Sarvary, 2016: 5). They are what Makoto anticipated as the "logical but revolutionary next step in the history of money (BPI B,nd) [21].

3. METHODOLOGY

Today, the need of the hour is to have Centralized Block chain, a cryptocurrency based on it and suitable legislation for its governance [22]. The issues outlined by Yermack and Roubini have been known to the crypto-currency community since its inception and have been debated. Roubini (2018) christened the problem the 'inconsistent trinity', following the ideas of one of the founders of a crypto-currency who tried to overcome the shortcomings of Bitcoin [23]. This idea is referred to as the "Buterin Impossibility Theorem" for crypto-currencies, in honor of its original proponent. Vitalik Buterin, in a white paper that created Ethereum, a crypto-currency intended to overcome the rigidity of Bitcoin, pointed out that crypto-currencies could not have at the same time: i) scalability, that is, the possibility of adjusting the money supply quickly to maintain stable prices and to function as a medium of exchange; ii) decentralization, and iii) security [24]. According to Buterin, you would always have to give up one of these characteristics in the design of a crypto-currency to obtain the other two. His theorem is sound when contrasted with the historical evidence we have for coins. Central banks offer scalability and security, but they are centralized and control the

supply of currency [25]. The decentralized systems of the existing currencies could have more flexibility and scalability, but at the cost of the security in the network that must be validating the transactions [26]. This problem has been verified with new crypto-currencies like altcoins which, although more scalable in design than Bitcoin, are successfully attacked by miners of consolidated coins in what is called a 51% attack. If you want to have a secure and scalable system (Cline, 2011), you must retain centralization in some way [27]. The latter was the bet of Ethereum and other crypto-currencies such as Peercoin. Its protocols, called "proof of interest" (proof-of-stake), give more weight in the consensus required to validate transactions to the user who has more interest in the destination of the currency, which implies a certain degree of centralization [28].

Centralized block chain: Finra R3 Research and their researcher Emily put forth a very valid document on Centralized Block Chain [29]. As per the research, a block chain can be either centralized or decentralized. It may be worth to note here, as per the research paper, that decentralized concept in this context may not be confused with distributed ledger principle in block chain and crypto-currencies [30]. Whilst a block chain is usually distributed, in that several many parties hold a copy of ledger, but still, it may not be fully decentralized (Doguet, 2012). A block chain may be centralized or decentralized, referring merely to the to the right of participating parties to the ledger [31]. Thus, in essence, it is merely is a matter of design and architecture. Within the decentralized framework, parties having almost equal rights may chose to either participate or transact in the ledger [32]. Hence, there needs to be some machinations to avoid some vulnerabilities as al participants seem to be having equal rights. Where there is a hierarchy of controller, like Government Agencies, not everyone can be assigned equal rights as mandated in the centralized concept. For example, Bitcoin – a decentralized arrangement, makes use of mining and proof-of-work for ensuring integrity of ledger, and one is well aware of the vulnerabilities in many transactions (Rutland, 2017).

A centralized network, which can be a better way in many respects, comprises only of parties whose identities are known [33]. So anyone, unlike in decentralized block chain, cannot just join the network and leads into a system that has better validity as parties having established credibility and reputation can post over the ledgers [34]. Since the network participant identity is established already, so the transaction is credible from a known party and not from an anonymous party as in the case of decentralized network like bitcoin [35]. Furthermore, centralized distributed ledger has its right potential to be used in the regulated industries like in BFSI Domain industries and financial services. This will help to minimize vulnerabilities. Whilst both decentralized and centralized block chains may still have related risks, but centralized networks are preferred for the purpose in that the identity of participants is verified [36]. Consequently, audit trail does exist, should an actor attempts to tamper the systems. It may be worth noting here that participants, including the founders, may not be verifiable as some even bear the pseudonyms. One never knows that how the things take shape in the future and some unanticipated risk warrants the need of an accurate identity (Rutland, 2017).

If the third world countries like India, wish to use Bloch Chain and crypto-currencies then it is required to have a careful choice of using a better technology for e-Governance (Heeks, 2009). Bringing in Block chain in e-governance and usage of crypto-currencies can be inevitable [37]. For example, bringing in this new disruptive technology can be necessary in BFSI Domains as well as in other domains like land records and agriculture [38]. This will not only bring efficiency and transparency, but, will also put a check on frauds. India, for instance saw a series of frauds like the one committed by Nirav Modi, Choksi, and others [39]. Block Chain can put an effective check, but, the technologies like Centralized Block Chains can be useful as the network would be participated from the people having known identity [40]. Though no one can say that Block chain can put a stopper to all frauds, but, at least it can arrest the growth of frauds [41].

A legal generalization of crypto-currencies: The state of the art of the study of crypto-currencies in the area of law is primary and less than that observed in areas such as science and economics. The situation is understandable [42]. This is an entirely new situation for which positive law has few answers. With electronic money, it was easy to adapt the existing categories and concepts, since the parts and content of the obligations, and in general everything that concerns the law, remained practically unchanged (Khan, 2008; Rogers, 2005).

In cryptocurrency, extant legislation with respect to wealth or property, cannot be extended to the virtual environment [43]. The problem coming from smart contracts, like irreversibility of transaction between anonymous participants, cannot be supported as in the existence law of contract, the parties cannot be anonymous [44]. For example, in Indian context, with reference to the Laws of Contract, the parties must be competent and specific in order to enter into a contract. In case of decentralized network, if the parties are working anonymously and enter in a smart contract, then such terms of contract cannot be validated by an Indian Court of Law or Indian Judicial system [45]. For example, if a minor enters into a contract, then this contract shall be null and void [46] Thus, the proposition is to make suitable amendments in Law such that these type of exceptions can be considered legal, which looks to be a remote possibility. The best solution, therefore, is to adopt suitable block chain technology and a crypto based on a suitable block chain [47].

Cryptom: A new crypto currency is being proposed, coined as “Cryptom”. This currency would be founded on a a centralized Block Chain. Such technology would work with parties that are specific and competent as well as empowered or nominated to act in their specific roles. The parties who can enter the network cannot be anonymous and shall be of verifiable identity. Thus, if they enter into some contract, the terms of the contract can be valid in the eyes of Law, as per the Laws of Contract specifications. The details of the currency, its source code and its specifications is attached at the appendix for reference [48].

4. CONCLUSION

In the face of such important gaps in positive law, it is inevitable to suggest the obvious. It is required that innovative approach, revised legislation and institution to support them is required so as to appropriately regulate user activities with crypto-currency. However, this is to be done carefully and watchfully, considering the cost benefit analysis. At present, it is proposed that the centralized blockchain and a crypto currency based on it like “Cryptom” can be tested and adopted if it comes out as a better strategy to limit or avoid an illegal use. Suitable legislation must be in place to prosecute imminent abuse, as other jurisdictions do, so as to normalize the use of crypto-currency with the help of newly adopted legal system. Attempt needs to ne made to consolidate crypto-currencies to start its use in the mainstream [49].

The best approach for the moment is therefore to wait. See how the conflicts between parties that transact in crypto-currencies in courts are evolving. The courts, which function in a decentralized manner and extending existing norms to supervening events, have the ability to collect cross-sectional information on potential conflicts such as those I described in the previous section regarding the exchange and forced execution, or to determine the criminal operation in the crypto-currencies that are wrapped. With a few years of conflict and the questions they bring, we may be in a position to understand what problems crypto-currency transactions cause real people in real transactions, and design regulation that puts them at the center. After all, the object is to wait and see adopt the system which is stable, durable and reliable.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

1. Kaplanov N. Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. Loyola Consumer Law Review. 2012;25(1):111-174. Available: http://bit.ly/2wFmr4u
2. Álvarez A, Bignon V. Walras L, Menger C: Two ways on the path of modern monetary theory". European Journal of the History of Economic Thought. 2013;20 (1);89-124. Available:http://doi.org/10.1080/09672567. 2011.596939
3. Ametrano F. Bitcoin, blockchain, and distributed ledgers: Between hype and reality. SSRN Electronic Journal; 2016. Available:http://doi.org/10.2139/ssrn.28322 49

4. Ametrano F. Hayek money: The crypto-currency price stability solution. SSRN Electronic Journal; 2016.
Available:http://doi.org/10.2139/ssrn.2425270
5. Auer R, Claessens S. Regulation of crypto-currencies: Evaluation of market reactions. BPI; 2018.
Available:https://bit.ly/2TZktpy
6. Arias G, Sánchez A. The digital currency challenge for the regulatory regime. Chilean Journal of Law and Technology. 2016;5(2):173-209.
Available:http://doi.org/10.5354/0719-2584.2016.43541
7. Babaioff M, Dobzinski S, Oren S, Zohar A. On Bitcoin and red balloons;(2012.
Available:http://doi.org/10.1145/2229012.2229022
8. Fung B, Molico M, Stuber G. Electronic money and payments: Recent developments and issues; 2014.
Available:http://bit.ly/2HX9dqc
9. Bjerg O, McCann D, Macfarlane L, Hougaard Nielsen R, Ryan-Collins J. Seigniorage in the 21st Century: A study of the profits from money creation in the United Kingdom and Denmark. Frederiksberg: Copenhagen Business School; 2017.
10. Peters G, Panayi E, Chapelle A. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. Journal of Financial Perspectives. 2015;3(3):92-113.
Available:http://bit.ly/2wFi614
11. Khan A. A theoretical analysis of payment systems. South Carolina Law Review. 2008;60(2):1-66.
Available:http://bit.ly/2wDCCzh
12. Rogers J. The new old law of electronic money. Southern Methodist University Law Review. 2005;58 (4):1253-1312.
Available:http://bit.ly/2XzrdfK
13. Gans J, Halaburda H. Some economics of private digital currency. In Goldfarb A, Greenstein S, Tucker C (eds.); Economic analysis of the digital economy. Oxford: Oxford University Press. 2015;257-276.
Available:http://doi.org/10.7208/chicago/9780226206981.003.0009
14. Barber A. Bitcoin and the philosophy of money: Evaluating the commodity status of digital currencies. Spectra. 2015;4(2).
Available:http://http://doi.org/10.21061/spectra.v4i2.241
15. European Central Bank. Virtual currency schemes. Frankfurt am Main: European Central; 2012.
16. Castronova E. Wildcat currency. New Haven: Yale University Press; 2014.
17. Böhme R, Christin N, Edelman B, Moore T. Bitcoin: Economics, technology, and governance. The Journal of Economic Perspectives. 2015;29(2):213-238.
Available:http://doi.org/10.1257/jep.29.2.213
18. Bonneau J, Miller A, Clark J, Narayanan A, Kroll J, Felten E. (undated). SoK: Research perspectives and challenges for Bitcoin and crypto-currencies. In 2015 IEEE Symposium on Security and Privacy. 2015;104-121.
Available:http://doi.org/10.1109/SP.2015.14
19. Brito J, Castillo A. Bitcoin: A primer for policymakers. Arlington: Mercatus Center at George Mason University; 2013.
20. Halaburda H, Sarvary M. Cryptocurrencies. InBeyond Bitcoin: The Economics of Digital Currencies 2016 (pp. 97-163). New York: Palgrave Macmillan US.
21. BPI B. (no date). Crypto-currencies: Beyond the trendy phenomenon.
Available:http://bit.ly/2Ilkqjj
22. Sai AR, Buckley J, Fitzgerald B, Le Gear A. Taxonomy of centralization in public blockchain systems: A systematic literature review. Information Processing & Management. 2021, Jul 1;58(4):102584.
23. Roubini N., Crypto is the Mother of all Scams and (Now Busted) Bubbles while Blockchain is the Most Over-Hyped Technology Ever, No Better than a Spreadsheet/Database, Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs, Washington; 2018.
24. Brito J, Shadab H, Castillo A. Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling. Columbia Science and Technology Law Review; 2015.
Available:http://doi.org/10.2139/ssrn.2423461
25. Castronova E. A cost-benefit analysis of real-money trade in the products of

synthetic economies. Info. 2006;8(6):51-68.
Available:http://doi.org/10.1108/14636690610707482

26. Chaum D. Achieving electronic privacy. Scientific American. 1992;267(2):96-101.
Available:http://doi.org/10.1038/scientificamerican0892-96
27. Cline E. Ready player one. Portland: Broadway Books; 2011.
28. Croman K, Decker C, Eyal I, Gencer A, Juels A, Kosba A et al. On scaling decentralized blockchains. In Clark J, Meiklejohn S, Ryan P, Wallach D, Brenner M, Rohloff K (eds.); Financial cryptography and data security: FC 2016. Lecture notes in computer science. 2016;106-125.
Available:http://doi.org/10.1007/978-3-662-53357-4_8
29. Rutland E. Blockchain Byte. FINRA. R3 Research. 2017;2.
30. Davidson L, Block W. Bitcoin, the Regression Theorem, and the emergence of a new medium of exchange. The Quarterly Journal of Austrian Economics. 2015;18(3):311-338.
Available:http://bit.ly/2HZ9uJf
31. Doguet J. The nature of the form: Legal and regulatory issues surrounding the Bitcoin digital currency system. Louisiana Law Review. 2012;73(4):1118-1153.
Available:http://bit.ly/2HYyIHF
32. Lastowka G, Hunter D. The laws of the virtual worlds. California Law Review. 2004;92(1):1-74.
Available:http://doi.org/10.15779/Z386H7P
33. Dourado E, Brito J. Crypto-currency. In The New Palgrave Dictionary of Economics. London: Palgrave Macmillan. 2014;1-9.
34. Heeks R. Understanding gold farming "and real-money trading as the intersection of real and virtual economies. Journal for Virtual Worlds Research. 2009;2(4):4-27.
Available:http://doi.org/10.4101/jvwr.v2i4.868
35. Dwyer G. The economics of Bitcoin and similar private digital currencies. Journal of Financial Stability. 2015;17:81-91.
Available:http://doi.org/10.1016/j.jfs.2014.11.006
36. Fenwick M, Kaal W, Vermeulen E. Legal education in the blockchain revolution. Vanderbilt Journal of Entertainment & Technology Law. 2017;20(2):351-383.
Available:http://bit.ly/2HXHc1A
37. Nazir M, Hamilton J, Tee S. Real money trading in virtual worlds. Proceedings of the 17th International Conference on Electronic Business; 2017.
Available:http://bit.ly/2KtsSzD
38. Filipkowski W. Cyber laundering: An analysis of typology and techniques. International Journal of Criminal Justice Sciences. 2008;3:(1):15-27.
Available:http://doi.org/10.2139/ssrn.2939127
39. Szabo N. Formalizing and securing relationships on public networks. First Monday. 1997;2(9).
Available:http://bit.ly/2Xw0cK2
40. Foley S, Karlsen J, Putniņš T. Sex, drugs, and Bitcoin: How much illegal activity is financed through crypto-currencies?. The Review of Financial Studies. 2018;32(5):1798-1853.
Available:http://doi.org/10.1093/rfs/hhz015
41. Dong C, Chen C, Shi X, Ng CT. Operations strategy for supply chain finance with asset-backed securitization: Centralization and blockchain adoption. International Journal of Production Economics. 2021;241:108261.
42. Gamble C. The legality and regulatory challenges of decentralized crypto-currency: A Western perspective. International Trade and Business Review. 2017;20.
43. Graf K. Commodity, scarcity, and monetary value theory in light of bitcoin. Prices & Markets. 2014;3(3):1-24.
Available:http://bit.ly/2HY84hZ
44. Tapscott D, Tapscott A. Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. New York: Penguin; 2016.
45. Task Force on Stored-Value Cards. A commercial lawyer's take on the electronic purse: An analysis of Commercial Law issues associated with stored-value cards and electronic money report. The Business Lawyer. 1996;52(2):653-727.
Available:http://bit.ly/2Ikh53P
46. Upadhyay SN. Legal Consequences of a Minor’s Agreement in India. Business Law Review. 2014;35(4).

47. Kolb J, AbdelBaky M, Katz RH, Culler DE. Core concepts, challenges, and future directions in blockchain: A centralized tutorial. ACM Computing Surveys (CSUR). 2020;53(1): 1-39.
48. Castronova E. Virtual worlds: A first-hand account of market and society on the cyberian frontier. CESifo Working Paper Series. 2001;618.
Available:http://bit.ly/2Ik0Io2
49. Yang X, Zhang Y, Wang S, Yu B, Li F, Li Y, Yan W. LedgerDB: A centralized ledger database for universal audit and verification. Proceedings of the VLDB Endowment. 2020;13(12):3138-51.

APPENDIX

Software work copyrighted:

New Legislation needed to adopt a Centralized Block Chain for e-Governance and development of a new

crypto-currency to support

Description of software

This software shows the proof of work for a Centralized Block Chain and based on the centralized network, which can be a better way in many respects, comprises only of parties whose identities are known. So anyone, unlike in decentralized block chain, cannot just join the network and leads into a system that has better validity as only credible and reputable participants may post to the ledger.

Since

the network participants identities are known, so their transactions can also be audited. Furthermore, centralized distributed ledger has its right potential to be used in the regulated industries like in BFSI (**Banking, financial services and insurance)** Domain industries and financial services.

Kryptom

A new crypto currency is being proposed, coined as “Kryptom”. This currency is founded on the centralized Block Chain.

Centralized Block Chain and Kryptom Coin

```
/////
// build central blockchain from scratch in go(lang)
//
//
//
// to run use:
// $ go run blockchain.go
package main
import (
 "fmt"
 "crypto/sha256"
 "encoding/hex"
 "time"
 "strconv"
)
type Block struct {
 Time int64 // seconds since (unix) epoch (1970-01-01)
 Data string
 Prev string // use []byte/int256/uint256 ??
 Hash string // use []byteint256/uint256 ??
}
// bin(ary) bytes and integer number to (conversion) string helpers
func binToStr( bytes []byte ) string {
 return hex.EncodeToString( bytes )
}
func intToStr( num int64 ) string {
 return strconv.FormatInt( num, 10 )
}
func calcHash( data string ) string {
```

```
 hashed := sha256.Sum256( []byte(data) )
 return binToStr( hashed[:] ) // note: [:] converts [32]byte to []byte
}
func NewBlock(data string, prev string) Block {
 t := time.Now().Unix()
 hash := calcHash( intToStr(t) + prev + data )
 return Block { t, data, prev, hash }
}
func main() {
 b0 := NewBlock( "Hello, Cryptos!",
"0000000000000000000000000000000000000000000000000000000000000000" )
 b1 := NewBlock( "Hello, Cryptos! - Hello, Cryptos!", b0.Hash )
 fmt.Println( b0 )
 // {1522687834 Hello, Cryptos!
 // 0000000000000000000000000000000000000000000000000000000000000000
 // d85da0f449ff9ddc2c5ba638b23b9524381811227eb463b8c9e0be40dc1b1a8a}
 fmt.Println( len( b0.Hash ))
 // => 64
 fmt.Println( len( b0.Prev ))
 // => 64
 fmt.Println( b1 )
 // {1522687834 Hello, Cryptos! - Hello, Cryptos!
 // d85da0f449ff9ddc2c5ba638b23b9524381811227eb463b8c9e0be40dc1b1a8a
 // e48ba730165d88e15435483fc3a60714be526096a0c9a71ad10623340e33c7e3}
 fmt.Println( len( b1.Hash ))
 // => 64
 fmt.Println( len( b1.Prev ))
 // => 64
 blockchain := []Block {b0, b1}
 fmt.Println( blockchain )
 // => [{1522687834 Hello, Cryptos!
 // 0000000000000000000000000000000000000000000000000000000000000000
 // d85da0f449ff9ddc2c5ba638b23b9524381811227eb463b8c9e0be40dc1b1a8a}
 // {1522687834 Hello, Cryptos! - Hello, Cryptos!
 // d85da0f449ff9ddc2c5ba638b23b9524381811227eb463b8c9e0be40dc1b1a8a
 // e48ba730165d88e15435483fc3a60714be526096a0c9a71ad10623340e33c7e3}]
}
pragma solidity ^0.4.24;
import './Ownable.sol';
import './ERC20Interface.sol';
/**
* @Kryptom
**/
contract Bank is Ownable {

 address public investmentAddr; // Investment contract address used to allow withdrawals
 address public coinToken; // COIN token address.
 address public cashToken; // CASH token address.
 /**
 * @param _coinToken address of the Coinvest token.
 * @param _cashToken address of the CASH token.
 **/
 constructor(address _coinToken, address _cashToken)
 public
 {
 coinToken = _coinToken;
 cashToken = _cashToken;
```

```
 }
/** ****************************** Only Investment ****************************** **/

 /**
 * @dev Investment contract needs to be able to disburse funds to users.
 * @param _to Address to send funds to.
 * @param _value Amount of funds to send to _to.
 * @param _isCoin True if the crypto to be transferred is COIN, false if it is CASH.
 **/
 function transfer(address _to, uint256 _value, bool _isCoin)
 external
 returns (bool success)
 {
 require(msg.sender == investmentAddr);
 ERC20Interface token;
 if (_isCoin) token = ERC20Interface(coinToken);
 else token = ERC20Interface(cashToken);
 require(token.transfer(_to, _value));
 return true;
 }

/** ******************************** Only Owner ********************************** **/

 /**
 * @dev Owner may change the investment address when contracts are being updated.
 * @param _newInvestment The address of the new investment contract.
 **/
 function changeInvestment(address _newInvestment)
 external
 onlyOwner
 {
 require(_newInvestment != address(0));
 investmentAddr = _newInvestment;
 }

/** ****************************** Only Coinvest ******************************** **/
 /**
 * @dev Allow the owner to take non-COIN Ether or tokens off of this contract if they are accidentally
sent.
 * @param _tokenContract The address of the token to withdraw (0x0 if Ether)--cannot be COIN.
 **/
 function tokenEscape(address _tokenContract)
 external
 onlyCoinvest
 {
 require(tokenContract != coinToken && _tokenContract != cashToken);
 if (_tokenContract == address(0)) coinvest.transfer(address(this).balance);
 else {
 ERC20Interface lostToken = ERC20Interface(_tokenContract);

 uint256 stuckTokens = lostToken.balanceOf(address(this));
 lostToken.transfer(coinvest, stuckTokens);
 }
 }
}
pragma solidity ^0.4.24;
contract ERC20Interface {
```

```
 function totalSupply() public constant returns (uint);
 function balanceOf(address tokenOwner) public constant returns (uint balance);
 function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
 function transfer(address to, uint tokens) public returns (bool success);
 function approve(address spender, uint tokens) public returns (bool success);
 function transferFrom(address from, address to, uint tokens) public returns (bool success);
 event Transfer(address indexed from, address indexed to, uint tokens);
 event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
pragma solidity ^0.4.24;
/**
* @title Ownable
* @dev The Ownable contract has an owner address, and provides basic authorization control
* functions, this simplifies the implementation of "user permissions".
*/
contract Ownable {
 address public owner;
 address public coinvest;
 mapping (address => bool) public admins;
 event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);
 /**
 * @dev The Ownable constructor sets the original `owner` of the contract to the sender
 * account.
 */
 constructor() public {
 owner = msg.sender;
 coinvest = msg.sender;
 admins[owner] = true;
 admins[coinvest] = true;
 }
 /**
 * @dev Throws if called by any account other than the owner.
 */
 modifier onlyOwner() {
 require(msg.sender == owner);
 _;
 }
 modifier onlyCoinvest() {
 require(msg.sender == coinvest);
 _;
 }
 modifier onlyAdmin() {
 require(admins[msg.sender]);
 _;
 }
 /**
 * @dev Allows the current owner to transfer control of the contract to a newOwner.
 * @param newOwner The address to transfer ownership to.
 */
 function transferOwnership(address newOwner) onlyOwner public {
 require(newOwner != address(0));
 emit OwnershipTransferred(owner, newOwner);
 owner = newOwner;
 }

 /**
 * @dev Changes the Coinvest wallet that will receive funds from investment contract.
```

```
* @param _newCoinvest The address of the new wallet.
**/
function transferCoinvest(address _newCoinvest)
external
onlyCoinvest
{
require(_newCoinvest != address(0));
coinvest = _newCoinvest;
}
/**
* @dev Used to add admins who are allowed to add funds to the investment contract.
* @param _user The address of the admin to add or remove.
* @param _status True to add the user, False to remove the user.
**/
function alterAdmin(address _user, bool _status)
external
onlyCoinvest
{
require(user != address(0));
require(user != coinvest);
admins[user] = _status;
}
}
```


Peer-review history:
The peer review history for this paper can be accessed here:
https://prh.mbimph.com/review-history/4254