The Risks and Dangers of Relying on Blockchain Technology in Underdeveloped Countries

Christopher G. Harris
School of Mathematical Sciences
University of Northern Colorado
Greeley, Colorado 80639
christopher.harris@unco.edu

***Abstract*—As a foundational technology, blockchains have demonstrated their ability to remove middlemen and streamline ledger-based transactions in everything from cryptocurrencies (e.g. Bitcoin) to centralized voting. In many underdeveloped countries, blockchain-based technologies provide opportunities for transparent transactions between parties, reducing corruption and facilitating trust. Much research on blockchains to date has focused on its virtues, but far less attention has been paid to its inherent risks and dangers. In this paper, we examine the risks and dangers of relying on blockchains in underdeveloped countries. Despite its many promises, blockchain technologies face significant hurdles for adoption in underdeveloped countries; in this paper, we explore eight these risks and dangers.**

Keywords—blockchain, distributed ledgers, transparency, smart contracts, underdeveloped countries, anti-corruption

I. Introduction

A blockchain consists of a distributed database of records or public ledger of all transactions or digital events that have been executed. The information about these transactions is shared among participating parties. Each transaction in the public ledger is verified by a majority consensus of the participants in the system. It is immutable; once entered, the transaction information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever recorded in the system.

The current digital economy is heavily reliant on central trusted authorities. All online transactions rely on trusting someone to verify the truth— it can be a certification authority telling us that a certain digital certificate is trustworthy, a bank telling us that a financial remittance has been delivered reliably to a creditor, an email service provider verifying that our email has been delivered, or a social network such as Facebook telling us that our postings of life events have been shared with only those friends we have given permission to do so. The fact is that we live our life precariously in the digital world by relying on a central trusted entity for the security and privacy of our digital assets. Unfortunately, these third-party sources can be hacked, manipulated or compromised.

Blockchain technology has the potential to revolutionize the digital world by enabling a "distributed consensus" where each online transaction involving digital assets, past and present, can be verified at any time in the future. If implemented correctly, it can accomplish this without compromising the privacy of the digital assets and parties involved. The distributed architecture, immutability and transparency are three important characteristics of blockchain technology.

II. Blockchain Technology in Underdeveloped Countries

In theory, the countries which could stand to benefit most from blockchain technology are in the developing and underdeveloped world. An underdeveloped country is a nation with less developed industrial base and low Human Development Index (HDI) [1]. According to Economist Eugene Staley, an underdeveloped country is a sovereign nation characterized by (i) mass poverty which is chronic and not the result of temporary misfortune and (ii) obsolete methods of production and social organization, which means that the poverty is not due to poor natural resources and hence could presumably be lessened by methods already proved in other countries [2]. For the reasons mentioned by Staley, nearly all underdeveloped countries are overburdened by heavy regulations, high corruption, and low transparency [3]. Although these characteristics are not limited to underdeveloped countries; for the purposes of our discussion, we consider any country that has these regulatory characteristics as underdeveloped.

Ballot rigging still persists in many parts of the world, particularly in underdeveloped economies. Because ballot boxes can be stuffed, the election results may differ from the choice of a nation's citizens. Voting is subject to manipulation by corrupted authority. Blockchain technology can ensure that every eligible vote is counted accurately without an opportunity for manipulation. Moreover, blockchain technology can transform the traditional paper-based voting system to a digitalized one, offering convenience to the voters in developed countries as well [4].

Corruption on the property and real-estate market is another unresolved issue for many underdeveloped countries. As an example, Honduras is notorious for being one of the most corrupt countries in the world, ranking 135th out of 180 countries on the 2017 Transparency International Corruption Perceptions Index [5]. In order to root out corruption in land

978-1-5386-3416-5/18/$31.00 ©2018 IEEE

registries, the Honduran government partnered with a blockchain start-up to develop a system that kept the land record on a transparent blockchain platform. Although political issues in Honduras have stalled its implementation [6], the transparency provided by the blockchain limits the potential abusing of power by government officials while encouraging landowners to register their lands on a publicly-accessible blockchain [7]. In addition to its transparency, users of the blockchain could search for any property records in real-time at no cost.

The corruption and bribery of officials occurs more frequently in underdeveloped countries than in developed (or developing) ones. [8]. The application of blockchain on developing and underdeveloped countries not only can root out corruption but also lift those countries out of poverty. Despite the potential opportunities, there are many limitations of blockchain technology that keep it from resolving many issues related to corruption. Although the data governance and privacy issues remain larger challenges, its application to underdeveloped countries will not be realized on a large scale anytime soon primarily due to two factors: the resistance of the existing leadership and lack of infrastructure.

III. Types of Blockchains

Blockchain technology can be implemented as public, semi-private, or private. Private blockchains offer the following benefits: faster transaction verification and network communications, the ability to fix any errors that occur and reverse transactions if necessary, the ability to restrict access, and the ability to reduce the chance of outsider attacks [9]. Because the control over who has access to the blockchain is controlled, private blockchain operators may choose to unilaterally deploy changes of which some users will not approve. Developers who work to maintain public blockchain systems, such as Bitcoin, still rely on individual users to adopt any changes they propose, which serves to ensure that changes are only adopted if they are in the interest of the entire system. Also, public blockchain technology does not restrict users in the way that private blockchains do. They provide transactions that are immutable. Due to the perceived anonymity of its users, public blockchains can hide the actions of its user base, thus making the detection of attacks far more difficult.

Somewhere between the two is a semiprivate blockchain, which retains chosen elements of both public and private blockchains. Governments which are not comfortable with the lack of control over public blockchain implementations may implement restrictions, such as on limiting the users who may participate in the blockchain or ensure all participants are known and can be tracked. These entities are likely to pursue the semiprivate blockchain option.

IV. Dangers and Risks

In addition to the promise that blockchain technology may offer, an understanding of the attendant risks and dangers is necessary. Like any valuable asset, Bitcoin and blockchain assets can be damaged, destroyed or stolen [10]. North Korea, considered an underdeveloped country, was reportedly behind a significant heist of Bitcoin [11]; the fact that this cannot be verified illustrates the risks of relying on blockchain technology as foolproof [12]. Below, we describe eight other dangers and risks that blockchain technologies present in the underdeveloped world.

A. Manipulation of the Majority Consensus

There are some potential security issues with blockchain technology. The most worrisome is the possibility of a 51-percent attack, in which one mining entity could grab control of the blockchain and double-spend previously transacted coins into his own account. The issue is the centralization tendency in mining where the competition to record new transaction blocks in the blockchain has meant that only a few large mining pools control the majority of the transaction recording. Double-spending might also still be possible in other ways—for example, spoofing users to resend transactions which could allow malicious coders to double-spend coins. Another issue is distributed denial of service (DDoS) attacks, which can significantly limit the opportunities of mining pools not aligned with an entity that wishes to game the system [13].

In underdeveloped countries, particularly where the government has some incentive to manipulate transactions, the government can introduce delays in the validation step, allowing government-backed mining entities to provide earlier timestamps or to manipulate the majority consensus rule using DDoS attacks, making the 51-percent attack far more likely to occur [14]. This is particularly true when the government only allows private and semiprivate blockchains to be implemented limiting the effectiveness of blockchain transparency.

B. Limiting the Access of Miners

The process of verification of the transaction is conducted by users called miners who use the power of their computers or specially-designed devices to solve mathematical equations. This is required for confirming transactions. By doing so, they earn a reward in the form of Bitcoin (or any other cryptocurrency), an amount which is determined in advance [15]. The difficulty of equations is expanded with the growth of mining computational power, in an effort to keep the time needed to write the data into a cryptographically-sealed block constant.

Limiting access of miners to solving these mathematical equations is one way in which some governments can make verification of transactions far less appealing. Since miners require considerable resources, particularly electricity, to solve these equations (miners worldwide consume as much power as 3.4 million homes in the US), these efforts can draw government attention rather quickly. In January 2018, China was considering limiting power usage of some suspected miners to crack down on the industry [16].

C. Privacy, Anonymity, and Pseudo-anonymity

Privacy is also a concern. Not all data should be shown on a public ledger, available for the world to see. Even in developed countries with strong legal enforcement, one company may not want its competitors or investors to know all the details of its daily transactions. This issue is even more acute when government transactions are involved that the government does

not want to be transparent. Second, although private blockchains can improve privacy issues, transactions between parties in semiprivate and public blockchains are pseudo-anonymous and not anonymous. With enough data, pseudo-anonymous users can be identified, and government entities with concerns about outside interference, which occurs in the developing world, can identify and track these users. This is particularly worrisome because many blockchain users believe they are anonymous.

D. Issues with Contract Law

Blockchain technology has the potential to make significant changes to contract law using self-enforcing digital contracts. These have the benefit of being executed without requiring intermediaries to verify that the conditions have successfully been met. Therefore, in any economy, the legal and technical ramifications of smart contracts need to be considered, particularly when incongruities may arise between real-world contracts and their digital counterparts.

One emerging use of blockchain technology involves "smart contracts". Smart contracts are computer programs that can automatically execute the prearranged terms of a contract. When a preconfigured condition in a smart contract among participating entities is met, for example, once a container of goods is delivered to a remote location (and verified by GPS tracking), a payment is automatically released per the contract and can be verified by any interested party. Unfortunately, many governments in underdeveloped nations may determine that such contracts are invalid unless there is some stage of government approval, which can slow down the process and remove one key benefit: the lack of third-party intervention. Governments in which corruption is endemic are unlikely to relinquish control to smart contracts unless they are convinced of the merits of transactional transparency or they are forced to do so.

Smart property is a concept related to smart contracts It involves controlling the ownership of a property or asset via blockchain with smart contracts. The property managed by these contracts can be physical such as car, house or smartphone, or it can be non-physical such as shares of a company.

Neither smart contracts nor smart property can be effective, for instance, without governmental buy-in. A great deal of coordination and clarity on how smart contracts are designed, verified, implemented, and enforced is required. Based on previous modifications to contract law in underdeveloped countries, it is highly likely that the institutions responsible for those daunting tasks will take a long time to evolve. Furthermore, the technological challenges, such as managing security, will certainly be daunting.

In most underdeveloped countries, laws to protect contracts varies considerably [17]. When contract laws are poorly enforced, there has historically been a negative impact on economic performance [18]. Many governments take legal reform as a threat to sovereignty and blockchain technology is no exception.

E. Regulation

Another challenge is the uncertain legal framework and government regulations. First, since blockchain solutions require cryptocurrency to operate (e.g. to reward miners or record transactions), it is necessary to adjust the regulatory framework to recognize Bitcoin and other cryptocurrencies as a legal means of exchange. Many countries, such as Russia, Bangladesh, and China refuse to recognize cryptocurrencies as legitimate currencies, introducing problems for legal enforcement [19]. Second, as already stated, the courts and other organizations need to recognize the regulatory aspects of smart contracts, which many underdeveloped countries are unwilling to do.

F. Taxation

Another issue is the adjustment of taxation practices to encompass the financial transactions which occur on the blockchain. It is challenging for the most developed nations to track financial transactions made between pseudo-anonymous users and for tax authorities to correctly tax companies in the sharing economy such as Airbnb and Uber in addition to their users. Although a shift from income-based taxation to consumption-based taxation would make these transactions easier to follow, few underdeveloped governments are set up to track such transactions. These will require a major overhaul of the current taxation system, which few underdeveloped nations are willing to implement quickly [20].

Managing regulatory risk, particularly as applied to taxation, is a complicated domain where new regulations are being written but old ones remain in force. Complicating this is the fact that not all countries share the same rules. Know your customer (KYC), anti-money laundering (AML) and tax and accounting obligations are some areas of focus for legitimate businesses that want to benefit from the technology while remaining legally compliant. This is true even in developed economies. For example, a recent US Internal Revenue Service subpoena to Coinbase, a crypto-currency exchange, shows how regulators continue to apply existing law to new technology. Most underdeveloped nations have taxation laws that would be challenging to apply to blockchain-based technology.

G. Scalability and Storage Issues

There are many technology issues that have yet to be resolved regardless of the advancement of a country's economy. One issue is related to the size of blockchain ledgers. Blockchains grow over time and require effective record management. Even with public blockchains, rapidly increasing size issues may lead to ledger centralization, which points to government regulation. This is likely to affect the future of blockchain technology.

Storage will also be a hurdle. Although a blockchain eliminates the need for a central server to store transactions and device IDs, the ledger must be stored on the nodes themselves. In many underdeveloped nations, the government has a controlling stake in the internet. Limiting access to these nodes can be done through government involvement, affecting the utility and reliability of a blockchain in those nations.

H. Speed and Veracity of Transactions

Individual blockchain transactions are slow in comparison to normal consumer payment standards. The blockchain cannot be finalized until the new chain (and its hash value) have been calculated and agreed to by a majority consensus of users (because an attempted double spend is possible before the blockchain is finalized). According to [21], 13 percent of transactions on public blockchains exceed 20 minutes, and 25 percent can exceed an hour. This delay opens up windows of opportunity for the system to be gamed by miners behaving badly. This is especially true when the government-backed miners can manipulate the majority consensus.

Security is a blend of confidentiality, availability, and integrity, or "C-I-A". Blockchain technology provides the "A" and the "C", but the blockchain integrity contains a number of inherent risks. Once committed to the blockchain, transactions are indeed immutable, but the veracity of each entry rests on who controls the private key of each account.

V. Conclusion

Blockchain technology contains three distinct advantages, namely distributed architecture, immutability, and transparency. These can help combat fraud and corruption occurring in the underdeveloped economies if it is permitted to flourish without government intervention [22]. Indeed, the blockchain could be used to carry out many functions of intermediaries and assure the public that public officials are not squandering taxpayer money.

When used properly, government and financial institutions can apply blockchain technology as a means of combating financial crime such as money laundering. Blockchains can also be used track any funds that are transferred for criminal activities such as terrorism. With the proper use of the technology, every transaction can be recorded without manipulation providing transparency from start to finish. However, some governments have a strong incentive to keep transparency to a minimum.

Blockchain technologies were designed specifically for one primary goal: preventing the “double spend” of electronic coins, without a central authority. However, underdeveloped economies, particularly those resistant to transparency, can introduce efforts to undermine this goal for the reasons we have mentioned in this paper. Thus, blockchain technology is neither necessary nor sufficient for many of its suggested applications. This is particularly true in economies where it is in their best interest to limit transparency.

As a foundational technology that will certainly power new applications in both developed and underdeveloped economies, blockchain offers numerous benefits to economies that can foresee and exploit its merits. Underdeveloped nations that are resistant to the merits of the blockchain will benefit far less than those embrace its advantages.

References

[1] United Nations Human Development Index. Available at: http://hdr.undp.org/en

[2] DasGupta, M. and Roy, N. (2017). National Rural Livelihood Mission (NRLM) and Sustainable Livelihood Development through Poverty Alleviation. Research Review International Journal of Multidisciplinary. 2(9), 107-113.

[3] Rose-Ackerman, S., & Palifka, B. J. (2016). Corruption and government: Causes, consequences, and reform. Cambridge university press.

[4] Foroglou, G., & Tsilidou, A. L. (2015). Further applications of the blockchain. In 12th Student Conference on Managerial Science and Technology.

[5] Transparency International Corruption Perception Index (2017). Availsble at https://www.transparency.org/news/feature/corruption_perceptions_index_2017

[6] Riley, D. (2015). “Factom’s Blockchain land registry tool trial stalls due to the politics of Honduras. Silicon Angle. Available at http://siliconangle.com/blog/2015/12/27/factoms-blockchain-landreigstry-tool-trial-stalls-due-to-the-politics-of-honduras/

[7] Brodbeck, L. (2015). Blockchain Could Help Fight Corruption In Honduras. Benzinga. Available from: https://www.benzinga.com/news/15/05/5518234/blockchain-could-help-fight-corruption-inhonduras

[8] Ayyagari, M., Demirgüç-Kunt, A., & Maksimovic, V. (2014). Bribe Payments and Innovation in Developing Countries: Are Innovating Firms Disproportionately Affected?. Journal of Financial and Quantitative Analysis, 49(1), 51-75.

[9] Berke, A. (2017). “How Safe Are Blockchains? It Depends.” Harvard Business Review. Retrieved from https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

[10] Brill, A. (2015). The Use of Internet Technology by Cyber Terrorists & Cyber Criminals: The 2014 Report.

[11] Pham, S. (2017). “North Korea may be making a fortune from Bitcoin mania.” CNN Tech. Retrieved from http://money.cnn.com/2017/12/12/technology/north-korea-Bitcoin-hoard/index.html

[12] Porru, S., Pinna, A., Marchesi, M., & Tonelli, R. (2017, May). Blockchain-oriented software engineering: challenges and new directions. In Proceedings of the 39th International Conference on Software Engineering Companion (pp. 169-171). IEEE Press.

[13] Vasek, M., Thornton, M., & Moore, T. (2014, March). Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In International Conference on Financial Cryptography and Data Security (pp. 57-71). Springer, Berlin, Heidelberg. Chicago

[14] Johnson, B., Laszka, A., Grossklags, J., Vasek, M., & Moore, T. (2014). Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In International Conference on Financial Cryptography and Data Security (pp. 72-86). Springer, Berlin, Heidelberg.

[15] Lazanis, R. (2015). How Technology Behind Bitcoin Could Transform Accounting as We Know It. Retrieved from https://techvibes.com/2015/01/22/how-technology-behind-Bitcoin-could-transform-accounting-as-we-know-it-2015-01-22

[16] South China Morning Post. (2018) “China plans to deter Bitcoin miners by curbing electricity use”. Retrieved from http://www.scmp.com/business/banking-finance/article/2126776/china-plans-curb-electricity-usage-drive-cryptocurrency

[17] Daniels, R. J., & Trebilcock, M. (2004). The political economy of rule of law reform in developing countries. Mich. J. Int'l L., 26, 99.

[18] Haggard, S., & Tiede, L. (2011). The rule of law and economic growth: where are we?. World Development, 39(5), 673-685.

[19] Raymaekers, W. (2015). Cryptocurrency Bitcoin: Disruption, challenges and opportunities. Journal of Payments Strategy & Systems, 9(1), 30-46.

[20] Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[21] Kanaracus, C. (2016). “Don't believe the blockchain hype: Examining the weaknesses and risks.” ZDNet. Retrieved from http://www.zdnet.com/article/dont-believe-the-blockchain-hype-examining-its-weaknesses-and-risks/

[22] Pilkington, M., Crudu, R., and Grant, L. G. (2016). Blockchain and Bitcoin as a Way to Lift a Country out of Poverty. Tourism 2.0 and e-Governance in the Republic of Moldova.