The Bitcoin Revolution: Future of Blockchain and the Legislation of Distributed Ledger Economy

Gökhan Eğri

Ever since its conception and subsequent execution in an anonymous paper by Satoshi Nakamoto, Bitcoin revolutionized the world economy in a multitude of ways with the introduction of decentralized, peer-to-peer transactions. These transactions unnecesitated the intermediary element, i.e. banks, between the transacters; giving users direct access to their resources while upholding a comfortable degree of anonimity.

Bitcoin is marked by its use of a *distributed ledger* in storing and approving transactions. A *ledger* is a list of interactions that are chronologically stored in a meta-document for future reference. In finance, these ledgers provide an account of the various economical transactions, i.e. funds, real-estate bonds and money, between two parties. The current global economic model is based on the privatization of such ledgers which necessitates the inclusion of a trusted third-party in overseeing and mutually reconciling individual transactions. This model has two major setbacks in that, one, the involved intermediary requires a formidable processing fee for every transaction and two, the approval period of a transaction is significantly long. Furthermore, the presence of a single authoritative ledger also makes it susceptible to being irreversibly obstructed or altered by unknown sources.

Bitcoin circumvents these problems by using a distributed ledger which differs from a conventional ledger in that access to transactions is not restricted to a trusted intermediary but

is publicized to all users of the platform which obliterates the need for trust by checking individually stored ledgers to reach a consensus on the legitimacy of transactions.

The first step in the legitimization of the ledger is the transaction creation. The transactor starts by creating a transaction message with information on the identity of the transactor, the identity of the transactee and the transaction amount. The Bitcoin wallet then uses the private key of the transactor and the transaction message to create a single-use signature via a complex mathematical function. This allows for *absolute backwards immutability* as any changes to the transaction amount or to the identity of the transactee invalidate the transaction.

After the transaction has been created, it is then announced to the public as a *pending transaction*. Pending transactions are simultaneously created transactions which are waiting to be bundled together into a block and added to the blockchain. This process of introducing new transactions into the ledger is aptly called *mining* as it marks the introduction of Bitcoins into the system. As individual users or user groups, commonly referred to as *nodes*, try to include their block as the next in the chain, they compete to solve a *cryptographic hash*. A *cryptographic hash function* takes a limited-sized input and then encodes this input as again a limited-sized, 256-bits long for Bitcoin, output. The two essential features of a cryptographic hash function is that, one, it must have an irreversible yet easily verifiable output and two, a menial change in the input should affect the output so drastically that the possibility of obtaining the same hash for two different inputs should decrease exponentially.

Bitcoin uses the SHA256 Cryptographic Hash Function on the inputs of the added transaction message and the previous transaction message on the ledger with a random guess to obtain a cryptographic hash which satisfies a certain requirement. This is called a *proof-of-work* in that it demonstrates extensive CPU usage that goes into finding an applicable solution. To give a more precise idea of the mentioned requirement and the extensiveness of these CPU

cycles, imagine that a 256-bits long hash[1] needs to have an alternating binary series of [10101010…] in its first 40-bits in order to satisfy the proof-of-work. Then a simple probabilistic analysis yields that the average number of random guesses needed to find an applicable hash is 2^{40} which is approximately equal to one trillion individual tries. This seemingly unsurmountable amount of computational effort takes about a mere 10 minutes if the majority of the nodes are working on the same proof-of-work for verification.

Prior to elaborating on the verified transactions, a discussion on how Bitcoin deals with the financial records of its users is in order since *"a key aspect of the Bitcoin protocol is the way it represents and changes the ownership of money."* [1] In centralized economical systems, the trusted third-parties are allowed to hold an extensive record on the income-outcome of their customers which are then presented to the users as their financial balance. In Bitcoin, since there is no central intermediary to hold a record in lieu of the user and since the publicization of a personal balance directly opposes the principle of anonimity in the system; the notion of balance is exchanged for that of a log. In verifying whether or not a user is allowed to transfer a certain amount of coins to another, his or her previous transactions on the public ledger are logged to calculate a total net income which serves as the overall financial balance of the transactor.

Continuingly, verified transactions are then stacked together in *blocks*. These blocks comprise the basis of the blockchain platform as they are responsible for the chronological priorization of transactions to overcome the Double-Spend Problem for which the following example should be enough to visualize:

> Consider an interaction between the users **A**, **B** and **C** where **A** is buying a product supplied by both **B** and **C**. Firstly, **A** transfers the required amount of money to the supplier **B**, from whom the product ships as soon as the transaction is in the public ledger. Assuming **A** has enough money for only one purchase, let us consider what would happen if **A** were to issue another

[1] actual length of an SHA256 digest

purchase from **C** who also ships the product instantly. In a centralized system, the trusted-third party would have checked **A**'s balance as soon as the transaction **A→B** was issued, subsequently halting the purchase **C→A** as **A** does not possess the required amount of money for the transaction. However, in a decentralized system such as Bitcoin, checking **A**'s balance for the validation of the first transaction takes a considerably longer amount of time in which **A** could have initialized a second transaction. Although the second transaction would eventually be illegitimazed by the majority of users, both **B** and **C** would have shipped their products prior to the actual verification of the transaction **A→C**, allowing **A** to have double-spent his limited resources.

The Blockchain platform solves this issue by an inherent verification mechanism which prefers the longest blockchain by default. In this case, to get his or her altered order of transactions accepted, **A** has to supply a longer blockchain than that of the majority of other nodes in order; the probability of which is practically zero *"as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes"*. [2]

Right now, Bitcoin is being hailed by many as the definitive mode of trade for the future which *"may have more impact than the internet"* [3]. While I agree that Bitcoin will play a crucial and disruptive role in our future economy which is evolving at an accelerating rate with unpredictable shifts in the political paradigms, the platform still has major issues to resolve which include various security problems, the unstable currency and the inefficiency of the proof-of-work concept. However, even if Bitcoin were to eventually resolve these inherent issues, it would still be unable to transition into the mainstream economy as people would not be willing to share their private information with the public despite how secure the system is or will be.

Furthermore, it is important to note that *"blockchain technology has attracted attention as the basis of cryptocurrencies such as Bitcoin, but its capabilities extend far beyond that, enabling existing technology applications to be vastly improved and new applications never*

previously practical to be deployed." [4] Bitcoin is as small a part of the Blockchain platform as is Web of the Internet which indicates that Blockchain platform can and will be utilized in many different ways including new ballot systems, publicized resource tracking, programmable money and most importantly, resource-oriented copyright enforcement. While Blockchain avoids many of Bitcoin's short-comings, it suffers from a similar inefficiency which is irresolvable due to the inherent qualities of the system since any attempt to increase the computational power of the nodes also increases that of the harmful sources which then requires even more time-consuming encryption methods *ad infinitum,* eventually prohibiting any increase in the overall efficiency of the system.

References

[1]A. Zohar, "Bitcoin", *Communications of the ACM*, vol. 58, no. 9, pp. 104-113, 2015.

[2]S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3]N. Carlson, "Star Silicon Valley entrepreneur: Here's why bitcoin will be bigger than the internet", *Business Insider*, 2015. [Online]. Available: http://www.businessinsider.com/how-bitcoin-may-have-more-impact-than-the-internet-2015-2. [Accessed: 18- Nov- 2016].

[4]S. Underwood, "Blockchain beyond bitcoin", *Communications of the ACM*, vol. 59, no. 11, pp. 15-17, 2016.