Nurym Kudaibergen

TA: Mevlut Turker Garip

CS 35L

December 8, 2017

Blockchain: Hype or Hope?

One of the trendiest topics in the technology world right now are cryptocurrencies, the most popular being Bitcoin. First introduced in 2008 by a pseudonym Satoshi Nakamoto as a scientific paper, it heavily relies on a technology named “blockchain” that was specifically tailored to fit the needs of the currency. The article “Blockchain: Hype or Hope?” delves into the intricacies of the technology: its core concepts, innovations, and applications.

To understand the concepts behind blockchain, it’s worth noting that the main design goal of Bitcoin as a cryptocurrency is decentralization. Transitioning from traditional fiat currency controlled by governments, Bitcoin strives to give the power to the free market. Decentralization foils the ability of governments to enforce tax laws, follow money trails or prohibit money transfer to certain parties. With the absence of a trusted authority, there is no trivial way of validating transactions. This main problem that arises is solved by introducing the concept of “blockchain”.

In its essence, blockchain is a public ledger (Figure 1) that all parties have access to. Nakamoto went with a very radical idea of publicizing all the transactions that ever happened. The ledger, in principle, is meant to be “append-only” and “immutable”. New records can be added, but previous records are permanent and are not meant to be modified in any way. Each record is called a “block”, where a small set of processed transactions are stored. Each

transaction is simply a statement of person X paying person Y a certain amount of money. The block also contains a pointer to a previously computed block. As a data structure, the ledger is analogous to a linked list, but comes with an important caveat. The pointers are, in reality, hash pointers that also store the hash of the previous block. The hash allows to check whether the previous block was tampered with in any way. Since the ledger stores all transactions from the beginning of Bitcoin, it's possible to trace back to the very first transaction and make sure that all of the records have not been changed, hence "immutable". Unlike traditional money, transactions are not bound to certain identities. Instead, each person is identified with a public key (a string of alphanumeric characters paired with a private key). A person is also incentivized to use multiple public keys to ensure anonymity.

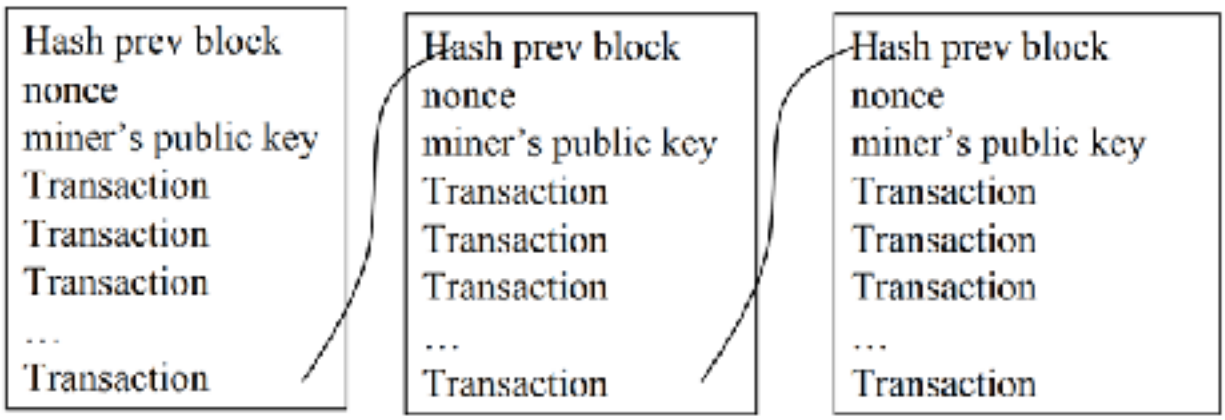

Figure 1. The ledger format

The bitcoin network lies on "miners", computers across the world that process the requested transactions and keep the currency alive. In Figure 1, we can also see the entry for miner's public key. It identifies the miner who was the first to compute the next valid block of transactions. The computation of a block is intentionally made very expensive. The difficulty of the hash computation is adjusted such that the network is collectively able to compute one block

in about ten minutes. The miner that finds the valid hash is rewarded with a certain amount of Bitcoin (that is how new coins are introduced to the system).

The article also discusses the differences between traditional integrity checks (RSA encryption in particular) and the blockchain hash. The integrity check is relevant when one generates a signature signing a certain transaction. With RSA and traditional public-private key system, it's a matter of milliseconds to generate and verify a signature, but it's incredibly computationally expensive to forge one. With 1024 bit RSA keys, it's about 2^{63} times more expensive to forge a signature than to make one. With the blockchain hash, it's just as difficult to generate a signature as it is to forge one. The purpose of making hash computation difficult is to defend against malicious miners who would want to forge hashes, which, in theory, can lead to computations of alternate ledgers with alternate transaction history.

Radia Perlman looks at other applications of blockchain and gives assignment of DNS names, storing health records and timestamping as examples. For each case, Perlman notes how expensive and impractical it is to use blockchain as a backbone of those applications. Since the ledger has to be copied and stored in multiple places, the amount of disk space used becomes incredibly large. On top of that, the sheer amount of computational power that the blockchain hash needs makes the idea of trusting a central party look appealing again. Also, decentralization leads to lack of responsibility in the system. If anything goes wrong, there is no central authority that can resolve disputes among its users. In conclusion, we can see that decentralization achieved by blockchain only fits a limited domain of applications. It's a technology worth experimenting with, but at this time, the most successful application of blockchain is Bitcoin itself.

Works Cited

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved December 8, 2017, from https://bitcoin.org/bitcoin.pdf

Perlman, R. (2017, Summer). Blockchain: Hype or Hope? *;login:*. Retrieved December 8, 2017, from https://www.usenix.org/publications/login/summer2017/perlman