Hashing and Cryptocurrency

CPSC 525 Research Homework

Sangeetha Verkot

***Abstract*—The concept of cryptocurrency was introduced in 1998 as "b-money", an anonymous, distributed electronic cash system. Bitcoin represents the first successful open-source, peer-to-peer cryptocurrency system. Bitcoin uses public key cryptography. Bitcoin mining is the process of authenticating transactions and generating new bitcoins. Hash functions are an essential part of Bitcoin protocol. Bitcoin mining uses the hashcash proof of work function to validate the blockchain transaction log. A wallet stores all the information necessary to transact bitcoins.**

***Index Terms*— Bitcoin, Blockchain, Cryptocurrency, Hash Functions, Mining**

I. Introduction

CRYPTOCURRENCIES are digital assets that can be used a medium to exchange goods or services using cryptography to secure the transactions and to control the creation of additional units of the currency. The notion of a digital currency was first proposed by Wei Dai as a digital currency system, dubbed b-money. Shortly thereafter, Nick Szabo created "Bit Gold". Like bitcoin and other cryptocurrencies that would follow it, Bit Gold was an electronic currency system which required users to complete a proof of work function with solutions being cryptographically put together and published. A currency system based on a reusable proof of work was later created by Hal Finney who followed the work of Dai and Szabo. They have grown in popularity in recent years because of its security, affordability, efficiency, ease of use, and anonymity. Bitcoin is the first successful implementation of a distributed cryptocurrency[11]. In addition to Bitcoin, there are other cryptocurrencies available on the market, collectively known as "altcoins". Ethereum, Litecoin, Ripple and Monero are some examples of altcoins.

II. What is a bitcoin

Bitcoin is a decentralized payment system which uses a peer-to-peer network that provides ways to use a cryptographically strengthened public ledger to record and protect transactions. Bitcoin's existence began with an academic paper written in 2008 by a developer under the pseudonym Satoshi Nakamoto. The first block on the Bitcoin blockchain—block 0—is called the Genesis Block. According to the timestamp in the block header, it was mined on 3 Jan 2009 at 18:15:05 UTC. The first transaction recorded

in the first block was a single transaction paying the reward of 50 new bitcoins to its creator. One important part of that system, is a way to release Bitcoins over time, to reward those people who dedicate their computer power to making the system's infrastructure work. The bitcoin process is limited to about twenty-one million coins. It's estimated that bitcoins will reach this level in 2140.

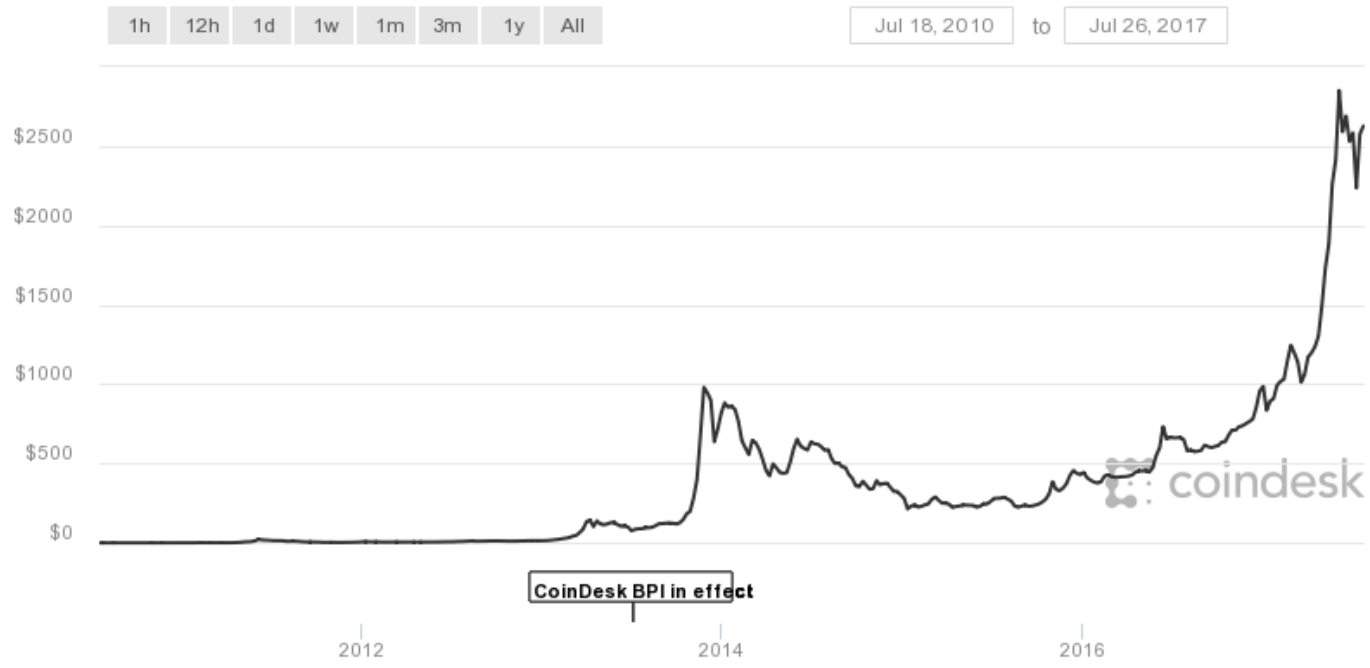


Figure 1 Value of Bitcoin Over the Years (Source: Coindesk)

III. THE BITCOIN NETWORK

The bitcoin network is a peer-to-peer payment network that operates on a cryptographic protocol. Users send and receive bitcoins, the units of currency, by broadcasting digitally signed messages to the network using bitcoin wallet software. Transactions are recorded into a distributed, replicated public database known as the blockchain, with consensus achieved by a proof-of-work system called "mining".

A. Block Hashing Algorithm

Bitcoin mining uses the hashcash proof of work function; the hashcash algorithm requires the following parameters: a service string, a nonce, and a counter [7]. In bitcoin, the service string is encoded in the block header data structure, and includes a version field, the hash of the previous block, the root hash of the merkle tree of all transactions in the block, the current time, and the difficulty. Bitcoin stores the nonce in the extraNonce field which is part of the coinbase transaction, which is stored as the left most leaf node in the merkle tree (the coinbase is the special first transaction in the block). The counter parameter is small at 32-bits so each time it wraps the extraNonce field must be incremented (or otherwise changed) to avoid repeating work. The basics of the hashcash algorithm are quite easy to understand and it is described in more detail here. When mining bitcoin, the hashcash

algorithm repeatedly hashes the block header while incrementing the counter & extraNonce fields. Incrementing the extraNonce field entails recomputing the merkle tree, as the coinbase transaction is the left most leaf node. The block is also occasionally updated as you are working on it.

Bitcoin is using two hash iterations known as “Double Hash” (denoted $SHA256^2$ ie "SHA256 function squared") and the reason for this relates to a partial attack on the smaller but related SHA1 hash. SHA1's resistance to birthday attacks has been partially broken as of 2005 in O(2^64) vs the design O(2^80), with practical attacks having been used successfully in early 2017[10]. While hashcash relies on pre-image resistance and so is not vulnerable to birthday attacks, a generic method of hardening SHA1 against the birthday collision attack is to iterate it twice.

B. Block chain

The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography. Over 16 million bitcoins are in circulation right now [9].

LATEST BLOCKS SEE MORE →

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
478006	2 minutes	1350	$ 111,289,054.15	BTC.com	998.27
478005	4 minutes	1714	$ 28,587,698.75	GoGreenLight	915.11
478004	7 minutes	2228	$ 171,652,150.31	BTCC Pool	989.23
478003	21 minutes	1822	$ 154,729,343.73	ViaBTC	999.16

Figure 2 Latest Blocks (Source: Coindesk)

C. Transactions

A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast between users and usually begin to be confirmed by the network in the following 10 minutes, through a process called mining. The transactions are irreversible, fast and cost very little compared to other money transfer methods.

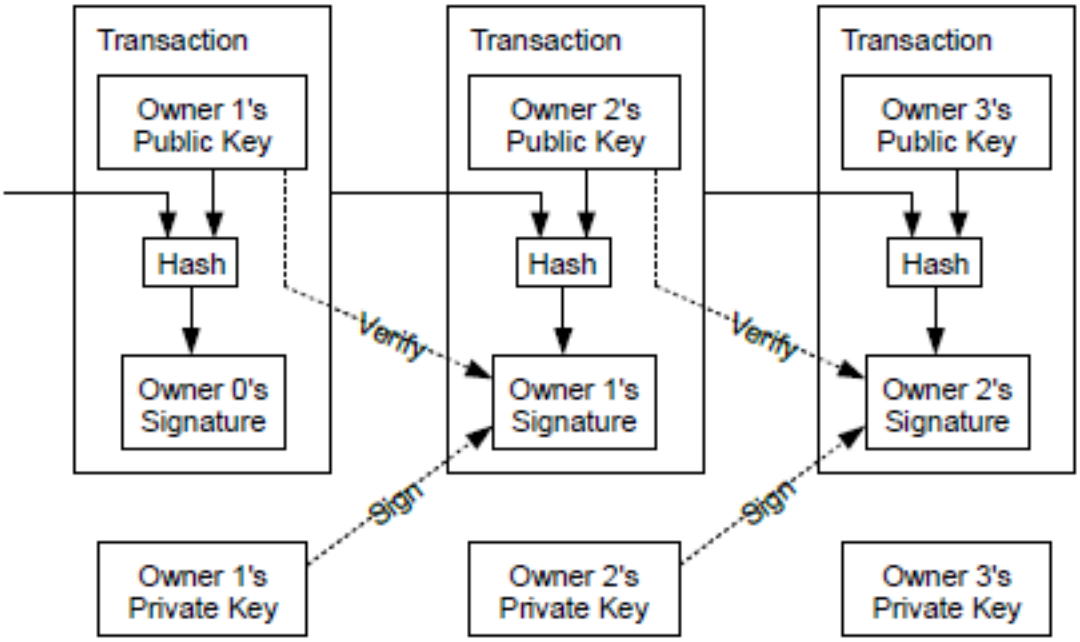


Figure 3 Simplified chain of ownership (Source: Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System)

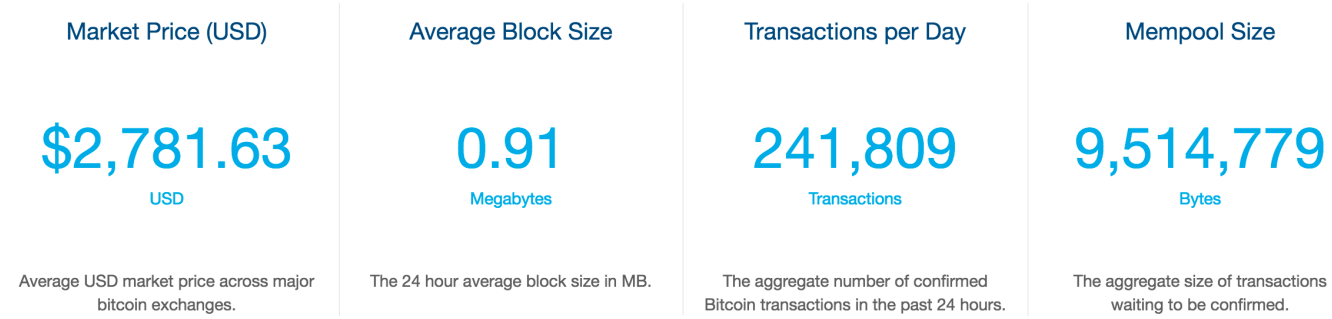
D. Mining

Mining is the process of verifying transactions and creating new bitcoins. Bitcoin mining serves two purposes:

1. Create new bitcoins in a controlled manner.
2. Prevent double spending.

Mining is a distributed consensus system and transactions are constantly being broadcasted over the bitcoin network. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain. This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.

The current reward for mining a bitcoin is $12.5 and the market price is $2,781.63.



E. Wallet

Bitcoin uses public key cryptography which is an encryption scheme that uses two mathematically related keys – a public key and a private key. A bitcoin wallet can be considered as a collection of these keys. Bitcoin wallets facilitate sending and receiving Bitcoins and gives ownership of the Bitcoin balance to the user. So, they can be described as something that "stores the digital credentials for your bitcoin holdings" and allows one to access (and spend) them. A wallet can be stored on the client's desktop, mobile device, on the web or hardware.

F. Security

Bitcoin transactions are sent from and to electronic bitcoin wallets, and are digitally signed for security[10]. Everyone on the network knows about a transaction, and the history of a transaction can be traced back to the point where the bitcoins were produced. Bitcoin uses a cryptographic algorithm known as Elliptic Curve Digital Signature Algorithm to ensure that the currency can only be spent by its rightful owner. The key concepts in this algorithm are a single unsigned 256-bit integer private key that is randomly generated, a public key that is derived from a private key which can either be 33 bytes compressed keys or 65 byte uncompressed keys and a signature which is mathematically generated from a hash of something to be signed, plus a private key.

G. 51% Attack

An interesting concept in bitcoin mining is that an entity with high enough computational power will be able to gain full control of the blockchain. While feasible, the difficulty of the mining algorithm makes such an attack hard to accomplish.

IV. Conclusion

Cryptocurrency is a relatively new and fascinating concept. It is a fast, efficient, inexpensive and secure way to transfer funds between two parties without the need for a central authority. Bitcoin is one of the most popular cryptocurrencies in the market right now. Yet most vendors do not accept bitcoins, though the number is still growing. The concept of cryptocurrency is not

easy for an average person to wrap their head around. That combined with the volatility of the bitcoin market, makes it hard to predict whether the bitcoin and other cryptocurrencies are going to be more mainstream in the near future.

REFERENCES

[1] Satoshi Nakamoto., "Bitcoin: A Peer-to-Peer Electronic Cash System"., https://bitcoin.org/en/, October 31, 2008
[2] https://en.bitcoin.it/wiki/Essay:Bitcoin:_A_Peer-to-Peer_Electronic_Cash_System
[3] Ghassan O. Karame, Elli Androulaki, https://eprint.iacr.org/2012/248.pdf
[4] https://www.coindesk.com/bitcoin-hash-functions-explained/
[5] https://en.bitcoin.it/wiki/Block_hashing_algorithm
[6] https://en.wikipedia.org/wiki/Bitcoin#Wallets
[7] http://www.bitcoinblockhalf.com/
[8] https://en.bitcoin.it/wiki/Hashcash
[9] https://www.coindesk.com/information/how-do-bitcoin-transactions-work/
[10] https://en.bitcoin.it/wiki/Main_Page