**Bits, Blocks, and Chains**

**A Concise Examination of Bitcoin and Cryptocurrency for the Novice**

Richard Givens

Lewis University, College of Arts and Sciences

Department of Computer and Mathematical Science

CPSC 52500: Encryption and Authentication

Abstract

The recent increase of the price of Bitcoin has sparked an interest in the field of cryptocurrency and the technologies supporting it. Once relegated to the fringes of a few early adopters and enthusiasts, Bitcoin now sits squarely in the public eye. Those seeking to understand Bitcoin, cryptocurrency, and blockchain are left sifting through conflicting sources with very little supporting documentation. Overly technical, or overly general, these sources fail to provide a concise examination of Bitcoin and cryptocurrency sufficient for the novice or layperson to understand.

Note, throughout this paper various sources are cited, however direct quotes are seldom used. This paper represents the sum of understanding from these sources.

Keywords: Bitcoin, cryptocurrency, blockchain

Introduction

Bitcoin, Cryptocurrency, Blockchain; occasionally an obscure fad takes root with the general population and creates a fervor, introducing new buzzwords, concepts, and methods which until their public debut, were unknown by the majority. Because of its current market price of 19,336.50 U.S. Dollars (USD), with an overall market cap totaling over 320 billion USD (CoinMarketCap), something once limited to a small segment of the population, early adopters, suddenly lands in the spotlight with little or no explanation preceding it. The effect is akin to a large elephant suddenly dropping from one’s ceiling, and landing in the center of a room. The purpose of this paper is to provide a brief, concise overview of Bitcoin, and will attempt to explain in layman terms the technological concepts driving it.

While the focus of this paper is Bitcoin, the concepts introduced carry over well to other forms of cryptocurrency, also known as altcoin. All cryptocurrency, digital representations of an alternative currency created through cryptography and advanced mathematics, and the methods involving its production rely upon established proofs and theorems; it is merely the implementation method which is unique.

Providing a concise explanation of cryptocurrency such that the layman, or average consumer, can understand is difficult. Though there are many resources which attempt to explain cryptocurrency, there is very little uniformity among them. Indeed, the many forms of cryptocurrency which originated from the idea of Bitcoin exceed one thousand variations; these claim some advantage due to the modification or addition of methods which produce them. While Bitcoin, the earliest and most popular cryptocurrency, and Bitcoin Mining, the production of Bitcoin, have existed for several years, and are based on methods established many years earlier, there is a fundamental lack of scientific knowledge which springs from an assumption that because these methods are based on mathematics and cryptography, there is little need to explain these concepts further. Whether this assumption is based on a perceived collective understanding of the advanced mathematical formulae involved, or a desire to avoid explaining them to others, the result is a heavy reliance on faith and assumption which contradicts common scientific principles and established mathematical proof of methods within cryptography. Nonetheless, the wave of cryptocurrency is gaining momentum, so a basic understanding is both beneficial and desirable.

An important note regarding this paper: There are no assumptions regarding the reader’s level of knowledge in mathematics, cryptography, or cryptocurrency in general. Thus, definitions will follow terms throughout its contents.

What is Bitcoin?

In 2008, an academic research paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” an individual referring to him or herself as Satoshi Nakamoto to a mailing list discussing cryptography, (Marr). Nakanoto’s paper detailed the first cryptocurrency, Bitcoin, describing it as “an electronic payment system based on cryptographic proof instead of trust,” (Nakanoto, 2008). In the introduction, Nakanoto describes the erosion of trust between transaction parties and third-party institutions providing trusted transaction services. In his paper, Nakanoto discusses a method in which willing parties engage in a transaction reliant upon cryptographic proof, thus eliminating the need for trusted third parties, and reducing costs related to transaction processing. Furthermore, this cryptographic proof serves as the security for the transaction, rendering it resistant to fraud or abuse. The Bitcoin is the record of such transactions, containing the most recent transaction itself, and the sum of all previous transactions, digitally authenticated by SHA (Secure Hash Algorithm)-256 cryptographic functions, which create unique mathematical signatures for each Bitcoin yet tie them all together in the blockchain, (Antonopoulos). A detailed description of blockchain is below, however to understand SHA256 hash function, one simply need know that any hash function is a cryptographic method relying upon mathematical calculations performed upon data of variable size (Antonopoulos). An input of variable sized data is hashed via mathematical operations using the specific algorithm, resulting in an output of fixed size (regardless of the original size of the data), in this case 256 bits, which encodes the data as a type of cipher. Due to the compression of the original data, and discarding bits of it to accommodate the fixed size the hashed data, known as the digest, deciphering the plaintext is impossible, except through currently unknown mathematical methods, (Antonopoulos). SHA256 is a type of hash function of the SHA-2 family of hash functions, published in 2001, resists attacks which were successful at breaking previous hash functions, (Pattanayak). In simple terms, the number of attempts required to successfully break the SHA256 function using the most prevalent attack is 2128, or approximately 3.4 multiplied by 1038. When describing Bitcoin, all hash functions are SHA256 and synonymous with the term “hashing”.

What is Blockchain?

As mentioned above, a Bitcoin is the record of the effort required to create the transaction and all previous transactions, residing on a blockchain, or a chain of digital transactions acting as an inalterable electronic ledger consisting of several blocks, timestamped to prevent duplication or alteration, (Antonopoulos). The current block in the chain receives the digest of the previous block header, appending (adding) the digest of the current block’s transactions (of which each undergoes multiple layers of hashing and appending with other current transactions within the block to create a single digest), then appending with version information which dictates the block validation rules, a timestamp, and a difficulty setting, to create a single block header. This header is hashed, and the digest passed to the next block, (Bitcoin Developer Guide

In simple terms, the Bitcoin is a record of the efforts required to create the current block, which consists of the records of the efforts required to create all previous blocks, and thus chains each Bitcoin to every other Bitcoin.

How is Bitcoin “Mined”?

The creation of Bitcoin, or the efforts required to complete the digital transaction of information, is known as mining, (Antonopoulos). Like the physical efforts of mining, Bitcoin mining consists of many operations which may not produce any result for some time. Similarly, it is through the collective efforts of several miners, pooling resources and thus sharing the dividends, that Bitcoin may be created, or mined, with any noticeable result. Those efforts, known as transactions, form a proof of work that, when it meets certain criteria serve as the validation that a moderately difficult cryptographic challenge has been solved.

The proof of work algorithm receives as its input the digest of the previous block’s header, generates a Nonce, or one-time pseudo random number, and then hashes both the digest of the previous block and the Nonce together, (Bitcoin Developer Guide). The digest of this hash is checked against the difficultly and validation requirements contained in the header of the previous block, and determines if it meets these criteria. The block/Bitcoin will only be considered valid if it falls within a certain value threshold, and if its hash is at least as challenging as the difficulty protocol determined by the preceding hash. Among the difficulty criteria is a requirement that the resulting hash must contain an increasing number of preceding zeroes before any other digit, and that the total length of the digest must meet a certain length, (Antonopoulos).

The difficulty involved in generating a single Bitcoin makes the effort too challenging for single or small groups of users (Antonopoulos). While the effort will eventually succeed, the amount of time required to meet the exact requirements at any time creates a perceived loss of value. Thus users, or miners as they are collectively known, often congregate in pools or nodes, (Antonopoulos). These nodes use special computing algorithms which run on host computers to create a distributed network of machines, all attempting to “solve” a block by creating the hash which meets the given criteria. The work completed by each miner is the transaction that is recorded as part of that block. When enough transactions result in a digest which meets the criteria, the block is validated, and the header created. The network of miners then receives the new header and begin computation of the next block in the chain.

How is Bitcoin Secure?

Though a detailed explanation of the security of Bitcoin is possible, it is best to express it simply. Each block contains a digest of the SHA256 hashing algorithm, which consists of the digests of multiple SHA256 hashing algorithms, as well as the SHA256 hash of the header of the previous block. This hashing within hashing within hashing creates a block that is directly tied to the first block created, known as the Genesis Block. SHA256, as part of SHA-2, has thus far remained resistant to the attacks which rendered previous hashing algorithms obsolete requiring an expenditure of effort (using current methods) too monumental to complete. As a newly created block must match certain validation requirements, including verification of the hash of the preceding block’s headers, such that the amount of effort required to forge or alter a block is at least as much, on average, as that required to create a legitimate block.

In simpler terms, the amount of effort required to forge or alter a single Bitcoin is equivalent to the sum of all the effort to create all previous Bitcoins, plus the sum of all the efforts required to create all ensuing Bitcoins, or those Bitcoins created after the forgery effort began.

Summary

Bitcoin, though highly technical in nature relies upon current mathematical models and cryptographic methods, which when explained in simplified terms, are easy to comprehend. The creation of a single Bitcoin relies upon a mathematical computation and multiple SHA256 hashing operations to create a block in a series of blocks which are all connected by their digests. Verifying the integrity of a block is a matter of comparing digests to expected output, and discarding any which fail to meet the given criteria. While breaking the secure hashing algorithm and creating forged or altered blocks is possible, the amount of effort required is so monumental that it would take less to simply attempt to create a legitimate block. All types of cryptocurrency descend from Bitcoin, but claim some advantage over previous methods used. However, the documentation of cryptocurrency is both diverse and vague, rendering a concise explanation based on proven scientific and cryptographic methods extremely difficult.

Works Citied

Antonopoulos, Andreas M. Mastering Bitcoin: Programming the Open Blockchain. O'Reilly, 2017.

“Bitcoin Developer Guide.” Developer Guide - Bitcoin, Bitcoin.org, bitcoin.org/en/developer-guide#block-chain.

“(BTC) Bitcoin (BTC).” *Bitcoin (BTC) Price, Charts, Market Cap, and Other Metrics | CoinMarketCap*, coinmarketcap.com/currencies/bitcoin/.

Marr, Bernard. “A Short History Of Bitcoin And Crypto Currency Everyone Should Read.” Forbes, Forbes Magazine, 6 Dec. 2017, www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/.

Nakanoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto.” Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute, 2008, nakamotoinstitute.org/bitcoin/.

Pattanayak, Anupam. “Revisiting Dedicated and Block Cipher Based Hash Functions.” Academia.edu, www.academia.edu/3037624/Revisiting\_Dedicated\_and\_Block\_Cipher\_based\_Hash\_Functions.