Blockchains: what are they and how do they work?

Arnold F. Shapiro

Smeal College of Business, Penn State University, University Park, PA 16802, USA

Abstract

In 2008, an elusive cryptologist named Satoshi Nakamoto proposed a peer-to-peer electronic cash system called bitcoin, which would allow online payments to be sent directly from one party to another without intervention. The underlying technology behind bitcoin was the blockchain, a decentralized transaction and data management technology. It featured a distributed, immutable digital record system that was shared among many independent parties and could be updated only by their consensus. Although blockchain started off as a core technology of bitcoin, it has emerged as an innovative tool with the potential to impact the way we design a number of online applications.

The purpose of this article is to provide an introduction to blockchains, with an emphasis on what they are and how they work.

1 Introduction

In 1999, the economist Milton Friedman prognosticated that[1]

> The one thing that's missing, but that will soon be developed, is a reliable e-cash. A method whereby, on the internet, you can transfer funds from A to B, without A knowing B or B knowing A. The way in which I can take a 20 dollar bill and hand it over to you and there's no record of where it came from. And you may get that without knowing who I am. That kind of thing will develop on the Internet.

Ten years later, in 2009, an elusive[2] cryptologist named Satoshi Nakamoto implemented bitcoin, the first successful cryptocurrency.[3] The essential features of his bitcoin was that it used cryptography instead of a central bank to provide security and verify transactions, and it was encrypted in a way that prevents it from being copied. Of course, bitcoin was not created in a vacuum; the predecessors of bitcoin are discussed in Halaburda and Sarvary (2016, §4.3).

The underlying technology behind bitcoin was a public blockchain (BC), which can be characterized as:

> An immutable digital ledger of transactions
>
> An open (transparent) ledger
>
> A database that is distributed to all network nodes (computers),[4] obviating the need for a centralized control.

[1] https://www.youtube.com/watch?v=onn34J74dnU http://youtu.be/mlwxdyLnMXM

[2] The pseudonym Satoshi Nakamoto is the name used by the unknown person or people who developed bitcoin. One history of the search for Nakamoto is recounted at https://en.wikipedia.org/wiki/Satoshi_Nakamoto.

[3] In 2009, the first bitcoins were transferred from Satoshi Nakamoto to Hal Finney, as a test. See

> https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?utm_term=.4d0886482796

Another piece of trivia is that on May 22, 2010, Laszlo Hanyecz made the first real-world transaction by buying two pizzas in Jacksonville, Florida, for 10,000 BTC. The price of bitcoin at the time was $0.008 for 1 bitcoin, although the actual cost of the pizza was $25. See

> https://bitcointalk.org/index.php?topic=137.0,
>
> https://en.wikipedia.org/wiki/History_of_bitcoin

[4] A blockchain is very similar to the concept of relational databases proposed by Codd (1970). In fact, Lind and Barner (2018: 38) assert that, in essence, a blockchain is a relational database.

In the foregoing, we differentiate between a public BC, which anyone can sign on to, and a private BC, which offers a degree of exclusivity, in that participation is by invitation only. In this article, we explore public BC characteristics.

The article proceeds as follows. It begins with a conceptualizing of the problem that BC is intended to solve. This is followed by an explanation of the BC solution. The topics addressed include: the concept of ownership, an open ledger, a distributed open ledger, the mining process, the hash function, proof-of-work, and the relationship between blocks of the BC. The article end with a comment with respect to subsequent versions of this preliminary article.

2 Conceptualizing the problem

We begin by conceptualizing the problem that a public BC is intended to solve. To this end, consider the traditional money transfer transaction depicted in Figure 1. The players are A, a client, B, a merchant, and a trusted 3rd party. [5]

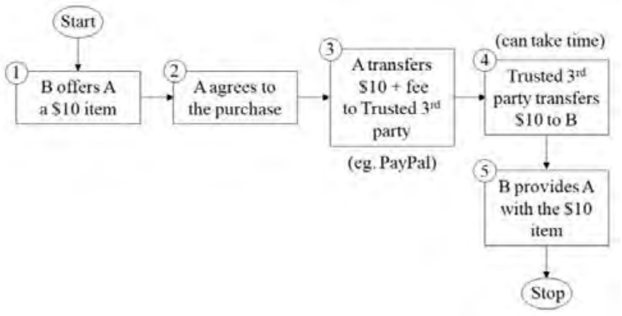

Start
1
B offers A a $10 item
2
A agrees to the purchase
3
A transfers $10 + fee to Trusted 3rd party
(eg. PayPal)
(can take time)
4
Trusted 3rd party transfers $10 to B
5
B provides A with the $10 item
Stop

Figure 1: Traditional money transfer transaction

Here, B offers A a $10 item, A agrees to the purchase, and transfers $10 plus a fee to a trusted 3rd party (a bank, say, or PayPal), that verifies that A has the required $10, and that the payment was made on behalf of B.

From a BC perspective, the problems that this scenario presents are the involvement of the trusted 3rd party, and the amount of disclosure associated with that, the size of the fees, and, depending on the nature of the transaction (e.g. a certified bank draft to a party in a foreign country) the time involved.

Figure 2 shows the characteristics of a preferred transaction format, which is Peer-to-Peer (P2P), that is, directly from A to B, as represented by the solid line. Under this scenario, the issues associated with a centralized trusted 3rd party would be eliminated.

[5] Portions of this section are adapted from Rubin (2016).

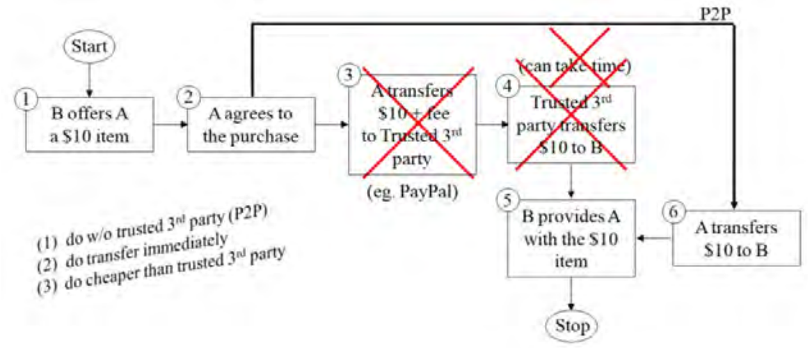

P2P
Start
1
B offers A a $10 item
2
A agrees to the purchase
3
~~A transfers $10 + fee to Trusted 3rd party~~
(eg. PayPal)
4
~~(can take time)~~
~~Trusted 3rd party transfers $10 to B~~
5
B provides A with the $10 item
6
A transfers $10 to B
Stop
(1) do w/o trusted 3rd party (P2P)
(2) do transfer immediately
(3) do cheaper than trusted 3rd party

Figure 2: A preferred transaction format

3 The Blockchain Solution

The solution depicted in Figure 2 can be implemented using a BC. Specifically, the BC can be used to provide a distributed open ledger to all participants, thereby eliminating the need for the trusted 3rd party, and it can also provide a vehicle for validating transactions and updating the ledger. In this section, we use a BC metaphor to illustrate how these things can be achieved.[6]

3.1The concept of ownership

Before proceeding, we need to deal with the concept of ownership, because, unlike the fiat money in general use (dollar, Euros, etc), which can be held in ones hand, cryptocurrencies only exist as a record in a ledger. To "own" the cryptocurrency means having the ability to transfer control of it to someone else.

In the BC metaphor of this section, although dollars are used for illustration purposes, they are assumed to be governed by the concept of ownership associated with cryptocurrency.

3.2An open ledger

As mentioned previously, BCs fall into two primary categories:

1. Those with open ledgers, such as the Bitcoin BC, which are designed to accommodate anonymous actors in the network, and

2. Those with private ledgers, where participation is by invitation only and participants must be identifiable

Here, we focus on the open ledger.

Our BC metaphor begins with a discussion of the open immutable ledger depicted in Figure 3. The ledger is characterized as immutable because once an entry is made, it cannot be changed.

[6] Portions of this section are adapted from Rubin (2016).

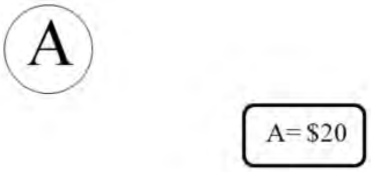


Figure 3: Open ledger

As indicated, it is assumed that there is an individual, A, who has a credit of $20 that is documented in the ledger. Moreover, access to the $20 credit depends on a public/private key combination. A must know the location of the $20 credit in the ledger, which is determined by the public key, and possess the private key that provides access.[7] Without the private key, no one has access to the $20.

A "spends" this $20, or some portion of it, by assigning it to someone else.

Now, A seeks to assign $10 to B. Once it is verified[8] that A, indeed, has $10 to assign to B, the transaction takes place, is documented in a block[9], as represented in Figure 4, and the block is chained to the previous open ledger.

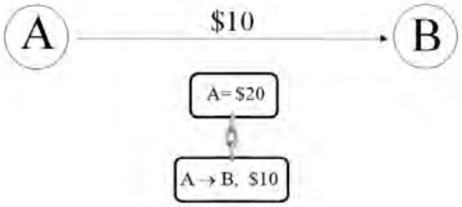


Figure 4: A assigns $10 to B

After an additional two assignments, verifications, and ledger entries, the situation is as depicted in Figure 5.

[7] See Rykwalder (2014) for a discussion of bitcoin keys and the math behind them.

[8] With Bitcoin, for example, after a transaction is created, it is forwarded to neighboring nodes (computers) until it gets propagated across the entire network. "As per protocol, each node needs to verify the correctness of a transaction before forwarding it to its neighbors, ensuring that only valid transactions are propagated and included in a block (invalid transactions are discarded by a node that encounters them)." [Cruz (2017: 26)]   To this end, as discussed in Antonopoulos (2014: 180), each node verifies every transaction against a checklist of criteria.

[9] In practice, many transactions would be included in a block. See Figure 10.

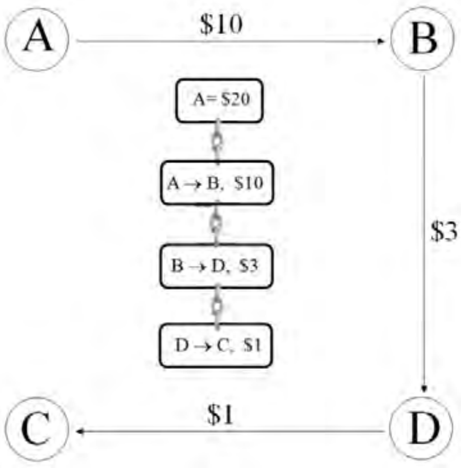


Figure 5: Further assignments to D and C

We note in passing that the open ledger thwarts any attempt at "double payment". For example, assume A now attempts to assign $15 to C. During the verification stage, it would be clear that A only has access to $10 ($20 minus the $10 assigned to B), so the transaction would be prohibited.

3.3A distributed open ledger

Given the open ledger of §3.2, the next step in our BC metaphor is to distribute the ledger, as shown in Figure 6.

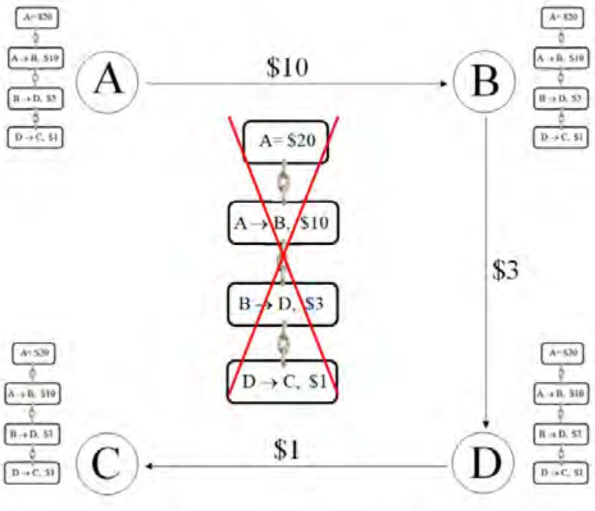


Figure 6: A distributed open ledger

As indicated, a copy of the open ledger is distributed to each of the individuals (actually, their nodes or computers), and the centralized open ledger is eliminated.

But now, this creates a new problem, how do the distributed ledgers get updated when there is a transaction? This problem is addressed in §3.4.

3.4The mining process

Under this public BC approach, the updating of the distributed ledger is accomplished by a process called mining, which is described in this subsection. Before proceeding, however, an understanding is needed of the terms mining, miner, hash, and proof-of-work (PoW).

3.4.1 Mining

The mining process involves 2 tasks: updating the distributed open ledgers and creating new cryptocurrency.

We have not yet addressed the issue of where cryptocurrency comes from (eg., in the context of our metaphor, where did A get the original $20). As it turns out, cryptocurrency is created during the mining process, and is used to compensate the miners for their efforts and expenditures. The only other way to have access to cryptocurrency is to purchase it.

Nakamoto (2008: 4) used the term mining because the process is similar to the mining of gold. The expenditure required to create new coins is analogous to gold miners expending resources to discover gold. In the case of BC, it is CPU time and electricity that is expended.

3.4.2 Miners

To facilitate the discussion of miners, we continue our BC metaphor, and assume that B would like to assign $5 to C, as depicted in Figure 7. The tasks we are confronted with are (1) validate the transaction, and (2) extend the ledgers.

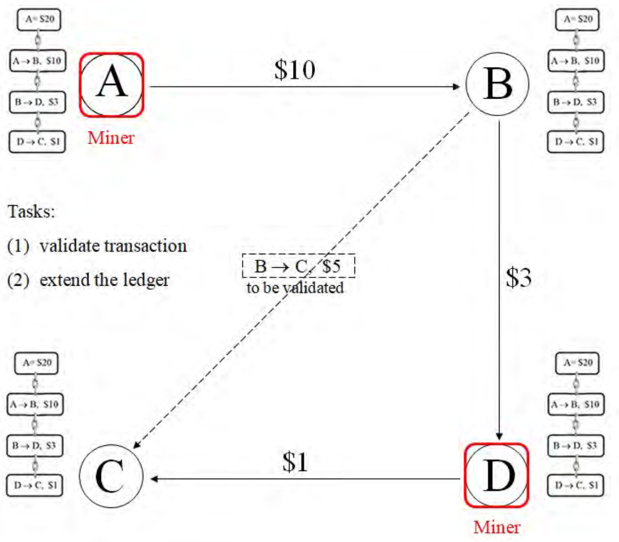


Figure 7: B seeks to assigns $5 to C; A and D are miners

Based on the figure, we assume that A and D have decided to become miners, so their nodes (computers) have been so labeled. Once the transactions have been validated, these miners seek to perform two tasks: solving a PoW puzzle and extending the BC to include a block of validated transactions.

The purpose of the PoW puzzle is to deter service abuses on a network by requiring some work from the service requester, which usually involves computer processing time.

In exchange for being the first miner to complete the PoW puzzle, and extending the BC, the winning miner receives a BC payment and an additional payment of transaction fees that are associated with each of the miner's included transactions.

3.4.3 The hash function

A key component of the public BC is a one-way function called a cryptographic hash function, or just hash function. It is one-way in the sense that if the function is applied to an array of values, the results of the hash function cannot be manipulated to reproduce the original array of values.

A common hash function is the Secure Hash Algorithm - 256, that is, SHA-256, which produces a hash function of 256-bit (64 hexadecimal characters).[10]

SHA-256 is applied in: [https://en.bitcoin.it/wiki/SHA-256]

1. Mining, where it is used as the PoW algorithm (discussed in §3.4.4), and

2. The creation of BC addresses, where it is used to improve security and privacy.[11]

As an example, consider the two hashes:

SHA-256 hash of "2018 Actuarial Research Conference"
33d2366fcf57e8172d740d64aecac1759012cb34d4bd04fbd8dda23510c8654c

SHA-256 hash of "2017 Actuarial Research Conference"
1145c87db918b5453a9a3155b5445c5cf286bac4eb39033c14c13599c8abfaa8

Notice if just one character is changed ("7" in 2017 instead of "8" in 2018), it results in an entirely different hash.

It is worth noting that hashes have been around for some time, a common use being for password protection. When a password is initiated on the web, what is retained is the hash of the password, and at each log on, when the password is entered, it is hashed and that hash is

[10] The details and mathematics of SHA-256 are discussed in Penard and van Werkhoven (2008) and FIPS (2015-08).

[11] In the case of bitcoin, for example, the location (address) of the bitcoin is a double hash of a public key.

compared with the one on record. That way, if the facility is hacked, the hacker can only obtain the hash of the password, which cannot be use to sign in.

3.4.4 Proof-of-Work-type example

As a PoW-type example, suppose that the string we were trying to hash is "hello world"

Our goal, in a PoW-context, might be to produce a hash that begins with the value "0000", which is called the target.

As shown below, we vary the string by concatenating an integer value to the end, called a nonce, starting at 0, and incrementing it each time. After each iteration, we check whether the hash, at that iteration, has satisfied the target. Thus,

```
"Hello, world!0" ⇒ 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" ⇒ e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
...
"Hello, world!1000" ⇒ f0983a3985af146ee611ffa5f9d036000c4dd42370935b0ad26a7c47f1c047d8
...
"Hello, world!4249" ⇒ c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" ⇒ 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

In this example, finding a match for "Hello, world" takes 4,251 tries.

In an actual PoW situation, the target might be a hash beginning with 18 zeros, or more, which would take many more iterations. See, for example, Figure 9.

Proof-of-work has been criticized for being an inherently wasteful consensus system, and other systems, such as proof-of-stake,[12] have been suggested. However, Catalini and Gans (2017) note that "from a game theoretic perspective it is exactly the wasteful nature of the mining computations that defends the ledger from an attack, [because] the sunk, irreversible commitment to the audit trail constitutes the cost a bad actor would have to sustain to manipulate it."

3.4.5 The mining solution (cont)

Getting back to the problem at hand, the miners, nodes A and D, in this case, once the transactions are validated, each strive to be the first to complete the PoW puzzle, and, thereby, qualify to be the one to add the transaction to the ledger.

For the sake of discussion, assume that D was the PoW winner. D would forward the solved block to the other miner, A, who would validate that the nonce is the solution for the block. If that is the case, that information would be conveyed to the other nodes, and all the ledgers would be updated, as shown in Figure 8.

[12] See Chepurnoy et al (2018) for a commentary on proof-of-work and proof-of-stake.

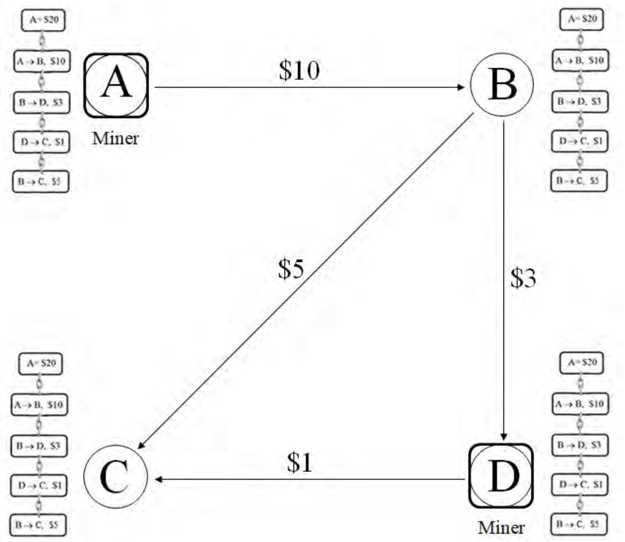
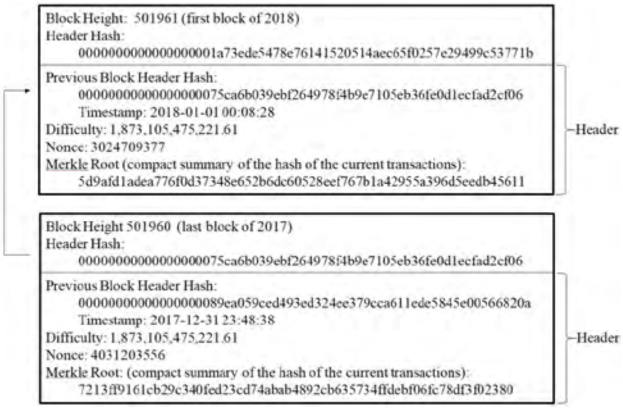


Figure 8:The updated network

Note that mining facilitates consensus where no party needs to know or trust another.

3.4.6 The relationship between blocks of the BC

This subsection provides further insight into how the blocks in the BC are chained together. A representation of this is shown in Figure 9.



Block Height: 501961 (first block of 2018)
Header Hash:
0000000000000000001a73ede5478e76141520514aec65f0257e29499c53771b
Previous Block Header Hash:
00000000000000000075ca6b039ebf264978f4b9e7105eb36fe0d1ecfad2cf06
Timestamp: 2018-01-01 00:08:28
Difficulty: 1,873,105,475,221.61
Nonce: 3024709377
Merkle Root (compact summary of the hash of the current transactions):
5d9afd1adea776f0d37348e652b6dc60528eef767b1a42955a396d5eedb45611

Block Height 501960 (last block of 2017)
Header Hash:
00000000000000000075ca6b039ebf264978f4b9e7105eb36fe0d1ecfad2cf06
Previous Block Header Hash:
00000000000000000089ea059ced493ed324ee379cca611ede5845e00566820a
Timestamp: 2017-12-31 23:48:38
Difficulty: 1,873,105,475,221.61
Nonce: 4031203556
Merkle Root: (compact summary of the hash of the current transactions):
7213ff9161cb29c340fed23cd74abab4892cb635734ffdebf06fc78df3f02380

Figure 9: The chaining of blocks

The important thing is that transactions are grouped into blocks, and the blocks are chained (interconnected) together, hence, the name blockchain.

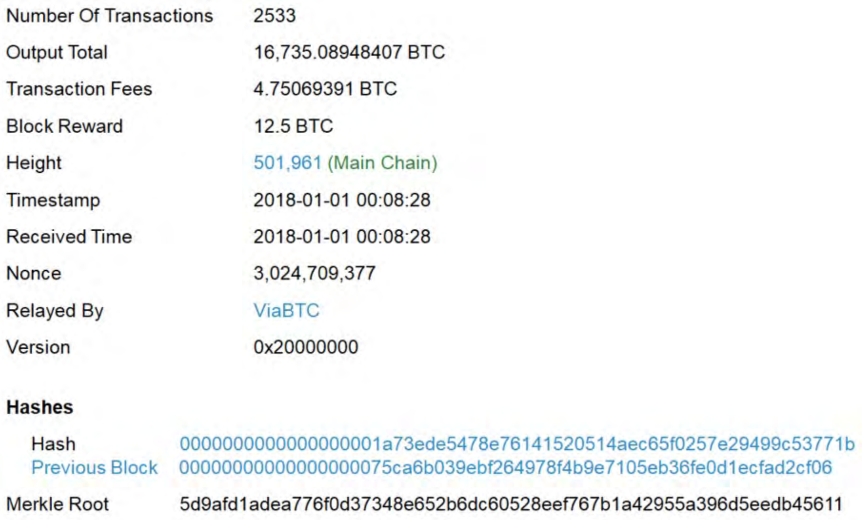
Now, each of these blocks has a header that describes them and their transactions, and each of these headers has a hash of that information.

The chaining is accomplished by including the hash of the previous block in the hash of the current block. For example, the hash of block 501960, the last bitcoin block of 2017 (indicated by the tail of the arrow) is included in block 501961, the first bitcoin block of 2018 (as indicated by the head of the arrow). In this way, cryptographic hashes are used to chain the blocks of the BC together.

A takeaway is that if any change is made in a previous block, it will be propagated through all the blocks, and the change will be obvious to all the nodes because of the open ledger.

3.4.7 Items of a block

Figure 10 provides some of the contents of the actual bitcoin block 501961.



Number Of Transactions	2533
Output Total	16,735.08948407 BTC
Transaction Fees	4.75069391 BTC
Block Reward	12.5 BTC
Height	501,961 (Main Chain)
Timestamp	2018-01-01 00:08:28
Received Time	2018-01-01 00:08:28
Nonce	3,024,709,377
Relayed By	ViaBTC
Version	0x20000000
Hashes	
Hash	0000000000000000001a73ede5478e76141520514aec65f0257e29499c53771b
Previous Block	00000000000000000075ca6b039ebf264978f4b9e7105eb36fe0d1ecfad2cf06
Merkle Root	5d9afd1adea776f0d37348e652b6dc60528eef767b1a42955a396d5eedb45611

Figure 10: Bitcoin block # 501961

Notable entries in this case are the number of transactions, 2,533, the timestamp, which gives the date and time, January 1, 2018 and 8 minutes 28 seconds, the nonce, of just over 3B, associated with the winning PoW, and the hashes of the current and previous blocks. The Merkle Root, shown on the last line, is a compact summary of the hash of the current transactions.[13]

4 Comments

In this article, we explored the characteristics of the basic public BC. This included a conceptualizing of the problem a public BC is intended to resolve, and a step by step discussion of the BC solution.

This version of this article should be viewed as preliminary, however. Subsequent versions will extend the discussion to include (1) public BCs that incorporate smart contracts, such as the Ethereum BC[14], (2) private BCs, which use alternate forms of consensus that do not involve mining, such as Hyperledger[15], and (3) insurance applications involving the foregoing.

[13] See Nakamoto (2008, §7)

[14] See, for example, https://www.ethereum.org/ and Wood (2018-02-25)

[15] See https://hyperledger-fabric.readthedocs.io/en/latest/

References

Antonopoulos, A. M. (2014) Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, Inc.

Catalini, C., Gans, J. S. (2017) "Some Simple Economics of the Blockchain (September 21, 2017). Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16. Available at SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598

Chepurnoy, A., Duong, T., Fan, L., Zhou, H.-S. (2018) "TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake," Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, 1-13.

Codd, E. F. (1970) "A relational model for large shared data banks," Comm. ACM 13(6), 377-387.

Cruz, J. P. M. (2017) The Bitcoin Network as Platform for Role-Based Access Control and Electronic Voting: Using Blockchain-Based Technology to Create Innovative Systems, Doctoral Dissertation, Nara Institute of Science and Technology

FIPS (2015-08) Secure Hash Standard https://csrc.nist.gov/csrc/media/publications/fips/180/4/final/documents/fips180-4-draft-aug2014.pdf

Halaburda, H., Sarvary, M. (2016) Beyond Bitcoin - The Economics of Digital Currencies, Palgrave Macmillan, England

Lind, M., Barner, K. (2018) Finance Unleashed: Leveraging the CFO for Innovation, Springer International Publishing AG

Nakamoto, S. (2008) "Bitcoin: a peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf

Penard, W., van Werkhoven, T. (2008) "On the secure hash algorithm family" https://docplayer.net/8726635-Chapter-1-on-the-secure-hash-algorithm-family.html

Rykwalder, E. (2014) "The math behind the bitcoin," https://www.coindesk.com/math-behind-bitcoin/

Rubin, S. (2016) "What is Blockchain," Citi Innovation Lab https://www.youtube.com/watch?v=93E_GzvpMA0

Wood, G. (2018-02-25) "Ethereum: A Secure Decentralised Generalised Transaction Ledger" https://ethereum.github.io/yellowpaper/paper.pdf