Homework Assignment #1:
Explanation of Key Blockchain Technology

Tanner Jones
Samuel Perl
Blockchain Fundamentals
September 20, 2022

Tanner Jones

Abstract

This paper will explain the use of blockchain and two key components. The use of a ledger isn't something new, but blockchain uses a digital ledger where all the transactions are distributed on the peer-to-peer (P2P) network. The transactions are added to the P2P network and validated by the users. Traditionally, a bank is the centralized authority, but in the use of decentralization, there is no central authority. The transactions are added to a block and are validated by miners. Two technologies that make blockchain possible are hash functions and distributed consensus. Blockchain is widely used for cryptocurrency, so I will be using the popular cryptocurrency called Bitcoin to demonstrate these two components. The technologies have similarities to other internet technologies such as relational databases. I will compare the differences between the digital ledgers and relational databases. Blockchain offers several benefits, and it has been widely considered for other applications. There are several things that need to be considered before implementing blockchain technologies into existing and new applications.

Tanner Jones

Blockchain Major Technologies

Within Bitcoin's blockchain, transactions are added to a public digital ledger, and when a new transaction occurs, everyone is notified of the new transaction at a random interval. The transactions are grouped together into a block. The block is limited to a 1MG block size limit which may consist of 10 or up to 3500 transactions (Blockchain, 2022). The blocks are added to the network and connected through hash or a hash pointer. These blocks are connected and create a tamper-proof block of data, hence the name blockchain. The blocks are mined by nodes or computers that are incentivized by transaction and block rewards. Each block is validated by solving a computation puzzle, and the block is added to the chain. Next, I will explain how hash functions are used within a blockchain.

Hash Functions

A hash function is a one-way mathematical function that can take an input string of any size and produce a fixed-sized output. The fixed-size length varies on the hash function used, but a SHA-256 is a common hash function which produces a 256-bit output. The hash acts as both the ID when requesting peers for the block and validation of the block once we have received it (Narayanan, 2016 pg. 41). Computing hashes is efficient and needs to have 3 properties to be a secure hashing function (Narayanan, 2016 pg. 2). I will briefly explain the properties and how they are important within a blockchain.

Property #1: Collision Resistance

It is important that every hash output is unique given its inputs. A collision occurs when two different inputs produce the same output. For example, if I were to generate a hash using the SHA-256 hashing algorithm and take the following strings as an input, the return would be a random output:

Figure 1: Collision Resistance

An example of a collision is if one were to input a complete different string, it would produce the same output as demonstrated below.

Figure 2: Transaction Hash

The SHA-256 hash function is collision resistant, or the likelihood of it occurring is statically unlikely. The example provided above was created to demonstrate what it would look like if a collision were to occur. Why is this important? Hash functions are used to validate the integrity of the data, and if the hash function isn't resistant to collisions, the data cannot be trusted. In a decentralized network, the integrity of the transactions within a block is validated by the hash.

Property #2: Hiding

The second property is hiding. The hiding property is given the output of the function y = H(x), so there is no feasible way to figure out what the input was (Narayanan, 2016 pg. 5). It is vital that the hashing algorithm being used is high min-entropy, meaning it is difficult to predict

what the outcome will be. Randomness is vital to ensure that when one character is changed in each input that it produces a completely different output.

Property #3: Puzzle Friendliness

The third property is puzzle friendliness, which is a bit more complicated to understand. Bitcoin uses computational puzzles to validate transactions. How does Bitcoin uses hash values to validate blocks? The miners try and solve mathematical puzzle called the nonce. The nonce in Bitcoin is the first 64 bits of the 256-bit hash. If a hash function is puzzle friendly, then there is no solving strategy for this type other than trying random values (Bettati, 2018). Solving this puzzle needs to be computationally taxing, which incentives the nodes to not subvert the process.

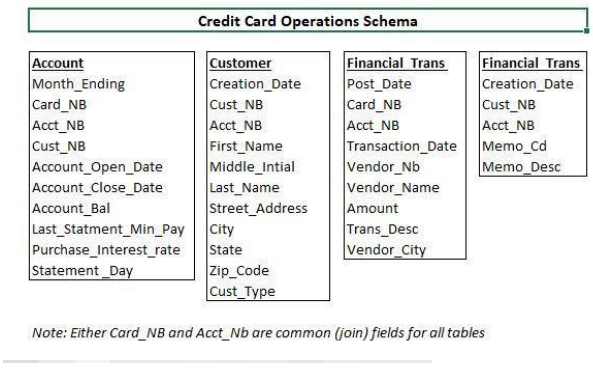
Consensus Algorithms

Bitcoin mining is the act of randomly guessing the nonce which creates the proof-of-work. The proof-of-works shows that certain amount of computation effort has been extended. Consensus takes place on a block-by-block basis (Narayanan, 2016 pg. 31). The block is validated 6 times, and the proof of work is achieved every 10 minutes on average. The first one to compute the nonce receives a transaction fee. The other incentive is called a block reward. The block reward allows the user that creates a block to receive a Bitcoin in exchange for the service of creating a block on the blockchain.

How many Bitcoins are there? Bitcoins are created when new blocks are added to the blockchain. The fixed amount started at 50 Bitcoins and halves every 210,000 blocks created. There is a fixed number of Bitcoins, which is 21 million. At the rate of halving every 210,000 blocks, that amount will be reached at 2140 (Narayanan, 2016 pg. 39). “That is the ultimate nature of truth in Bitcoin: ownership of bitcoins is nothing more than other nodes agreeing that a given party owns those bitcoins” (Narayanan, 2016 pg. 47).

Traditional Internet Component

In traditional finance networks such as credit card networks, there is a central authority such as a bank. The information is stored in different tables that are stored in a database. The database could contain tables with usernames, personal information, passwords (hopefully hashed passwords), and transactions. The relational database uses a key-pair to store information. For example, a key could be call “customer” which contains my demographic data such as name and address (Mills, 2021). All of my data is tracked and maintained by the centralized authority. If I use my Visa credit card to purchase a new laptop, the credit card company will know the location, price, seller, time, etc. and my purchase is easily trackable. I am not anonymous. There is one central power or controller that has custody of my data. The figure to the right is a simplified version of credit card schema. This is the information that is tracked by a financial institution.



Tanner Jones

The use of a decentralized rather than a centralized system changes the situation entirely. The transaction is recorded on the public ledger, randomly assigned to a block, and the block is verified and added to the blockchain for everyone on the network to see. The data that is shared on the blockchain is different and is more anonymous by design. In a blockchain, I have anonymity and a level of privacy.

In Bitcoin blockchain, the nodes (users) are random key value pairs. The first key is the public key which is used as an address or name. The public key is publicly available for everyone to see. The second key is the private key. The private key is mathematically tied to the public key. Due to the nature of the keys, the key-value pair is used to verify which node (user) owns which bitcoins. It is vital that your private key is not shared, because if anyone were to have access to your private key, they can steal your Bitcoins. Every public is tied back to an individual or entity. The image shows the details of the transaction such as the data, amount, transaction fee, hash, and which person paid who.

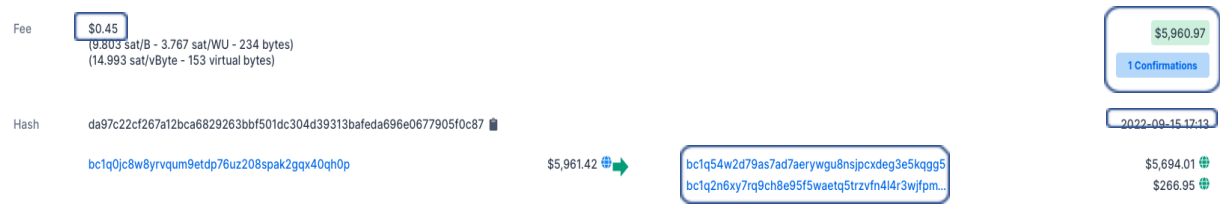


Figure SEQ Figure * ARABIC 4: Bitcoin Transaction:
https://www.blockchain.com/btc/tx/da97c22cf267a12bca6829263bbf501dc304d39313bafeda696e0677905f0c87

Blockchain differs from traditional databases for several reasons, but the biggest difference is the use of a decentralized public ledger that allows everyone to see what transactions are occurring. The data is anonymized, and cryptographic technology is used to generate a key-value pair that connects the data by hash pointers that are stored into blocks. The traditional database uses key-pairs to store the data and is centrally controlled. Each technology has its use-case, and one isn't considered to be better than the other. The figure below outlines some of the benefits of a traditional database and blockchain (Bhardwaj, 2021).

Traditional Database Use	Blockchain Use Case
Confidential Records	Financial Transfers
Relational Data	Real-time Data Exchange
Conventional Storage Systems	Identifying and Authenticating Records
Data That Would be Frequently Modified	Decentral Applications (dApps)

Figure 5: Traditional DB vs. Blockchain

The use of blockchain does have its drawbacks. It is important to consider the drawbacks of blockchain in the technical details of how it works. Components of blockchain can be altered to meet the needs of the data and processes being ran on a blockchain. Cryptocurrency isn't the only use-case of blockchains, though it is the most popular. Bitcoin is only one cryptocurrency of thousands of altcoins based on similar blockchain architecture. The distributed consensus is a slow process, high energy consuming, efficient, and lacks interoperability. The creation of other altcoins like Ethereum and BitCash were developed to

change certain parameters of the Bitcoin blockchain such as 10-minute distributed consensus or the time it takes to validate a block or the block size itself (Narayanan, 2016 pg. 243).

Problems Aspects with Blockchain Technology

The use of blockchain doesn't solve the problem, but rather it is a component used within a product service to solve a problem. Often in business proposals, people recommend that blockchain be used when they don't fully understand the technical implications of using blockchain technology. People often think that they should implement a blockchain rather than a traditional database. Just because it works in Bitcoin, they assume it should work in a business application. As mentioned earlier, there are benefits and drawbacks of using blockchain technology which need to be properly considered. Other problem aspects of blockchain technology solutions that need to be considered are scalability, maintenance, fraudulent/illegal behavior, privacy, development/debugging, control, customer/user buy-in, and policy and governance (Iredale, 2022). The human aspects of business interaction remain when implementing blockchain. The Blockchain Decision Tree is a great reference when considering using blockchain technology. Figure 6 outlines the decision tree and some questions that you should ask when evaluating blockchain (Pedersen, 2019).

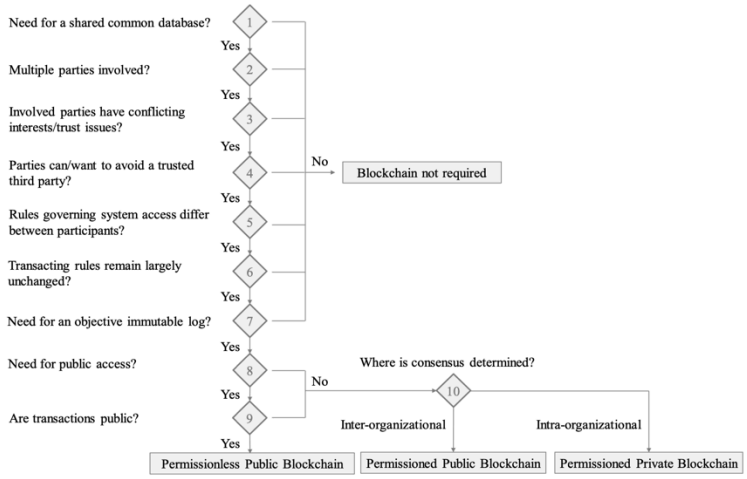


Figure 6: Blockchain Decision Tree

The benefits of blockchain technology such as smart contracts are promising, but due diligence is necessary to ensure the correct technology is being used to satisfy the specific business requirements. The future could be greatly impacted by the use of blockchain and other technologies that will be influenced by blockchain-related technologies.

References

Bettati, R. (2018). *Intro to cryptography and Cryptocurrencies - Texas A&M University*. Texas A&M University Engineering. Retrieved September 16, 2022, from https://people.engr.tamu.edu/bettati/Courses/489CryptoCurrencies/2017A/Slides/CryptoAndCryptoCurrencies.pdf

Bhardwaj, C. (2021, September 22). *Blockchain vs traditional database: Which is better for a startup?* Appinventiv. Retrieved September 16, 2022, from https://appinventiv.com/blog/traditional-database-vs-blockchain/

blockchain, blockchain. (2022). *Explorer*. Blockchain.com | Explorer. Retrieved September 16, 2022, from https://www.blockchain.com/explorer

Iredale, G. (2022, August 15). *Top disadvantages of Blockchain technology*. 101 Blockchains. Retrieved September 16, 2022, from https://101blockchains.com/disadvantages-of-blockchain/

Mills, R. (2021, February 22). *Build a sample customer database tool - any size database one click*. Excel and VBA Craftsman. Retrieved September 16, 2022, from http://excelandvbacraftsman.com/build-a-sample-database/

Narayanan, A. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Pedersen, A. B., Risius, M., & Beck, R. (2019, June). *A ten-step decision path to determine when to use Blockchain Technologies*. Research Gate. Retrieved September 16, 2022, from https://www.researchgate.net/profile/Marten-Risius/publication/333545589_A_Ten-Step_Decision_Path_to_Determine_When_to_Use_Blockchain_Technologies/links/5d38fc9b4585153e591f52cb/A-Ten-Step-Decision-Path-to-Determine-When-to-Use-Blockchain-Technologies.pdf

Paralect, P. (2022). *Particles*. Particles, by Paralect. Retrieved September 16, 2022, from https://blog.paralect.com/