Blockchain – A Data Structure

Blockchain is one the most interesting topics currently. It has grabbed the attention as every person in the tech field and even others who are interested in making the quick dime are looking into it. In this paper I will explore what exactly a blockchain is by researching its history, its current and future uses, how it works and try writing a personal piece of code that relates to this technology.

When I was browsing different topics, I found one or two topics on which I felt to write a paper, but nothing grabbed my attention like blockchain. When I researched a bit more about it, I found out that essentially, blockchain is a linked list. I will talk more about how blockchain works in depth on page three.

It is interesting to see that big companies like IBM and Google have already started adopting to this new technology and integrating in into their operations. This gives evidence to the theory that this piece of technology isn’t a one hit wonder with the Blockchain but has uses in countless other fields.

Some of the interesting fields that can use it in the real world are in car keys, smart appliances and one of my favorite topics, Internet of Things. Internet of Things (IoT) is basically a set of interconnected computing talking to each other without human interference.

Before we look at what a blockchain is we need to understand the concept of decentralization.

What is decentralization?

Decentralization is basically a system in which no single entity has absolute control over the system. 

The above picture is a representation of what a decentralized system looks like. None of the nodes above have sole authority over all the nodes.

A simple example of decentralized network is of a fast food franchise where every restaurant in the chain is responsible for its own operation.

What is blockchain?

Blockchain is a technology invented by Satoshi Nakamoto which is a pseudonym used by a person or a group of people. Originally, this technology was created for the cryptocurrency Bitcoin, but it is so versatile that it has numerous uses in many different industries.

Blockchain is a technology that allows information to be distributed without being copied. This is done by using Hash values. Using hash functions, a piece of information can be converted into a string of letters and numbers that correspond to that particular piece of information. This string of letters and numbers is called hash value. This hash value is unique to that piece of information and changes as soon as there is any change in the information, signaling that some change has occurred in it.

History of blockchain

Blockchain technology was created by person/group of people named Satoshi Nakamoto for developing a decentralized cryptocurrency which was named Bitcoin. Some people say Satoshi Nakamoto is a group of companies (Sa(Samsung)Toshi(Toshiba) Naka(Nakamichi) Moto(Motorola)) but there is no proof. Satoshi Nakamoto owns 980,000 bitcoins. It is very interesting that 0 bitcoins have been spend by Satoshi even with his gigantic fortune.

Bitcoin

Bitcoin is where it all started, when a person/ group of people created it using the concept of blockchain technology. Here are the main points worth noting:

1. First cryptocurrency ever created using blockchain technology
2. It is decentralized, which means no one controls its network.
3. It has limited supply unlike centralized currencies (dollars, rupees etc.) In case of bitcoin, the algorithm controls its supply. About 1800 new bitcoins are created every day until the cap of 21 million bitcoin is reached, which is also set by the algorithm of the cryptocurrency.
4. Bitcoin is both anonymous and non-confidential at the same time. Sender and receiver of bitcoin do not reveal their identity as there is no single third-party present to verify the transaction. Instead, the transaction is added to Bitcoin’s public ledger, the blockchain which is used to confirm transactions to the rest of the network.
5. No return policy – Once a transaction is done, the bitcoin cannot go back from receiver to sender because of no central authority that can facilitate the return process.
6. Satoshi – The smallest unit of a bitcoin is which is one hundred millionth of a bitcoin making it very flexible to pay the smallest amounts.

Ethereum

Ethereum is an open software platform that runs on the blockchain technology. This platform lets developers create different applications that are decentralized.

What is the similarities and differences between Bitcoin and Ethereum?

* Both Bitcoin and Ethereum run on blockchain technology
* Both bitcoin and Ether are tradable currencies
* Bitcoin blockchain technology is created for the sole purpose of tracking digital currency, Ethereum blockchain technology focuses on running the platform on which different applications can run

Ethereum has 2 different currencies. The first one is called Ether, which is paid during a transaction, like Bitcoin. The second crypto is called gas, which the executer of a smart contract needs to include for the miners to prioritize the transaction. More gas, more miners, faster transaction.

Smart Contract

Smart contract is like a regular contract, where someone asks for services in return for some tradable currency, but it is decentralized, i.e. there is no middle man. The middle man here is the underlying code that makes sure that transaction from A to B only happens when B fulfills all the requirements set by A.

The best way to explain Ethereum is said by the co-founder of Ethereum, Dr. Gavin Wood:

“Bitcoin is first and foremost a currency; this is one particular application of a blockchain. However, it is far from the only application. To take a past example of a similar situation, e-mail is one particular use of the internet, and for sure helped popularize it, but there are many others.”

Litecoin

As many people would call Bitcoin the digital gold, Litecoin is the digital silver.

* Bitcoin has a cap of 21 million whereas Litecoin has a cap of 84 million, 4 times that of bitcoin.
* It is like bitcoin except for the a few key features like they use different algorithms and has 4 times faster mean block time.

Real world uses of Blockchain

1. Modernizing voting and preventing voter fraud

* Blockchain technology makes any online transaction secure and private.
* Voting systems today still use offline ballots. Since blockchain technology offers a secure and private transaction, in this case a vote, offline ballots will become redundant.
* Offline ballots create a huge problem of voter fraud, as hacking into voting systems is very easy. Blockchain transactions are very easily verifiable and very hard to hack into making it a great choice for voting.

1. Economic freedom to poor countries

* Blockchain cryptocurrencies provide access to cost free money transactions for people of low income
* Since there is a lack of infrastructure in poor parts of the world, banks are hard to come by. Having cryptocurrency just requires having a phone and an internet connection

My code

After searching online on tutorials on how to create a blockchain, I came across one on GitHub. This code uses 3 classes: Transaction, Block and Blockchain.

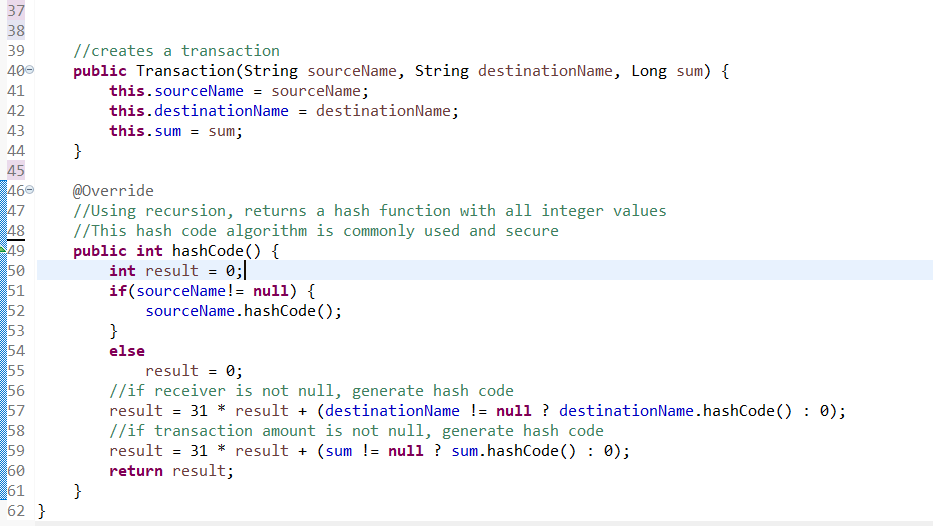
Transaction class creates a transaction between person A and person B of a certain value.

Block class uses the transaction class to obtain the transaction and creates a block

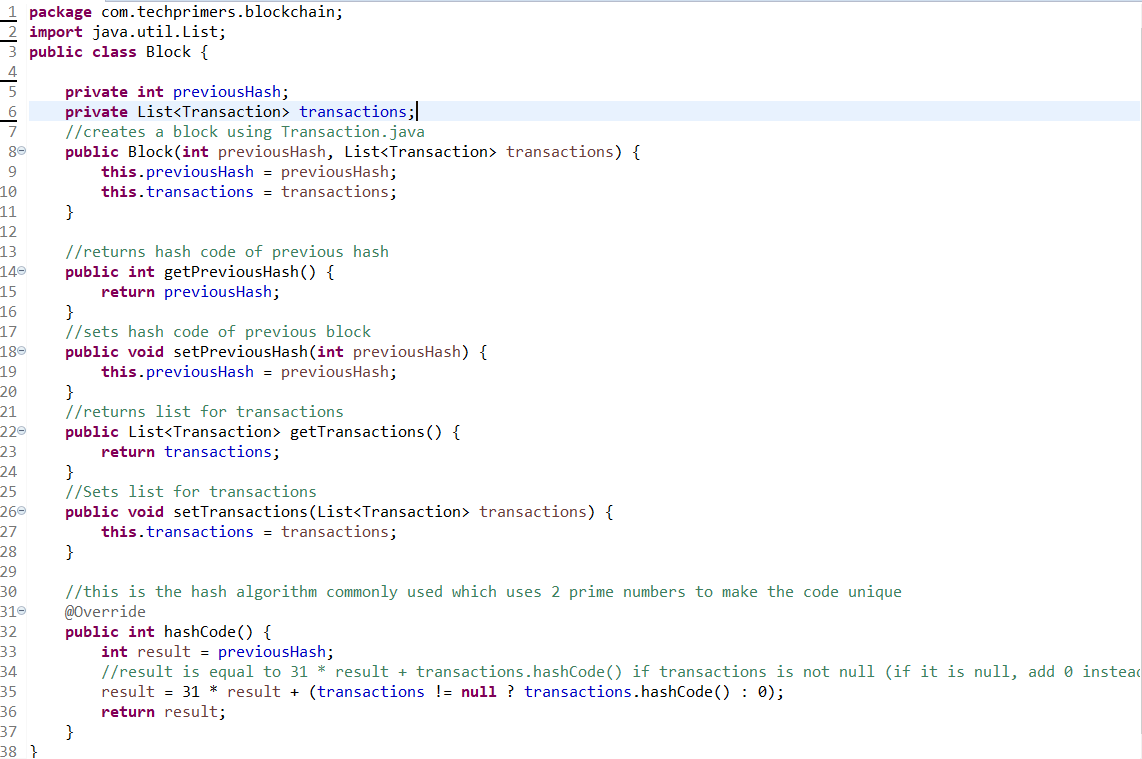
To create a blockchain, the credentials of receiver of the previous block has to match the credentials of the sender of the next block. I created a blockchain in the class blockchain.

Transaction.java:

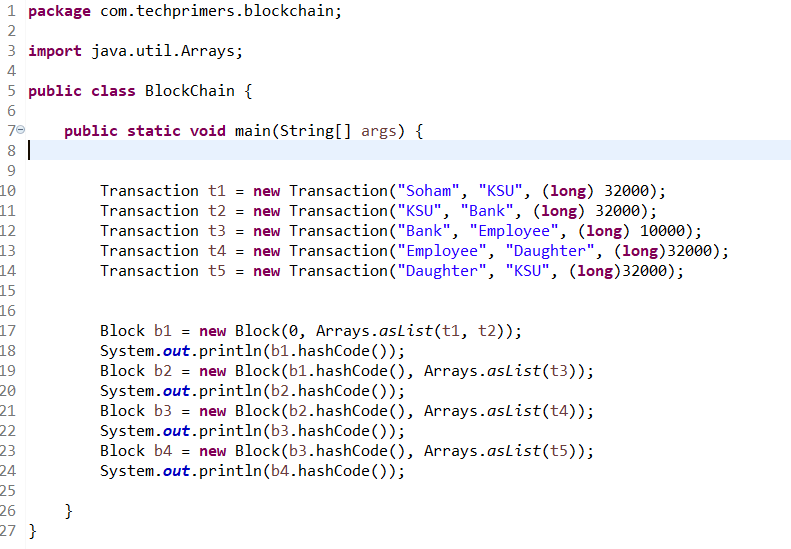




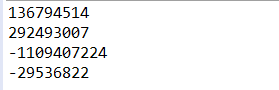
Block.java



Blockchain.java



Output:



Output prints out the hash code for each block. If any value is changed in the block, a new unique hash code is created.

Works Cited

1. Buterin, Vitalik. “The Meaning of Decentralization – Vitalik Buterin – Medium.” *Medium.com*, Medium, 6 Feb. 2017, medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
2. Acheson, Noelle. “What Is Bitcoin?” *CoinDesk*, CoinDesk, 20 Aug. 2013, www.coindesk.com/information/what-is-bitcoin.
3. Quora - A Place to Share Knowledge and Better Understand the World.” *How Many New Bitcoins Are Created on Average per Day?*, www.quora.com/How-many-new-bitcoins-are-created-on-average-per-day.
4. Quora - A Place to Share Knowledge and Better Understand the World.” *How many bitcoins has Satoshi Nakamoto spent?”,* https://www.quora.com/How-many-bitcoins-has-Satoshi-Nakamoto-spent
5. Acheson, Noelle. “What Is Bitcoin?” *CoinDesk*, CoinDesk, 20 Aug. 2013, www.coindesk.com/information/what-is-bitcoin.
6. TechPrimers. “TechPrimers/Java-Blockchain-Example.” *GitHub*, 22 Dec. 2017, github.com/TechPrimers/java-blockchain-example/tree/master/src/main/java/com/techprimers/blockchain