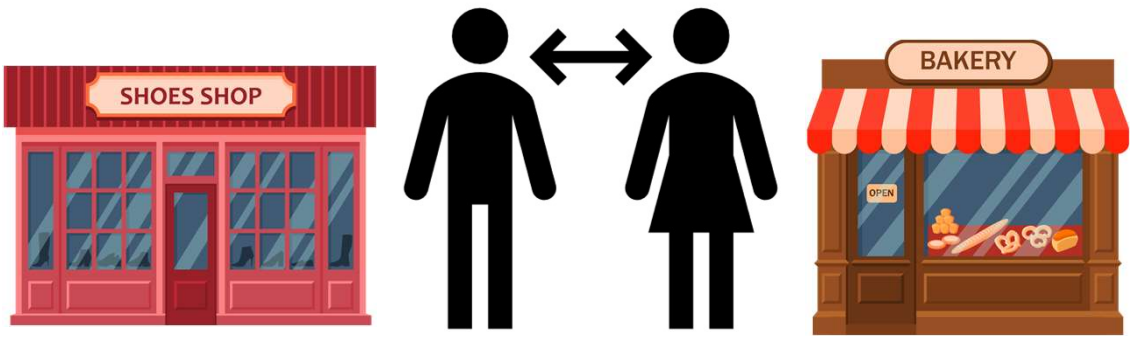
Today, let's talk about blockchain. At the mention of blockchain, the first thing that comes to your mind would probably be bitcoin. Bitcoin is a type of cryptocurrency that is an example of blockchain application. For this class, we will use bitcoin as the focus for you to better understand how a blockchain works. But before we get into that, let's discuss the history and evolution of money and payment.



While money is something that we use almost every day, the exact meaning of money can be quite abstract. Imagine you make shoes for a living and need to buy bread to feed your family. You would like to trade your shoes for bread with a baker, but he does not need that many pairs of shoes. Unless you find another baker who needs that many pairs of shoes, this trade cannot be carried out. This is so called barter economy.

In the early days, people use commodities as a mode of payment. One example are the Aztecs, People in central Mexico, they used cocoa beans for trading. However, using such commodities for trading has its disadvantages as their size and shelf-life matter.

Hence, we use currency (or money) as a solution.

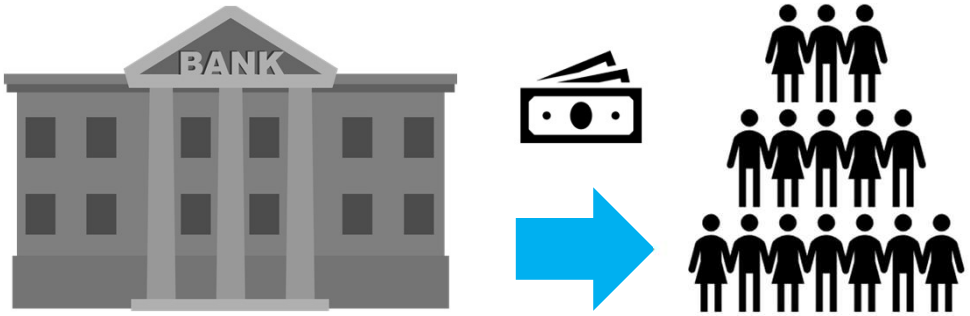
According to mainstream economics, money relieves the issues arising from commodity trading as it is a universal store of value that can be readily used by anyone.

This allows faster transactions as sellers have an easier time finding a buyer with whom they want to do business with. By transacting with currency, a seller can simply sell his or her goods and in turn pay their trading partners with the money earned.

There are other important benefits of currency too. For instance, it is much easier to bring currency around as compared to bringing bags of cocoa beans each time you need to buy something. Furthermore, coins and papers last longer than most commodities used for trading. For example, if a farmer relies on direct trade using his corns, he will only a few weeks to trade before his corns become rotten. Currency, on the other hand, can be accumulated and stored.

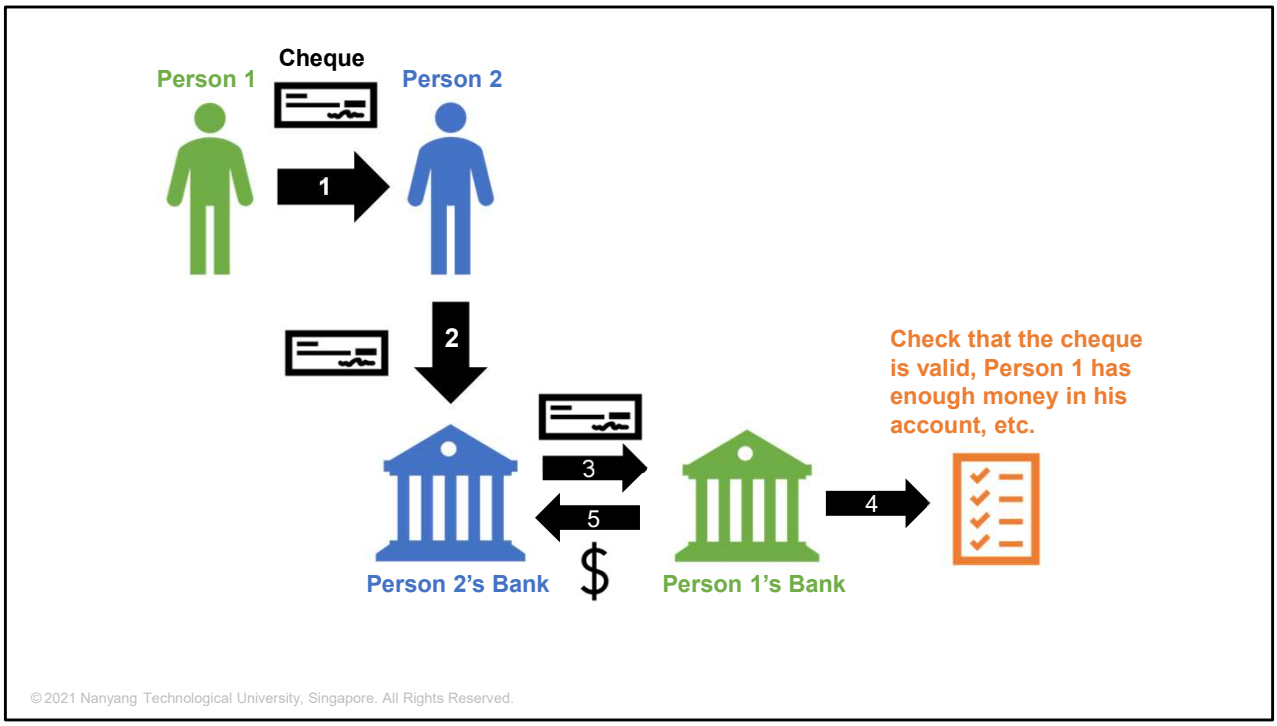
This is why minted currency was such an important innovation. As far back as 2500 B.C., Egyptians created metal rings to use as money. Then actual coins made from precious metals such as gold, silver, or copper appeared around 700 B.C..
The problem is the metallic coins were quite heavy to carry for daily transactions.

So, we have paper money. The first recorded use of paper money was purported to be in China during the 7th century A.D. It worked quite similar as modern-day banking. Individuals would deposit their coins with a trustworthy party and receive a note denoting how much coins they had deposited. The note could then be redeemed for currency at a later date.

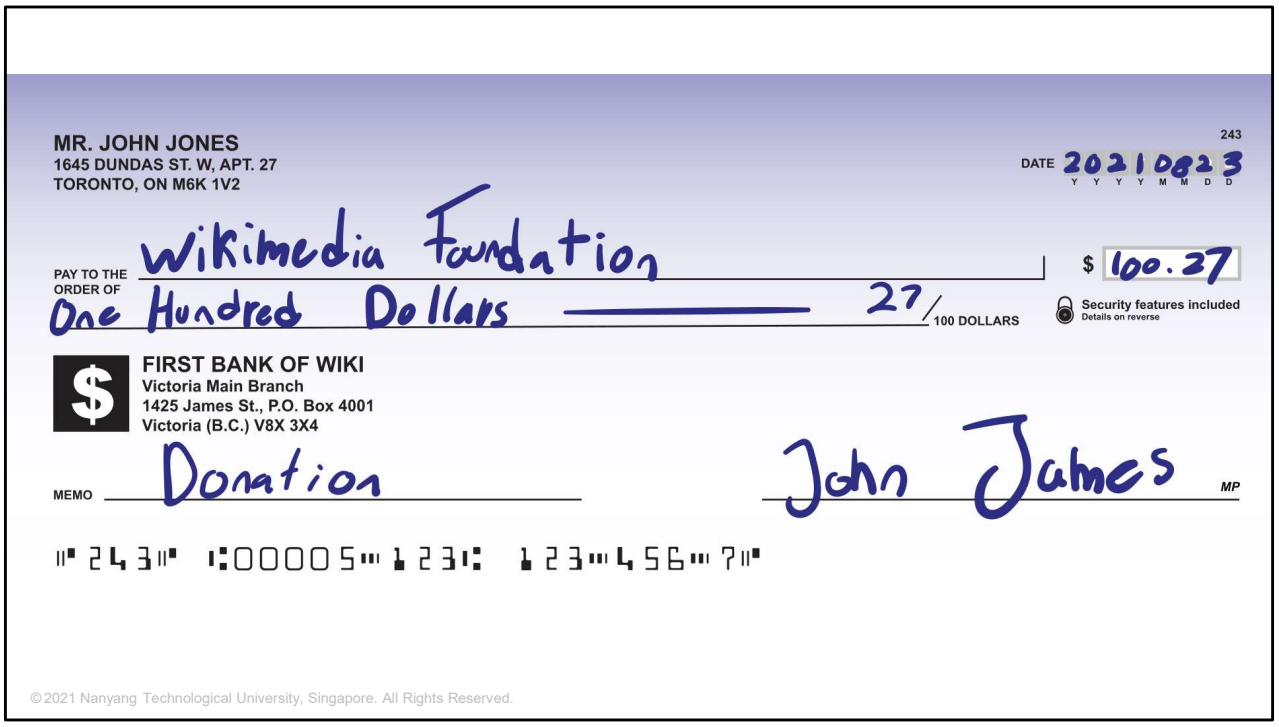


When we talk about paper money, we have to discuss a modern money related key concept—Central Bank. As we know, paper money is a country's official paper currency that is circulated and accepted for the transactions of goods and services. It is the country's central bank that authorises and regulates the printing of paper money, ensuring that the flow of funds aligns with the monetary policy.

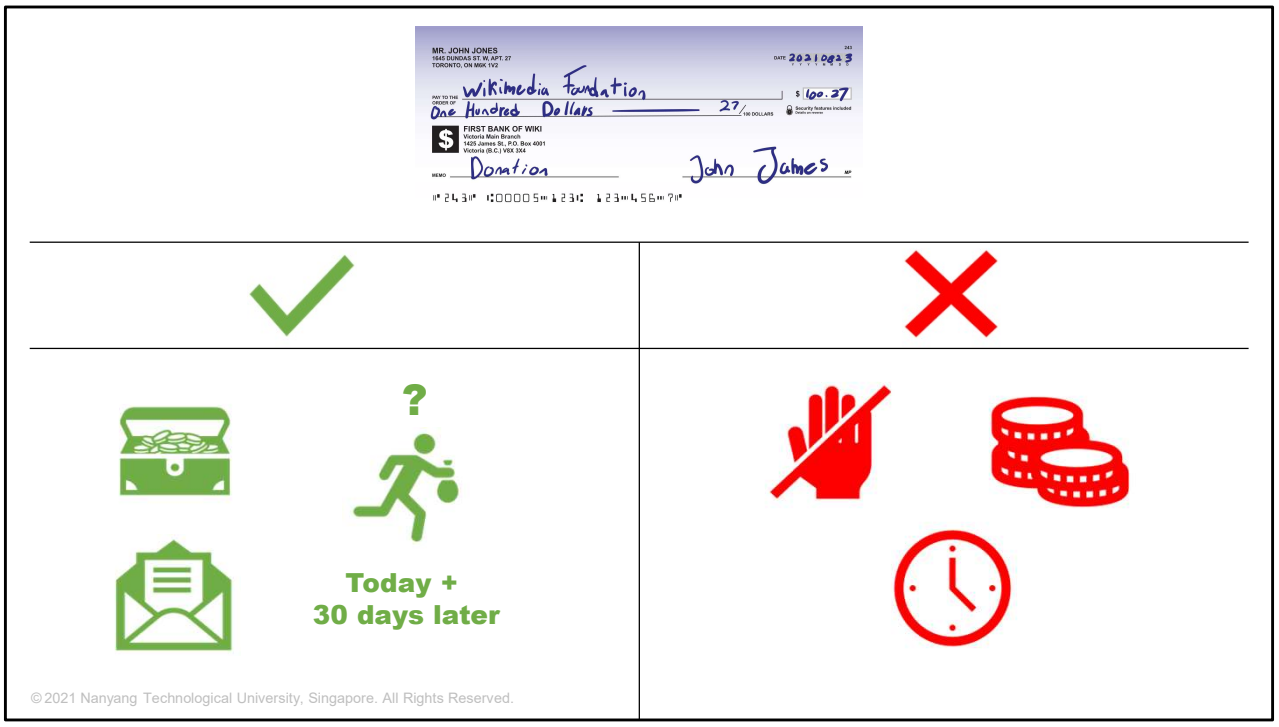
Paper money used to be backed by a certain amount of gold and later on government-issued currency is purely based on a country's government, so called fiat currency. The relationship between supply and demand of the fiat money, and the stability of the issuing government, defines the value of fiat money.



In 20th century, cheque becomes a very popular non-cash method for making payments. A cheque is a document that orders a bank to pay a specific amount of money from a person's account to the person in whose name the cheque has been issued. The person writing the cheque, known as the drawer, has a transaction banking account where the money is held. Say for example, person 1 issues a cheque to person2. When person2 drop cheque at the deposit box, person 2's bank will send the relevant information to person 1's bank. After person1's bank check that the cheque is valid and person 1 has enough money in his account, person1's bank will transfer the money to person2's bank account.



This is how a cheque looks like.

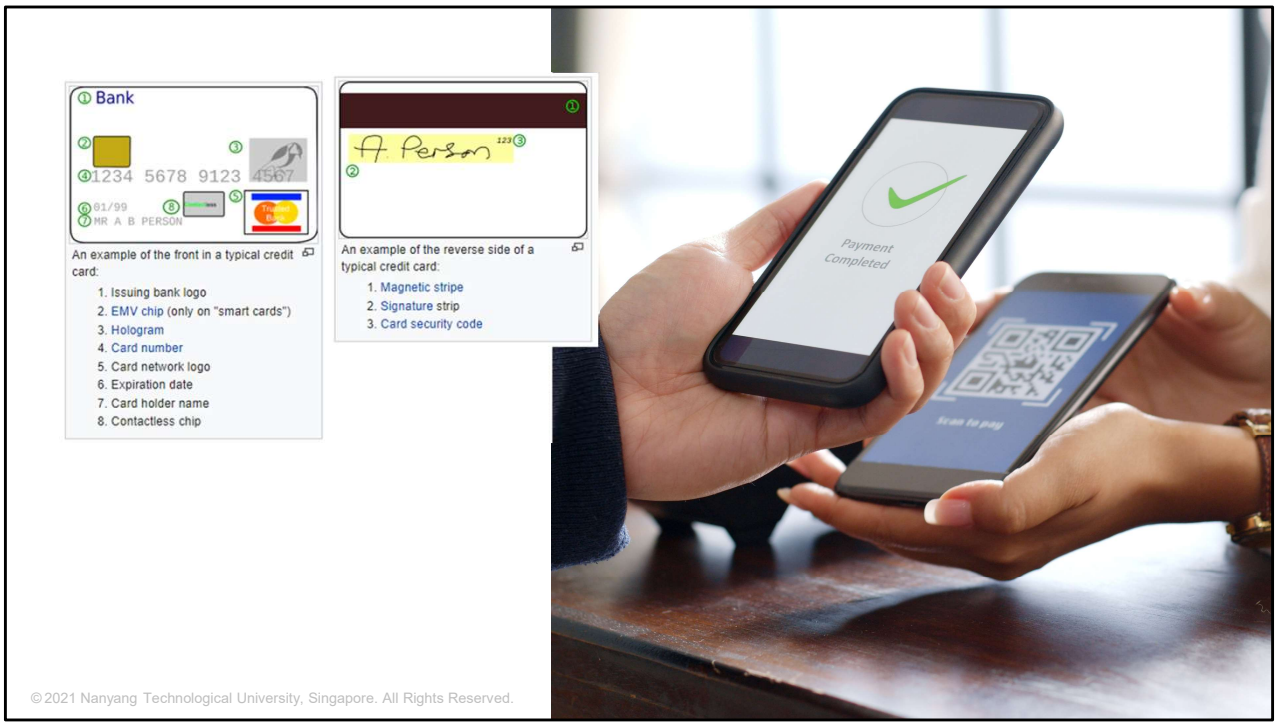


Advantages of cheque:

- It is more convenient than carrying a large amount of cash around.
- Cheques are safer than cash when carrying them around since a thief can't do much with your cheque book.
- They can be post-dated.
- They can be posted.

Disadvantages of cheque:

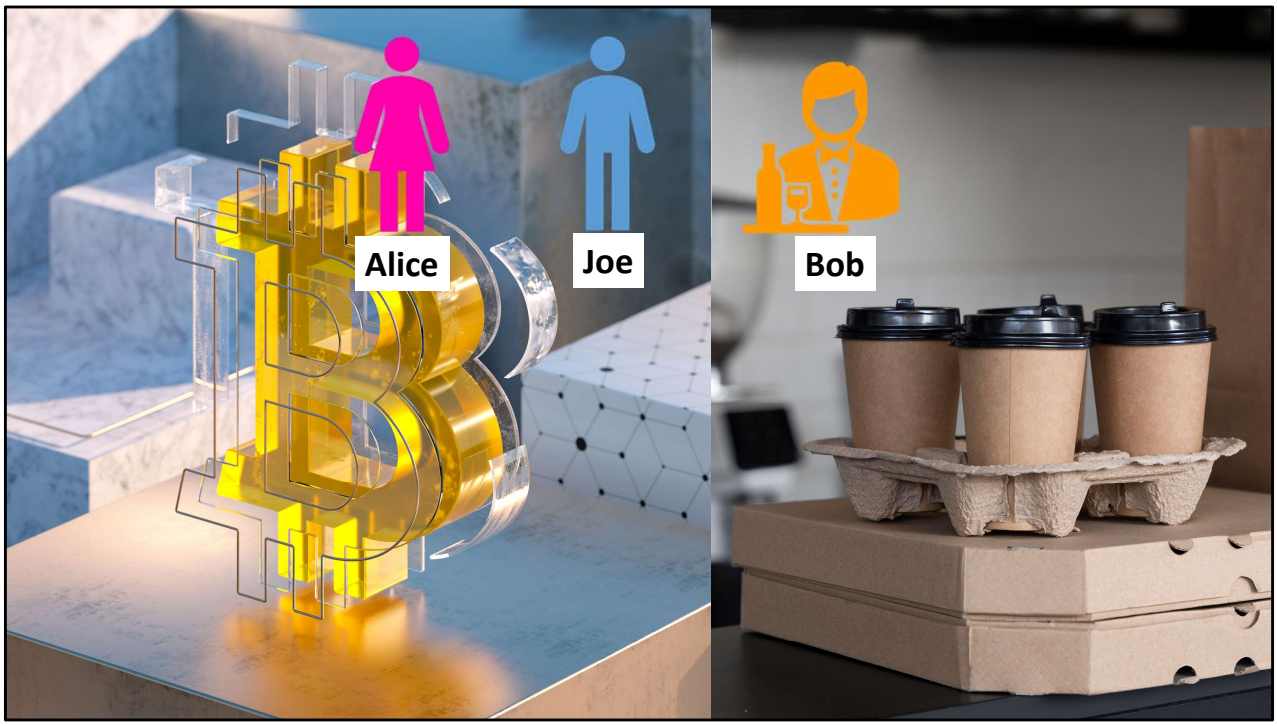
- Cheques are not legal tender; creditors can refuse to accept them.
- Cheques are valueless if drawer has not enough funds in their account.
- There is a lead time from posting to drawing a cheque.



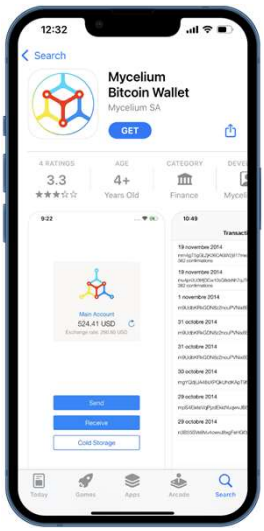
Another payment method is credit card. The card issuer creates a bank account for the cardholder, from which the cardholder can borrow money (with a limit) for payment to a merchant or as a cash advance.

More recently, contactless payment or mobile payment has become the main tool to transact in our everyday life. We generally do not carry cash, cheques or credit cards around nowadays. We simply use our mobile phone to make a payment.

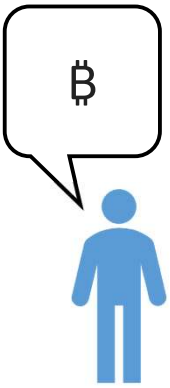
Now, let’s get into the details of bitcoins.



Let's consider a real-life use case. Alice lives in California's bay area. She has heard about bitcoin from her techie friends and wants to start using it. We will follow her story as she learns about bitcoin, acquires some, and then spends some of her bitcoin to buy a cup of coffee at Bob's cafe. This story will introduce us to the software, the exchanges, and basic transactions from the perspective of a retail consumer.



Alice



Joe

Alice, is not a technical user and only recently heard about bitcoin from her friend Joe. While at a party, Joe is enthusiastically explaining bitcoin to everyone around him and is offering a demonstration.

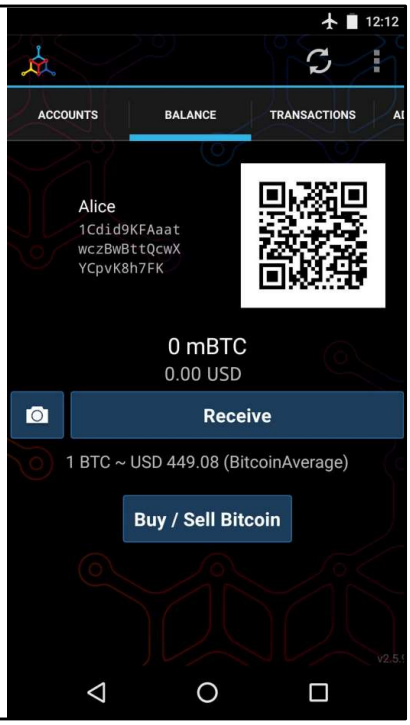
Alice finds it really interesting and asks how she can get started with bitcoin. Joe suggests that new users begin with a mobile wallet and recommends a few of his favourite wallets. Alice downloads “Mycelium” for Android on her phone.

The most important part of this screen is Alice's bitcoin address. On the screen it appears as a long string of letters and numbers:

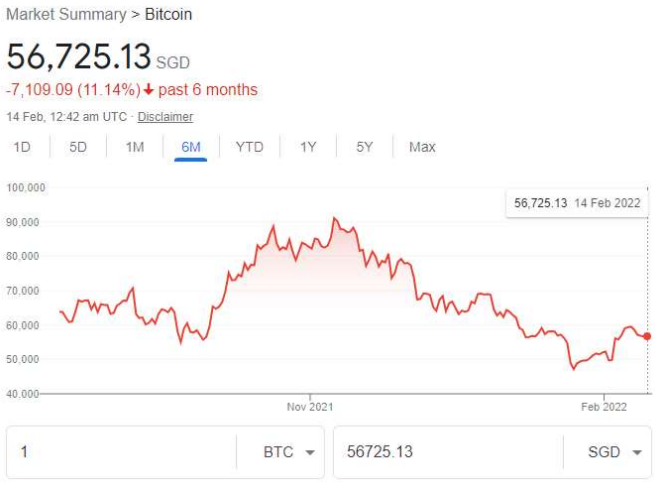
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

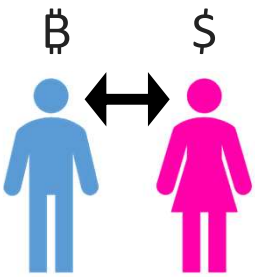
Next to the wallet's bitcoin address is a QR code, a form of barcode that contains the same information in a format that can be scanned by a smartphone camera.

Alice is now ready to use her bitcoin wallet.



After she installs the wallet, this is how her screen looks like.





Next, we will look at how she buys bitcoin from her friend Joe and how Joe sends the bitcoin to her wallet.

Before Alice can buy bitcoin from Joe, they have to agree on the exchange rate between bitcoin and US dollars. This brings up a common question for those new to bitcoin: “Who sets the bitcoin price?”

The short answer is that the price is set by markets. Bitcoin, like most other financial assets, has a floating exchange rate with fiat currency. That means that the value of bitcoin fluctuates according to supply and demand in the market.

Alice has decided to exchange USD10 for bitcoin, so as not to risk too much money on this new technology. She gives Joe USD10 in cash, opens her Mycelium wallet application, and selects Receive. This displays a QR code with Alice's first bitcoin address. Joe then selects Send on his smartphone wallet and is presented with a screen containing two input:

1. A destination bitcoin address
2. The amount to send, in bitcoin (BTC) or his local currency (USD).

Let's make the math simple and assume that the current bitcoin price is USD100. MBTC is milliBTC and 1 bitcoin = 1000 mbtc. We input 100 milliBTC or USD10.

100 mBTC or 0.1 BTC

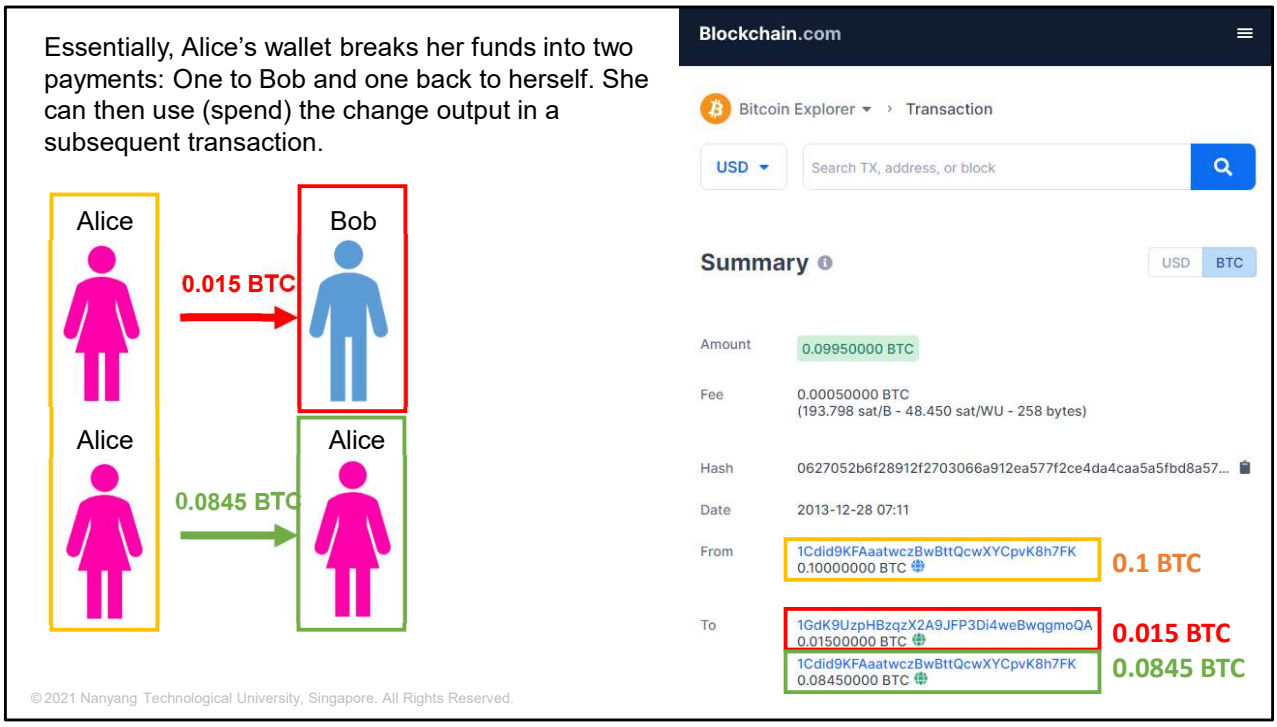
After buying bitcoins from Joe, Alice is now the proud owner of 100 mBTC or 0.1 BTC and she is ready to buy a cup of coffee using bitcoin from Bob's Café to further experience how it works.

Bob's Cafe recently started accepting bitcoin payments by adding a bitcoin option to its point-of-sale system. The prices at Bob's Cafe are listed in US dollars, but at the register, customers have the option of paying in either dollars or bitcoin.

Alice places her order for a cup of coffee and Bob enters it into the register, as he does for all transactions. The point-of-sale system automatically converts the total price from US dollars to bitcoin at the prevailing market rate and displays the price in both currencies:

Total:
$1.50 (USD)
0.015 BTC

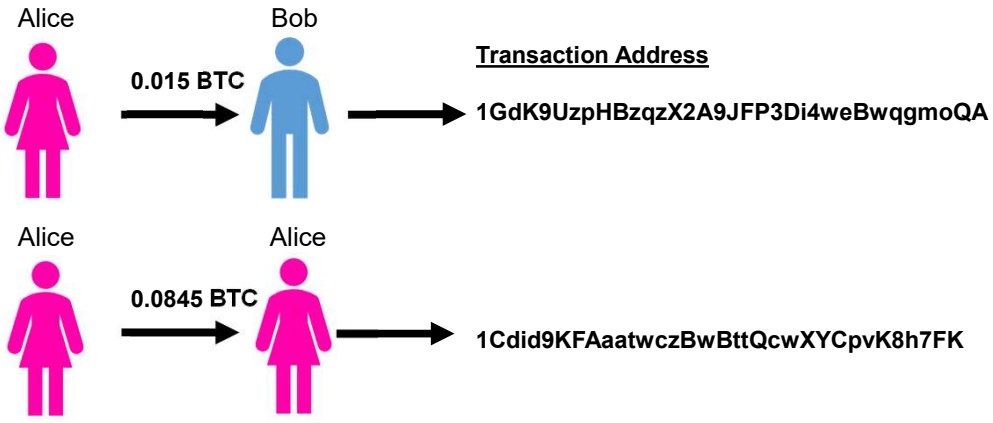
Bob says, "That's one-dollar-fifty, or 0.015 BTC."



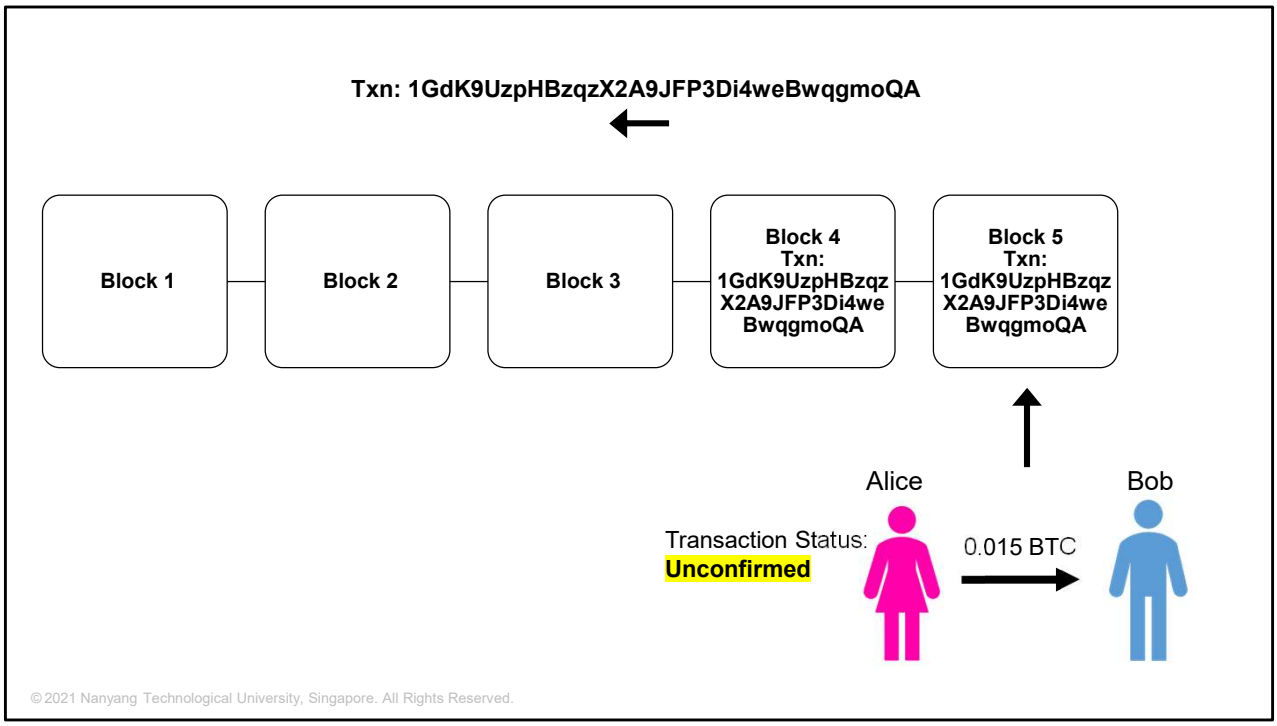
Essentially, after Alice makes the payment with bitcoin for her coffee, Alice's wallet breaks her bitcoin funds into two payments: One to Bob and one back to herself. She can then use (spend) the change output in a subsequent transaction. This is called the UXTO unspent transaction output. The transactions will be recorded on the bitcoin blockchain. The transaction ledger can be checked by anybody through various bitcoin explorer. The screenshot on the right is one example.

Alice's wallet application contains all the logic for selecting appropriate inputs and outputs to build a transaction to Alice's specification. At Bob's café, Alice only needs to specify destination and amount, and the rest happens in the wallet application without her seeing the details.

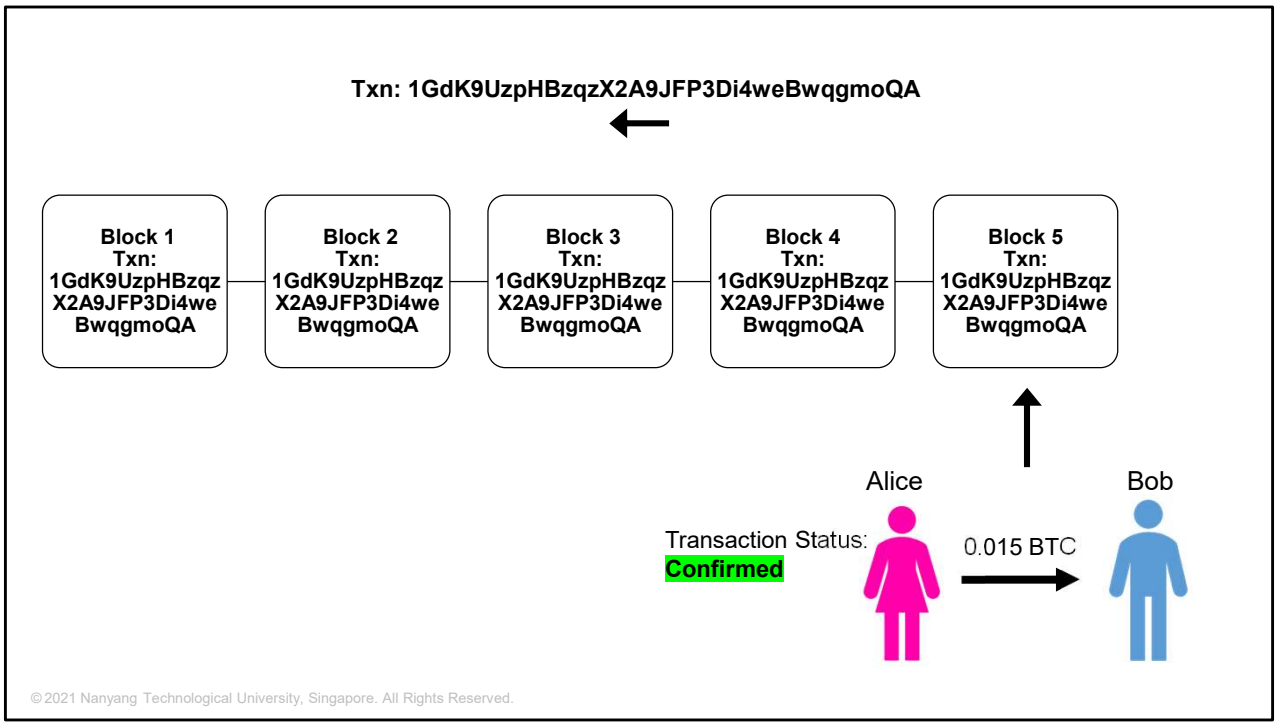
Alice's funds are in the form of a 0.10 BTC output, which is too much money for the 0.015 BTC cup of coffee. Alice will need 0.845 BTC in change. The difference of 0.0005 will be treated as transaction fee to reward the miner, who is the ledger keep of the transactions.



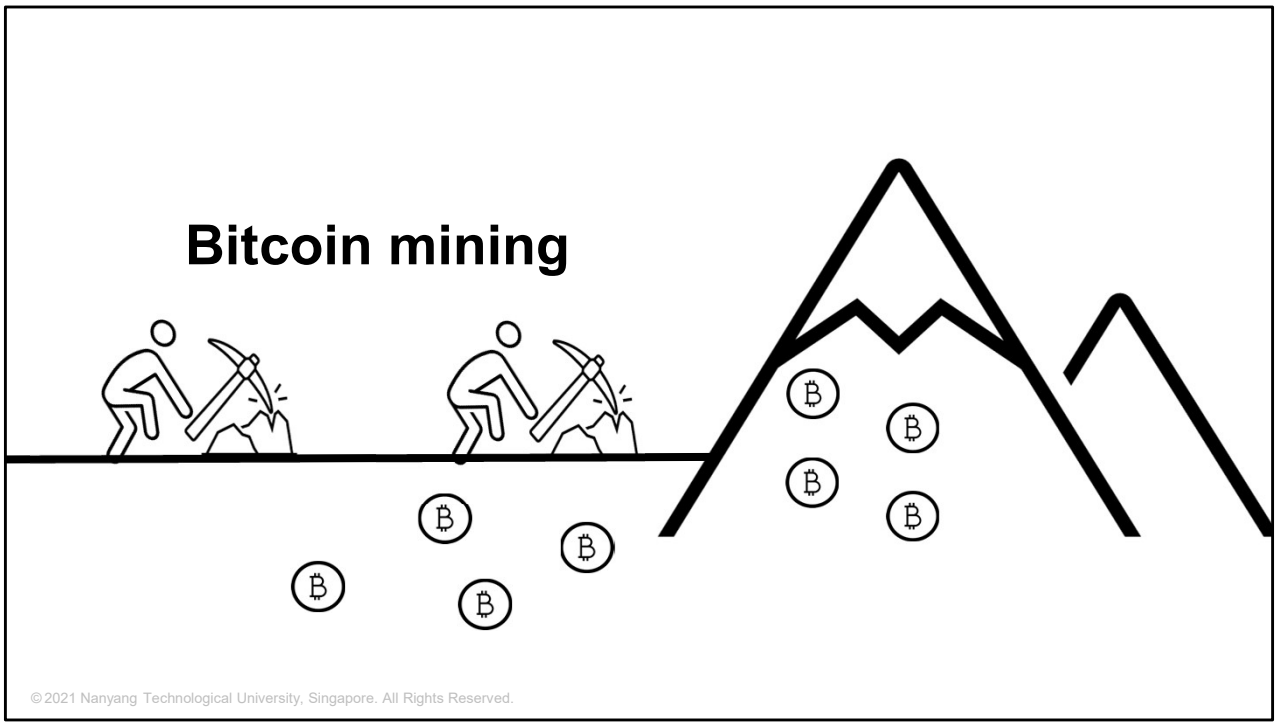
The transaction created by Alice's wallet application is 258 bytes long and contains everything necessary to confirm ownership of the funds and assign new owners. Now, the transaction must be transmitted to the bitcoin network where it will become part of the blockchain.



When the transaction is in the process of propagating to the blockchain network, the transaction status remains unconfirmed. Now, there is a chance that Alice's bitcoin might be fake and be rejected by the network. Hence, Bob should not give her the coffee until the transaction is confirmed. This is similar to how a cheque works.

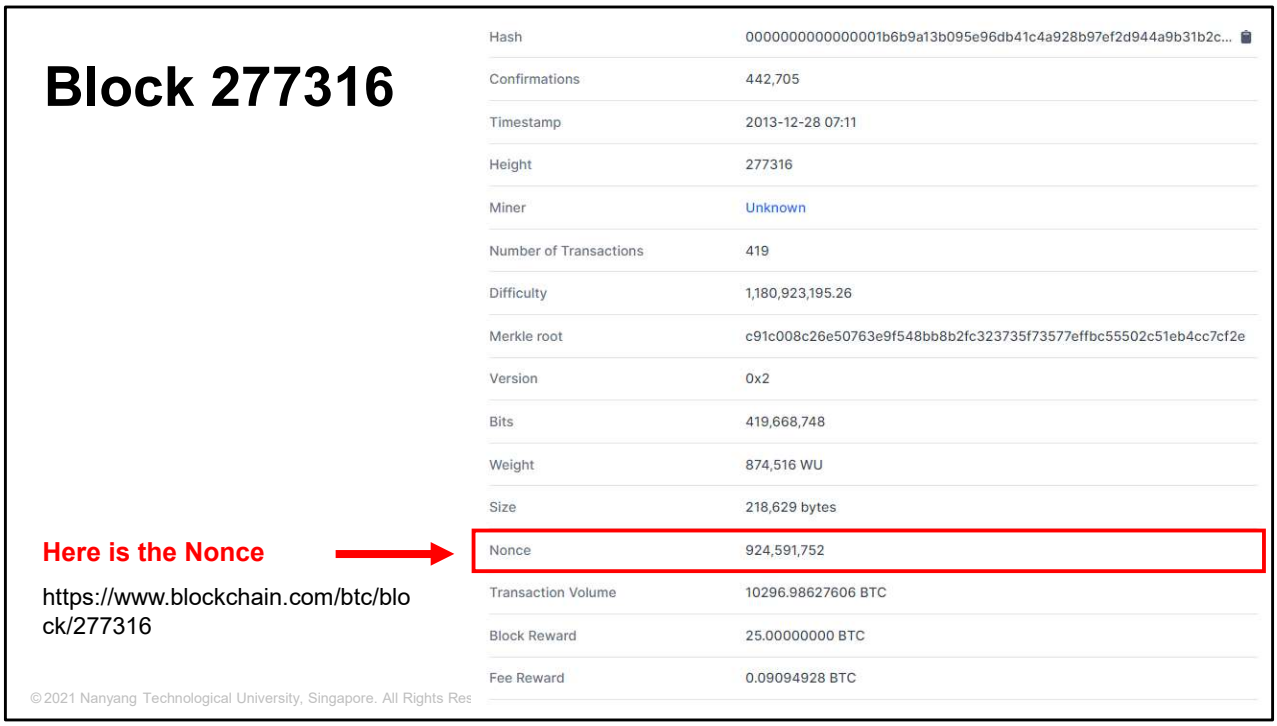


Once the transaction has been propagated to every block and accepted in the network, Alice's transaction is confirmed and Bob can give her the coffee. For small transactions such as this, usually Bob will simply give the coffee even before the transaction is confirmed. Besides, confirmation only takes a few seconds.



Besides buying bitcoin from someone, you can also mine it, like how miners did with gold and other precious metals. This is also known as the bitcoin mining process. This is similar to how Central Bank issues money in the modern world.

Block 277316



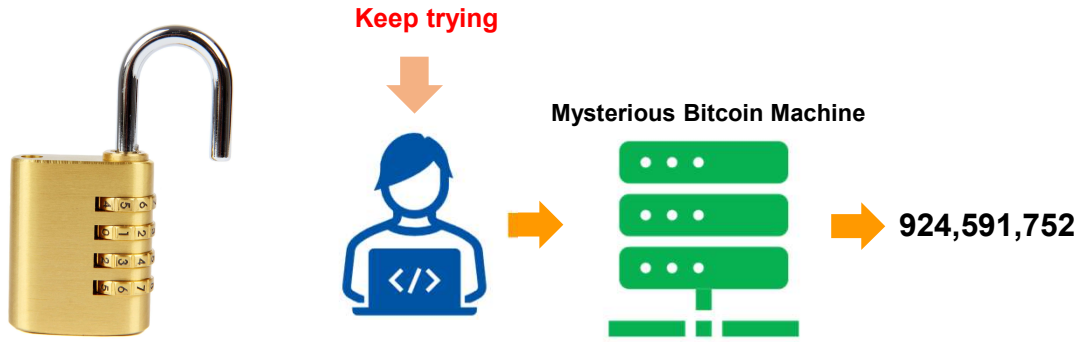
Here is the Nonce

https://www.blockchain.com/btc/block/277316

Let's use Block 277316 as an example, which also contains Alice's transaction, for bitcoin mining.

The key to bitcoin mining is the "nonce" value. Nonce is an abbreviation for "number only used once", which is a unique random generated number. The nonce is the number that blockchain miners are solving for, in order to receive bitcoin reward.

Bitcoin Hash Puzzle

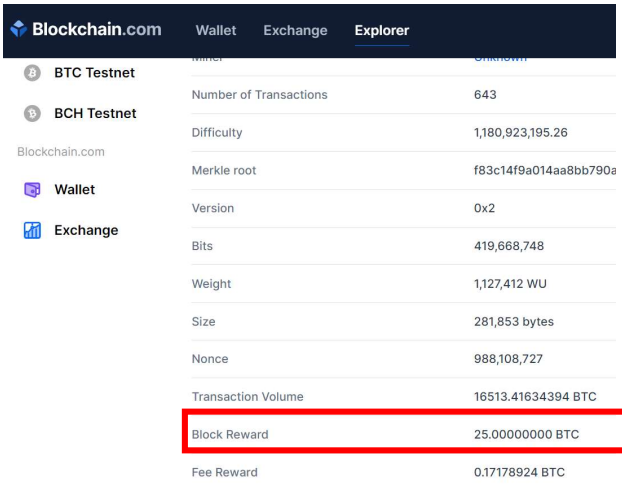


Imagine the mining process as a competition where all the miners compete to open the lock without knowing the password. How? It's not the same as solving a complicated math problem. What you can do is keep trying different combinations of these four digits. The search for a nonce is similar, it's done by sheer brute-force use of processing power. Just keep trying, to solve this so-called hash puzzle set by the network of bitcoin blockchain.

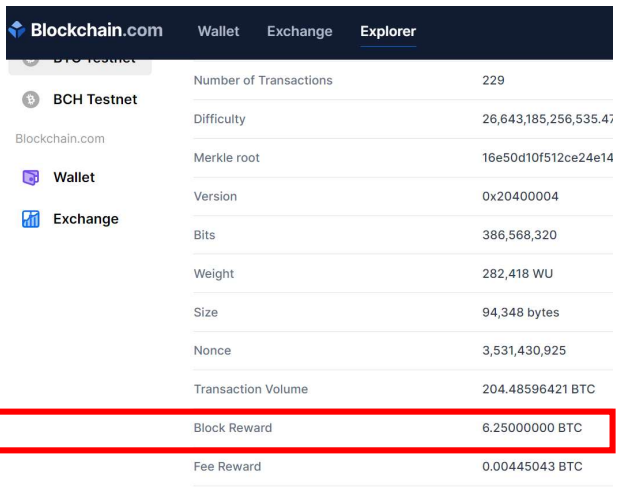
Given the above example, you must find the correct nonce **924,591,752** to get the reward for mining the block 277316.

You can consider this as you have a mysterious bitcoin mining machine, like the miner or ledger keeper who records all transactions between Alice and Bob, the machine will search for this nonce that can be combined with all transaction records and generate a hash value that meets the pre-determined requirement.

Block 277317

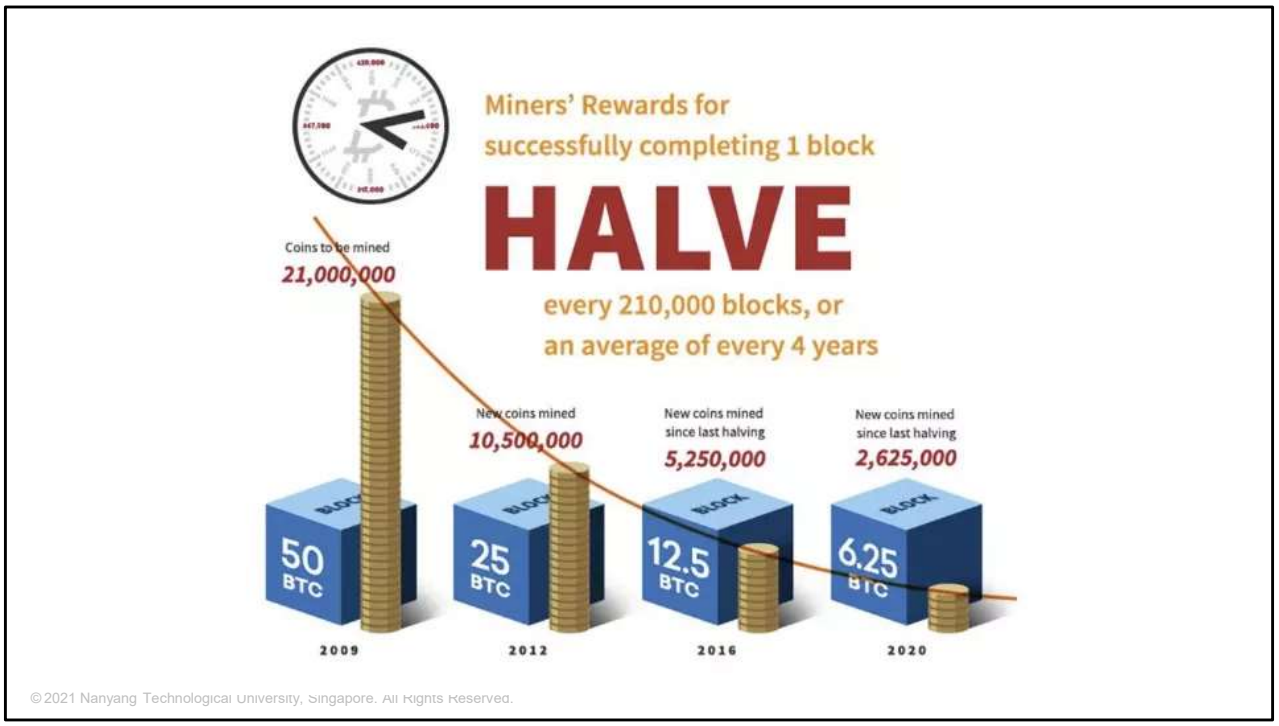


Block 720041



How much are the bitcoin rewards? Answer is, it depends.

You would be rewarded with 25 BTC (slightly over $1,200,000 SGD) if you successfully mined Block 277317, but you would only get 6.25 BTC (slightly over $300,000 SGD) if you successfully mined Block 720041 (the latest block in the chain as at 23 January 2022, 10:08pm Singapore time).



This is because miners' rewards for successfully completing 1 block halve every210,000 blocks or an average of every 4 years. The supply of bitcoins is capped at 21 million, which is forecasted to be all mined by the year 2140.

The mining sounds like a good deal? Think of the electricity and telecommunication bills you have to pay for while mining the bitcoins. Also, think of the competition around the world. After all the effort and expenses, there is a chance that you might get nothing.

Original:
Sounds like a good deal? Think of the electricity and telecommunication bills you have to pay for while mining the bitcoins. Also, think of the competition around the world. There is a block generated every 10 minutes, and the supply of bitcoins is capped at 21 million, which is forecasted to be all mined by the year 2140.

After all the effort and expenses, there is a chance that you might get nothing.

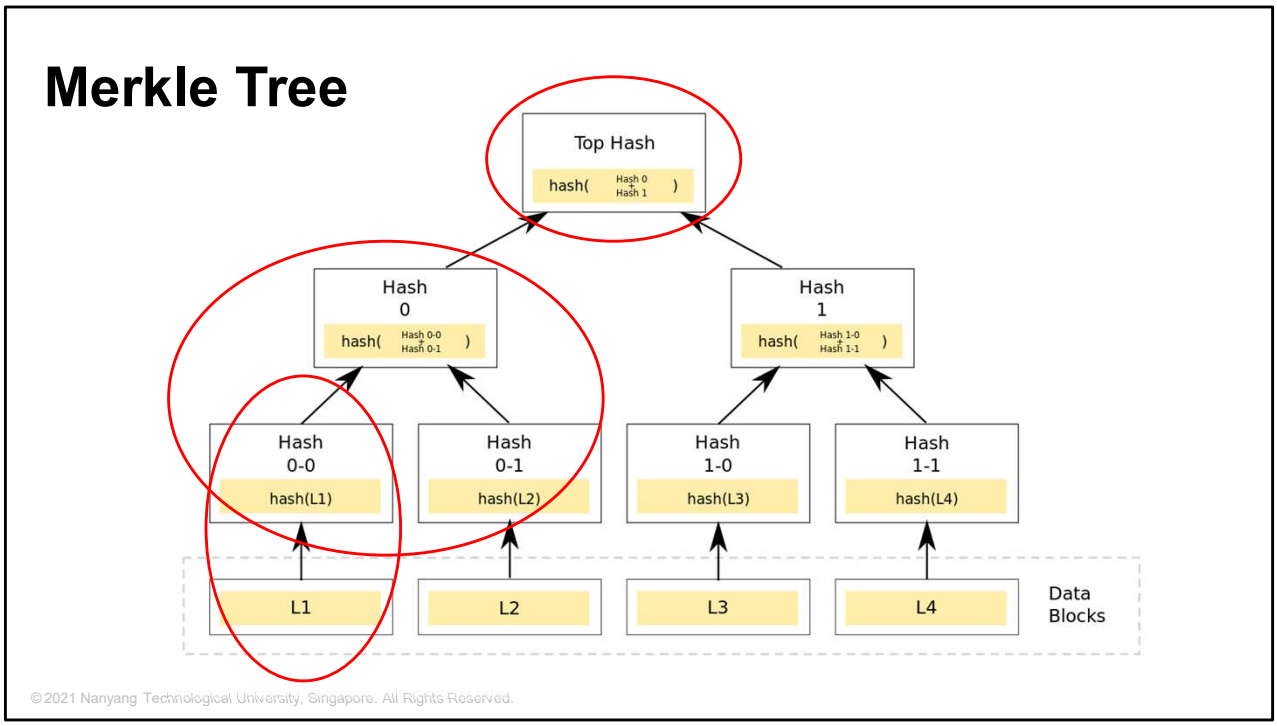
Hash Function

- The mathematical algorithm that transforms any kind of message into a bit array of a fixed size (the "hash value"), regardless of the size of the input message. It is a one-way function and infeasible to invert.
- Example:
  - SHA256(Blockchain) = 625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1
  - SHA256(blockchain) = ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

Now let's take a look at how blockchain structures and records data.

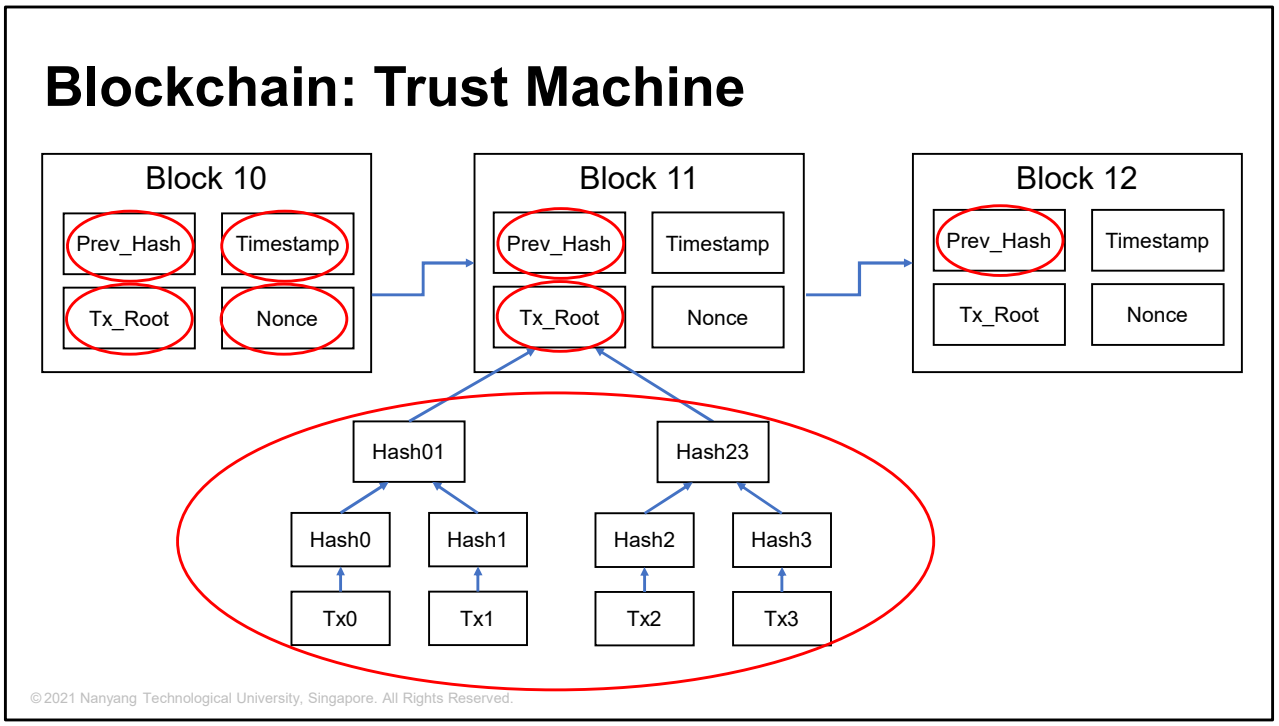
The first step is to hash the information. Hash is a mathematical algorithm that transforms any kind of message into a bit array of fixed size (that is, the "hash value"), regardless of the size of the input message. It is a one-way function and is infeasible to invert.

Take the hash function SHA256 for example. It generates a unique, fixed size 256-bit hash. A tiny change of the input information, say changing uppercase B to lowercase b in the word "Blockchain", leads to a completely different output.



After converting individual transaction message into hash values, a pair of hash values can be hashed again. We keep doing so until we have one single hash value on the top. By doing so, we bundle up transactions in a tree-like manner, deriving a single hash value at the top, which is known as the Merkle tree root. Any small change in original information will lead to a completely different Merkle tree root.

As we can see, the Merkle tree is a data structure used for efficiently summarising and verifying the integrity of large sets of data. It is constructed by recursively hashing pairs of nodes until there is only one hash, the root.



Now let's zoom in on the blockchain data structure.

A block first collects information together. These transactions are aggregated into the Merkle tree root. Each block stores the Merkle tree root for the transactions , as well as nonce, timestamp, and the hash value of the previous block, that is the hash value of the block information. Blocks are then linked using the hash value of the previous block.

In this way, any change in a single transaction will result in a change in the Merkle tree root. It will then change the hash value of that block and result in a change for all the following blocks. It is not possible to manipulate the earlier record without changing the following. This is how blockchain makes the data tamper proof.

Step 1: Hash the Five Highlighted Components

Block 277315

Hash	0000000000000002a7bb
Confirmations	442,733
Timestamp	2013-12-28 06:57
Height	277315
Miner	Unknown
Number of Transactions	40
Difficulty	1,180,923,195.26
Merkle root	5e049f4030e0ab2debb92

Block 277316

Hash	0000000000000001b6b9a13b095e96db41
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735
Version	0x2

Next, we'll look at the hash value of a block in BTC implementation, which is the identity of the block. Note that other implementations (such as ETC) might use other methods to achieve similar outcomes.

The block header is created with six fields:

1. Version number
2. Hash of the previous block
3. Timestamp
4. Difficulty
5. Merkle root computed in the previous step

Note:
A Merkle root is created by hashing together pairs of Transaction IDs, which gives you a short yet unique fingerprint for all the transactions in a block.

Height is simply the "serial number of the block" where first block is 1 and so on.

Difficulty is a measure of how hard it is to find a valid block to mine. For example, if a previous block is mined in less than 10 minutes, then the next block would be

targeted at more than 10 minutes to be mined by increasing the number of bits as a “password” and so on. BTC targets 1 block to be mined every 10 minutes.

Step 2: Hash the Current Block Header

Block 277315

Hash	0000000000000002a7bbc
Confirmations	442,733
Timestamp	2013-12-28 06:57
Height	277315
Miner	Unknown
Number of Transactions	40
Difficulty	1,180,923,195.26
Merkle root	5e049f4030e0ab2debb92

Block 277316

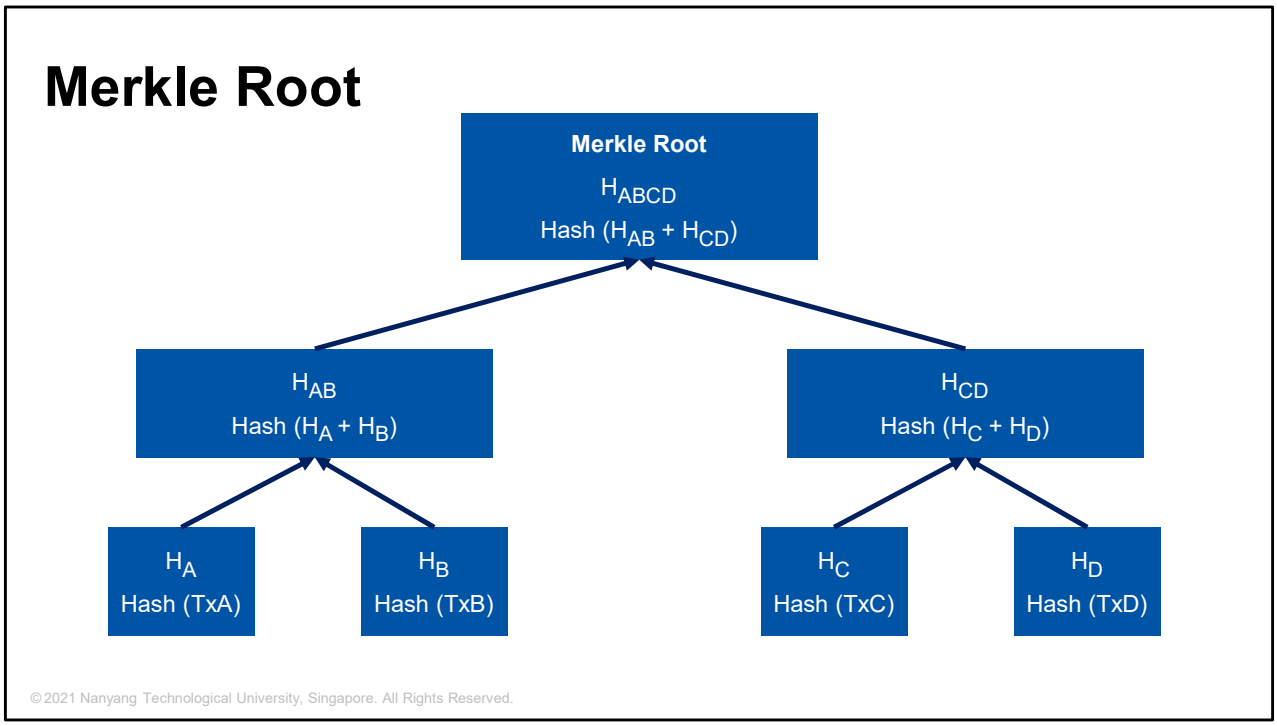
Hash	0000000000000001b6b9a13b095e96db41
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735
Version	0x2

The block header (which contains the Merkle root) is hashed, resulting in the block hash.

Step 3: Hash Values in Steps 1 and 2

Hash a and b =

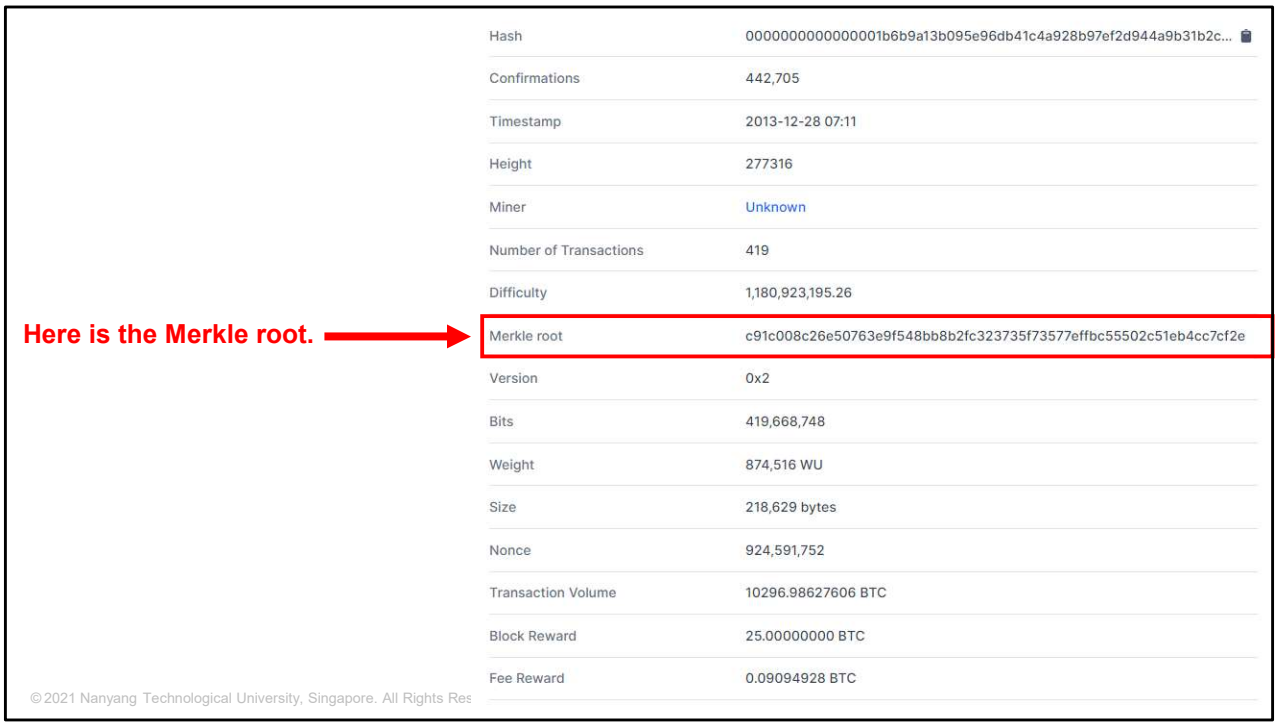
Hash	0000000000000001b6b9a13b095e96db4
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735
Version	0x2



Merkle Root

Each block in the bitcoin blockchain contains a summary of all the transactions in the block using a Merkle tree. A Merkle tree, also known as a binary hash tree, is a data structure used for efficiently summarising and verifying the integrity of large sets of data. Merkle trees are binary trees containing cryptographic hashes.

A Merkle tree is constructed by recursively hashing pairs of nodes until there is only one hash, called the root, or Merkle root.


Here is the Merkle root.
Hash
0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2c...
Confirmations
442,705
Timestamp
2013-12-28 07:11
Height
277316
Miner
Unknown
Number of Transactions
419
Difficulty
1,180,923,195.26
Merkle root
c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e
Version
0x2
Bits
419,668,748
Weight
874,516 WU
Size
218,629 bytes
Nonce
924,591,752
Transaction Volume
10296.98627606 BTC
Block Reward
25.00000000 BTC
Fee Reward
0.09094928 BTC
©2021 Nanyang Technological University, Singapore. All Rights Res

What Makes the Bitcoin Blockchain Safe?

After the discussion on the real-life use case, let's discuss several questions.
First, what makes the bitcoin blockchain safe?
Well, the cryptographic system makes transactions irreversible, which means once a block is created on the chain, it cannot be modified. You can, however, can add information to it. This restricts people from reversing any transaction that has already taken place.

Second, the bitcoin blockchain is public which may make it seem unsafe—but in the case of bitcoin, it helps to make it safe. Despite the anonymity of the user, all transactions on the network are accessible to the public, making it difficult to hack or cheat the system.

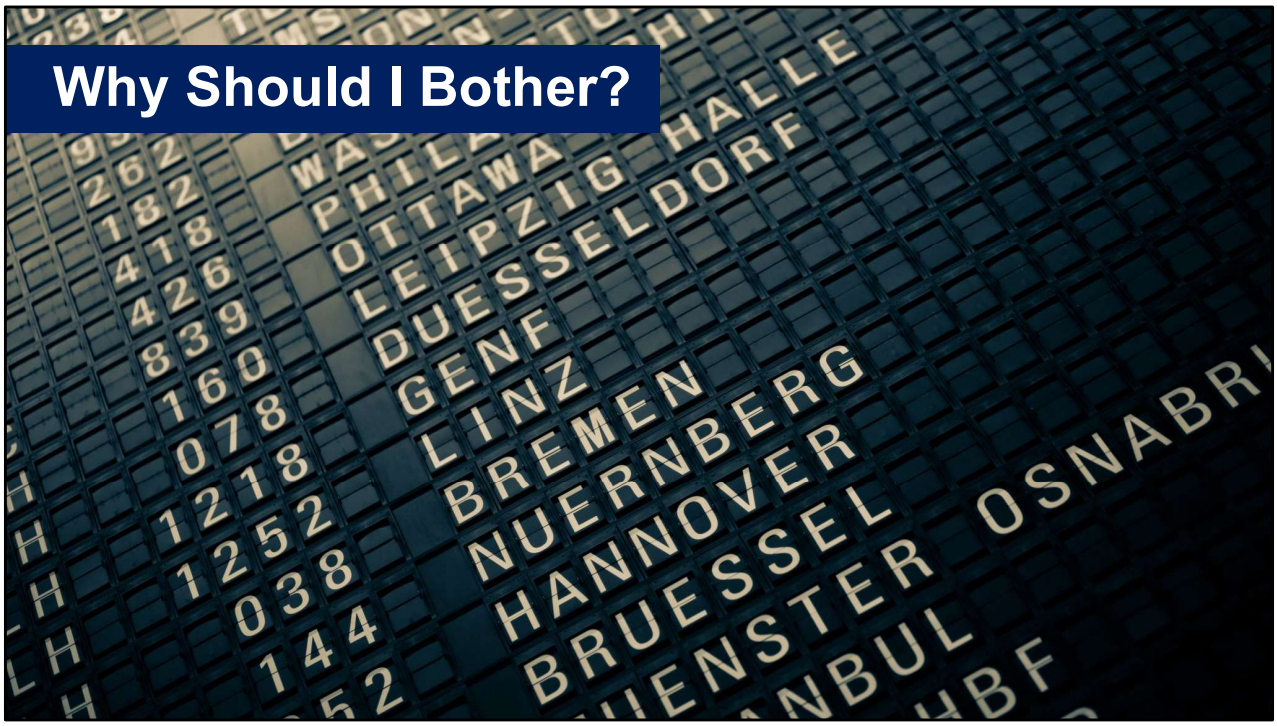
Finally, the decentralization contribute to the security as well. The bitcoin network is distributed and has thousands of nodes all over the world that keep track of all transactions happening on the system. This ensures that in case something goes wrong on one server, there are others to back up. This makes it meaningless to hack any one server.

So, what's the big deal about bitcoin? No, I don't mean the price. I mean how does that help the society?

If you want to trade bitcoin, the lowest unit you can trade is called Satoshi, which is the name of its founder, Satoshi Nakamoto. 1 unit of bitcoin is equivalent to 100 million Satoshi. Assume a bitcoin is worth 42,500 SGD now, a unit of Satoshi will be worth 0.000425SGD. 1SGD will give you about 2353 units of Satoshi.

If you go and buy a coffee that costs 1SGD today, you can use cash, credit card or one of the most popular instant payment systems, PayNow. PayNow is easy to use, and you just need to have your phone and not have to worry about carrying your wallet around. Imagine paying for the cup of coffee with 2353 units of Satoshi using a PayNow equivalent system. As of the current moment, we don't have such a system. For convenience sake, let's imagine a term and call it SatoshiNow. So, you go and buy a cup of coffee using SatoshiNow. You might think, erm, why do I bother since I already have PayNow?

Why Should I Bother?



You are correct. You don't have to bother. But if you are travelling overseas for a holiday, for example, visiting Seoul and checking out its iconic observation tower, or Switzerland for its famous and beautiful Chapel Bridge, and you wanted to buy a cup of coffee. What do you do? You'd either have gone to a money changer to get the local currency with the risk of under or overspending before the trip; or you can solve that issue by paying with a credit card which usually has highly unfavourable exchange rate. Either way puts you at a losing end.

Now, imagine the whole world is accepting bitcoin and its equivalent subunits Satoshi and you have SatoshiNow app on your phone. You want to go for holiday tomorrow? You'll just need to book a ticket and pack your luggage.

Is it just for the finance industry? There are definitely more possibilities. Imagine one day, someone creates a reliable Covid-19 test app that can securely identify you as the one being tested, and at the same time, link the result with it. After which, this information is propagated throughout the world using blockchain technology. You won't have to go to the doctor for a Covid positive or negative certification when you travel.

Once the platform is available, you can simply walk into a mall and travel on a flight with the secure app. And if, what if, the implementation of this technology is you? Stay tuned for the more discussion on blockchain in other courses. We are expecting your big invention.

Here brings to the end of my presentation for this module. Hope you enjoyed and thank you.