Investment Management
Prof. Abhijeet Chandra
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

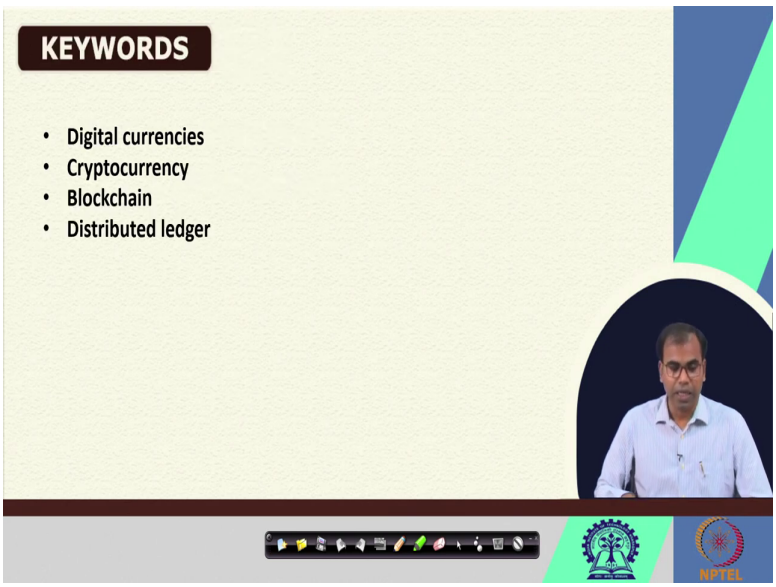
Lecture - 34
Cryptocurrencies

Hello there. While discussing about alternative investments and different asset classes, there is one particular asset class that we cannot ignore and those are digital currencies or in general digital assets. In this session, we are going to talk about one particular type of digital currency that is Cryptocurrencies.

(Refer Slide Time: 00:46)

Basically, we are going to talk about cryptocurrencies as digital assets for the purpose of inclusion in a portfolio and along with that we will also discuss about some salient features of cryptocurrencies that make them attractive for any investor.

(Refer Slide Time: 01:05)



(Refer Slide Time: 01:06)

Essentially, when we talk about digital currencies, the one thing that comes in our mind is an alternative to money. If you go back in the history to understand what money means for humankind, we know that money is defined as a commodity typically accepted by general consent as a medium of exchange, particularly those transactions or those exchanges where economic value can be specified.

It also implies that money is something in which prices and values of goods, commodities and services can be expressed. Money can also serve as a currency. It circulates anonymously from one person to another person from one place to another place and thus facilitating trade, exchange of goods and services. It is also considered as the principal measure of wealth.

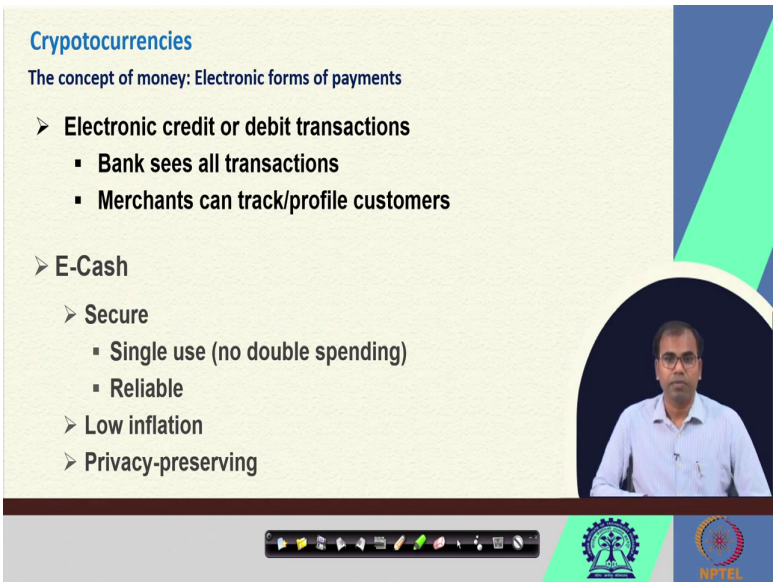
So, money has its own definition and when it comes to money, we know that in the history of humankind, money has been denoted as different type of commodities or metals or for that

matter any other goods. But what is important is the soundness of money. Aristotle defines sound money as durable, transferable and divisible. He also insisted that money must provide some intrinsic value particularly that is independent and contained in the money itself.

It is also should also be scarce, recognizable and fungible. When we talk about these characteristics of a sound money, we know that over a period of time, the money that we see these days, particularly the physical form of money, mostly fit into these characteristics. We know that the money that we have today, particularly the physical form of money are durable, mostly secure, they are mostly non-traceable and typically they do not lose value much, which means they have low inflation.

They typically cannot be used in online transaction directly and also, they might have certain transaction cost. We know that the money that we are having today are transferable, they can be divided into smaller sums of money and they have intrinsic value of itself, they are recognizable, we can trace them and they are fungible.

(Refer Slide Time: 04:03)



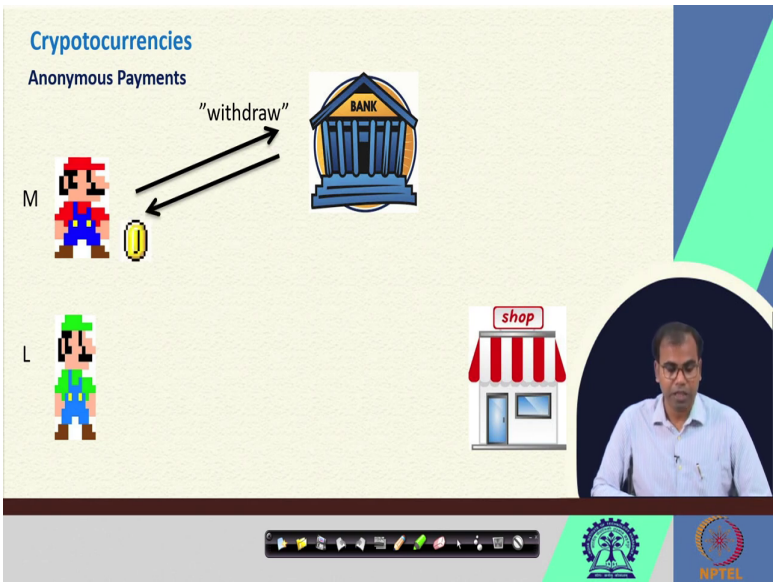
Now, with this understanding of money from the historical perspective, we know that over a period of time, people and particularly those who are involved in transaction of trades of goods and services feel that the money of physical form has become less relevant or sometimes creates some problem.

For example, in olden days, when people use to carry coins as a for trade and exchange of goods and services, it used to be very difficult and insecure for them to carry heavy gold or silver coins for the purpose of trade of goods and services. So, imagine a traveler or a trader traveling to a distance location with lots of gold and coins and silver coins for the purpose of executing certain trades. It is not only difficult to carry, but also it was insecure because of certain reasons.

Now, over a period of time particularly in recent years, we see that electronic form of payment or electronic form of money has been more popular. We see that there are electronic transactions, both debit and credit type, but it also has certain limitations. For example, whenever we make electronic transactions or electronic payment, we know that banks are the entities that see all the transaction that can trace all the transaction.

Not only banks, but also the involved merchants, they can also track profile, the customers and they can accordingly use that data that information for the purpose of pushing their goods or services or making certain advertisements. We have an alternative concept of money that is e-cash or electronic cash, mostly it is secure, it has no double spending opportunity, which means it is of single use, it is mostly reliable, it has low inflation and it is privacy preserving.

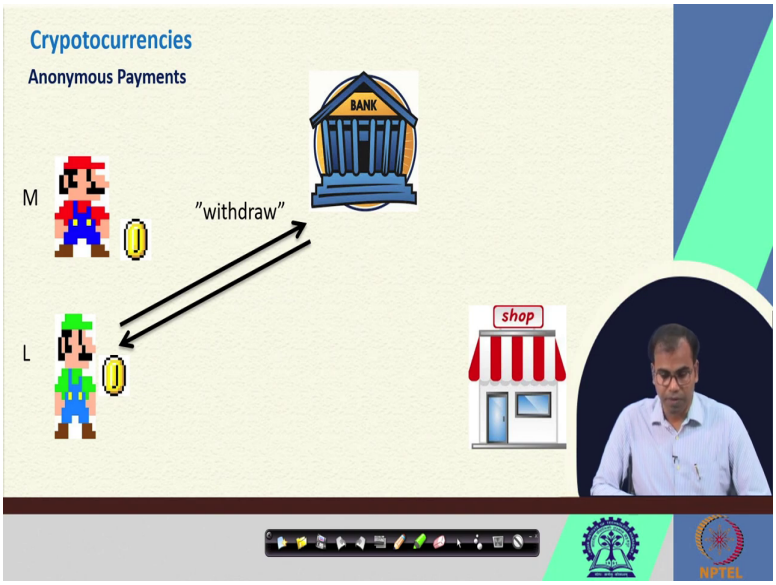
(Refer Slide Time: 06:22)



With these features, in recent years, people have realized that anonymity or secrecy of the origin of the money is more important for keeping the profile of the users, a secret or anonymous has become more important and. This can be understood from this particular graph, where we see that there is a bank and bank is basically the place or entity that offers money as lender or that keeps money as the depositor.

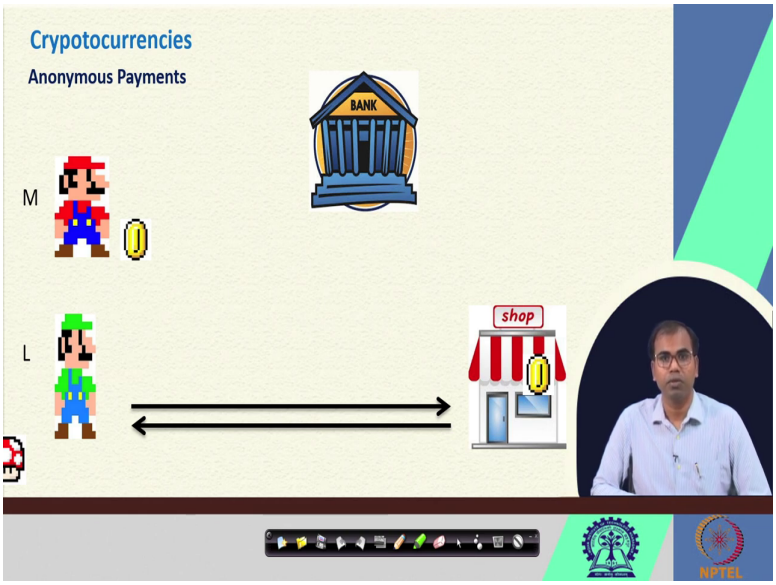
When there are two entities, suppose two individuals, M and L and they have certain deposits with bank. Suppose, person M wants to withdraw certain amount of money, he goes to the bank, asks for withdrawal and receives some money from the bank.

(Refer Slide Time: 07:37)



Similarly, if person L also wants to withdraw some money, he goes to the bank withdraw some money and receives some of money in return. Now, one of these two people goes to the shop to buy certain goods or services.

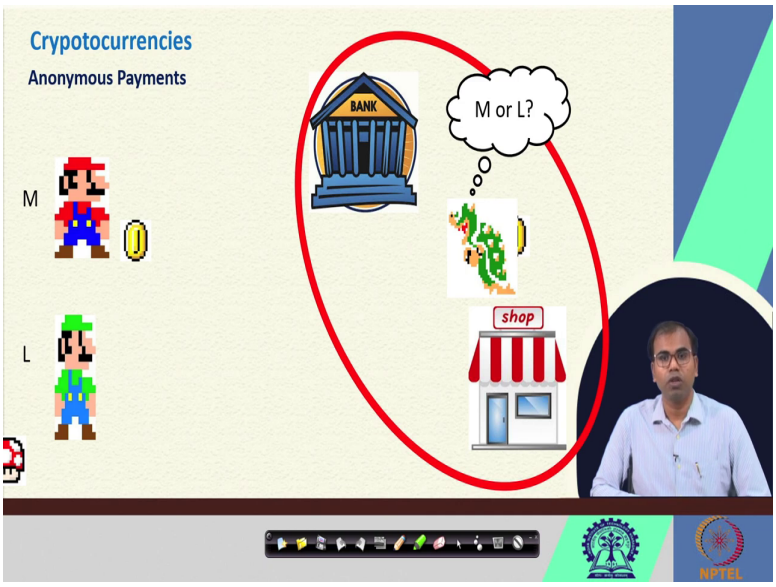
(Refer Slide Time: 07:43)



So, imagine that person L goes to the shop pays money and buys some goods or services.
(Refer Slide Time: 07:57)

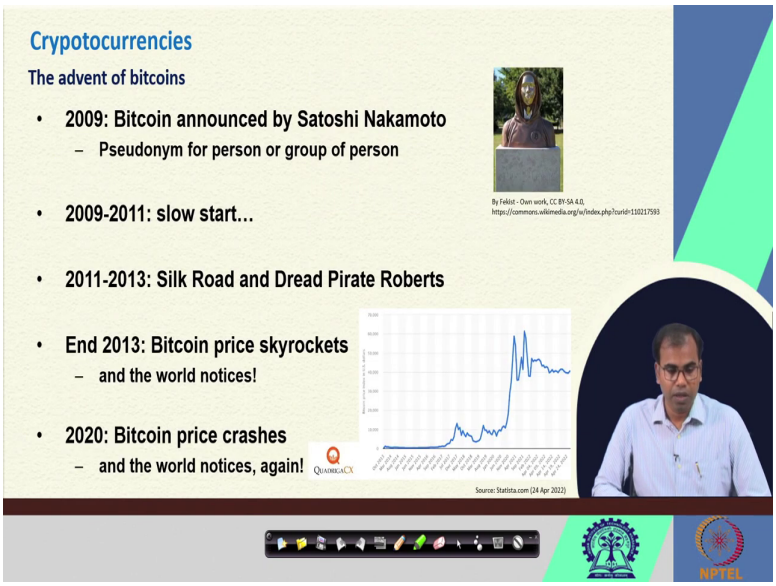
When shopkeeper wants to deposit that money received from the customer to the bank, we know that this transaction can be traced, but this cannot remain anonymous.

(Refer Slide Time: 08:03)



So, the point of secrecy here is bank should not be able to know whether the money that shopkeeper is depositing is coming from person L or person M. If we are able to keep that kind of confidentiality or anonymity in the transaction, it serves as a good or a sound money in true sense.

(Refer Slide Time: 08:28)



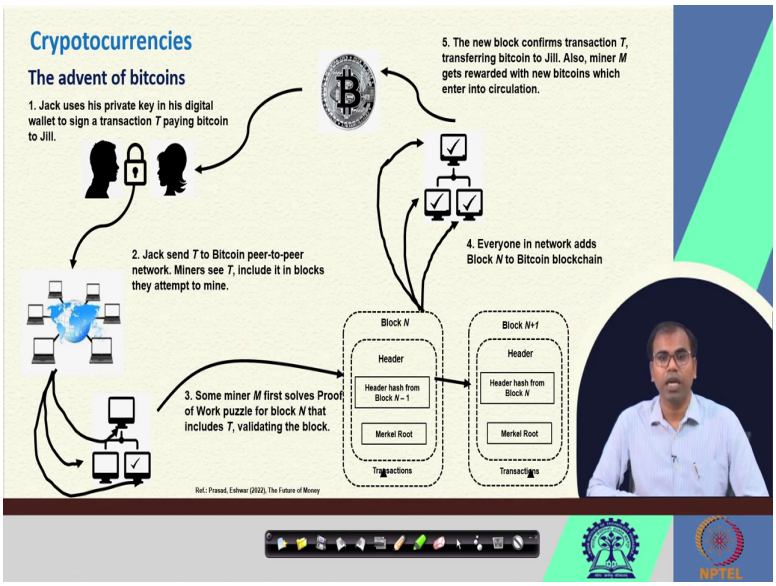
And that is one of the reasons why Bitcoin was conceived. If we know the history of Bitcoins, it was initially conceptualized by a person named Satoshi Nakamoto, who was probably a person or a pseudonym for a group of person who announced Bitcoin through a white paper in 2009.

And in the beginning, it was a slow start when Bitcoin did not catch up much. In 2000, from 2011 to 2013, Silk Road and Red Pirate Roberts gave it more popularity and by the end of 2013, we realized that Bitcoin price skyrocketed. And then, it was noticed by everyone related to financial sector. If we look at the trend by the end of 2020, we see a huge crash in the Bitcoin prices and again people started talking about it.

In the meantime, we have seen Quadriga CX sort of scams as well, but to say so, we have seen Bitcoin going up and down over the period of last 20, 25 years where it has gained popularity among the investing class as well as those who are fascinated by financial world.

If we know that Bitcoin is serving as one of the digital currencies, which are basically some sort of cryptocurrency based on certain technology called Bit Blockchain, it serves as a medium of exchange and it also has more or less almost every feature of a sound money.

(Refer Slide Time: 10:17)



If you look at the way Bitcoins are operated or mined, essentially, if you look at a situation where suppose there are two persons, Jack and Jill and Jack uses his private key in his digital wallet to sign a transaction referred to as T in order to pay Bitcoin to another person, Jill.

Once Jack is able to execute the transaction here, Jack sends the reference of transaction T to Bitcoin peer to peer network where there are several miners or Bitcoin miners that ct, the transaction and include it in the blocks that they attempt to mine. Once this a transaction T is included in the blocks of all the transactions, several transactions, it is available on the peer to peer network where there are several miners who might be able to mine it.

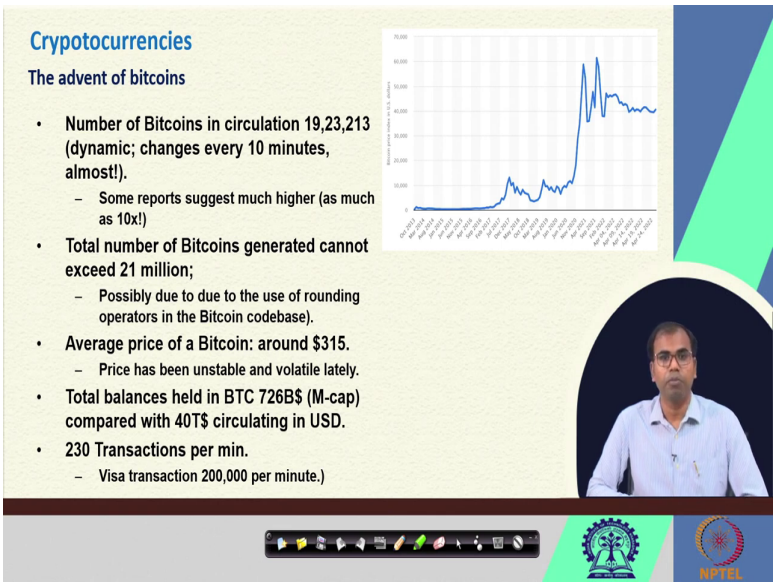
Some miners, let us say M, first solves proof of work puzzle for block N and this block N essentially carries transaction T and thereby validating the block. So, imagine that Jack started with his own personal key, put the transaction T details on peer to peer network in a block and that block is solved by a miner M who solves the block N that includes transaction T and this block N is validated.

Once the block N is validated, then it will have certain features where there will be header, header has from any other previous block and then this transaction is included as part of the network where everyone in the network will add block N to Bitcoin blockchain and then this particular new block is confirmed where transaction T is also confirmed and thus the money, the fund that was included as part of transaction T is transferred to jill.

In the same, in the process, miner M will also get rewarded with new Bitcoins which enter into circulation. This is the whole process of transaction through a Bitcoin network in order to transfer Bitcoins from one user to another user where miners also play a significant role in terms of solving the proof of work puzzle and including the block of transactions on the peer to peer network where block once solved can be validated.

And it is added to the network of block Bitcoin blockchain and then successfully transferred to the recipient who is who is intended to be receiving the Bitcoin. With this kind of secrecy or confidentiality in terms of solving the proof of puzzle and using the personal key for transferring Bitcoin or any other cryptocurrency to any other person.

(Refer Slide Time: 13:49)



We see that Bitcoin is serving as one of the fascinating digital currencies in recent years. If you look at the numbers, we know that as of now we have number of Bitcoins in circulation to the extent of 19,23,213 and it keeps on changing every 10 minutes almost. In fact, if we believe some reports, the numbers is suggested are much higher maybe to the extent of 10 times.

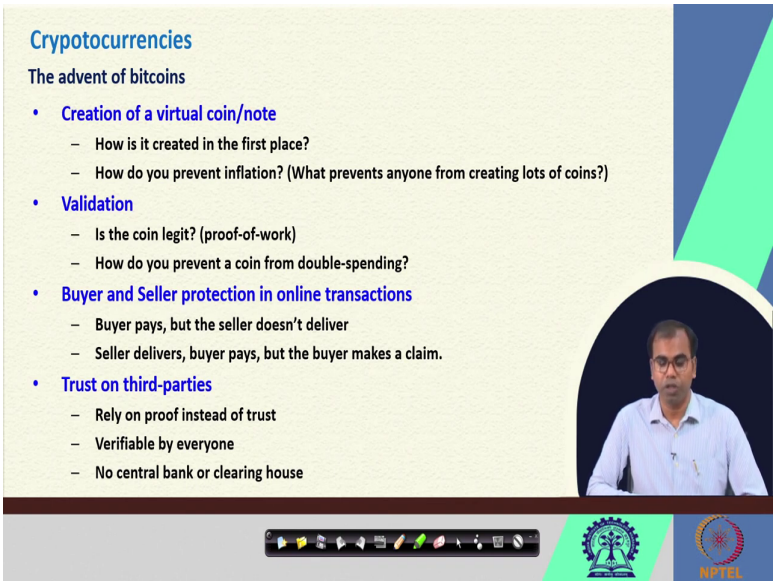
Total on number of Bitcoins cannot be exceeding more than 21 million and this is because the use of rounding operation in the Bitcoin code base. If you look at the average price of a Bitcoin that is around 315 dollar, but it has been unstable and volatile lately, we know that the prices has been going up and down sometimes it was to the tune of thousands of dollars.

Total balances held in Bitcoin value in terms of Bitcoins is 726 billion dollars in terms of market cap which is essentially the number of Bitcoins and the price or the value of every

Bitcoin multiplied with each other. If we compare this value of portfolio or investment or money held in terms of Bitcoin compared with money held in US dollar, we have 40 trillion US dollars being held at any point of time and compared to that 726 billion of bit worth Bitcoin are held in different exchanges, different portfolios.

When we compare the number of transactions per minute for Bitcoin particularly, we see 230 transactions per minute are being carried out with respect to Bitcoin. When it comes to transaction through Visa that is credit card or debit card processing company, when the transaction processed by Visa is 200,000 per minute. Although it might sound trivial, but for being a recent advancement in terms of digital currencies, Bitcoin has been catching up a lot.

(Refer Slide Time: 16:07)



Now, if you look at having looked at these numbers, we might wonder what makes Bitcoin so special. So, if you look at their characteristics, we know that Bitcoin has certain features that

makes it unique and attractive for investors who want to hold assets in diversified portfolio. The first feature is about creation of a virtual coin or a virtual node.

We know that how a particular currency is created in first place and how do we stop the currency to lose its value which is essentially the way we can prevent anyone from creating lot of coins that is how it gains its value or its uniqueness. If there are many people who can mine lot of cryptocurrency, lot of Bitcoins, then; obviously, the Bitcoin will start losing value.

But we know that there are very few people who might be able to successfully mine Bitcoins and thereby the number of Bitcoins to be created can be always limited. Second characteristic is about validation. We need to see whether the coin is legit and that is validated by solving the proof of work puzzle.

So, not every coin is solved easily. So, when we know that if a coin is legit, it cannot be created multiple times, it cannot be spent multiple times. So, we cannot have any coin that is doubly spent or double it was sent in duplicate to multiple people. Also, with respect to Bitcoins, buyers and sellers and their protection particularly in online transaction is of utmost importance.

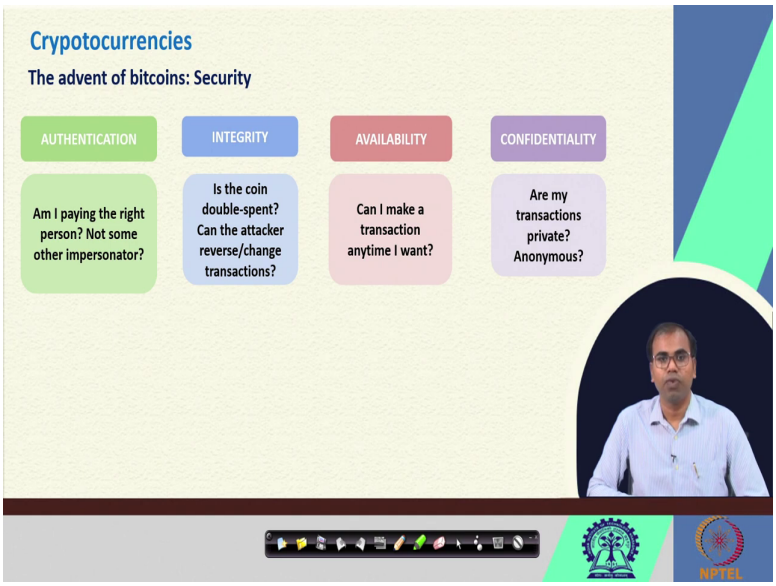
We know that buyers pay, but the seller does not deliver. That is a scenario which might which might make any person afraid. If that happens, then there will be no security or no guarantee of any transaction to be successfully completed. For that similarly, seller delivers buyer pays, but the buyer makes a claim about having paid, but not actually paid.

So, to avoid these situations, we know that Bitcoins are typically included in a blockchain or in a block of Bitcoins only after it is validated by miners who would solve the proof of work puzzle and then only it can be included in the peer to peer network and subsequently included in the block of crypto Bitcoins.

Another unique aspect of Bitcoins in general and cryptocurrency is in general is the trust on third party. Typically, we need to rely on proof instead of trust that is what is happening in

Bitcoins. It is verifiable by everyone on the network and there is no central bank or clearing house that is involved in order to validate or prove any particular Bitcoin or any particular transaction to be true.

(Refer Slide Time: 19:28)



Security is one of the reasons why many people might look at Bitcoins with suspicion. If we look at the security aspect, there are four aspect of securities. The first one is authentication. Security is one of the important aspects for which any investor or any person will look at Bitcoin or for that matter any other cryptocurrency with suspicion. If we look at the security aspect of Bitcoins, the first feature of security or first aspect of security is authentication.

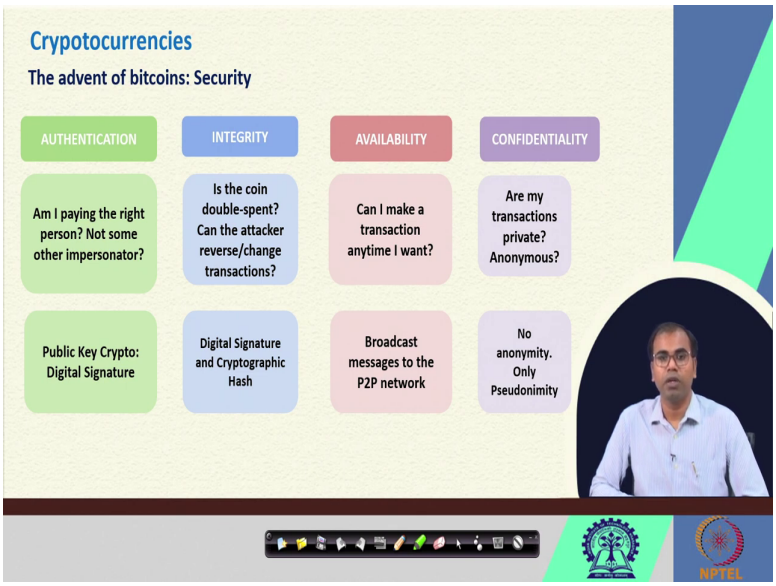
Any person involving in the transaction of Bitcoin will worry whether I am paying the right person and not someone who is impersonating. Second aspect is about integrity. It might be a concern for anyone whether the coin that he has received or he is paying is double spent or

not. Whether there is already a used coins that are coming to me or that I am giving to someone else. Can the attacker reverse or change the transaction?

These aspects essentially indicate towards the integrity. Similarly, availability is another aspect where a person and investor, a person who is making transaction would worry whether I can make transaction any time I want. And finally, the confidentiality or anonymity are my transaction private or are the transaction that I am making through are anonymous.

If you look at these four aspects authenticity, integrity, availability and confidentiality, all these four features with respect to security are well integrated, well included in the cryptocurrencies in general and Bitcoins in particular.

(Refer Slide Time: 21:26)



When you look at the authentication, essentially it is taken care of as well as other features such as integrity, availability and confidentiality. When it comes to authentication, we have seen that the authentication is done through a publicly key crypto where digital signature is involved in the very beginning of the transaction. And subsequently when the transaction is validated, then also minor creates certain public key which are available in the blockchain of cryptocurrencies or blockchain of Bitcoins.

Essentially, it is available as part of the block of transactions which are referred to as N earlier. When it comes to integrity, we have digital signature and cryptographic hash as part of the integrated algorithm when it comes to the validation and integrity of Bitcoins. Similarly, if we talk about availability, mostly broadcast messages are available to the peer to peer network.

So, whenever I want to make a transaction, whether it is to make a payment or to receive a bit, receive a payment in terms of Bitcoin, we can see the broadcast messages on the peer to peer network along with the public key digital signature and key code. And finally, the confidentiality, of course, it might not be 100 percent confidential or anonymous, but it is pseudo anonymous and that makes it more secure than any other currencies in general.

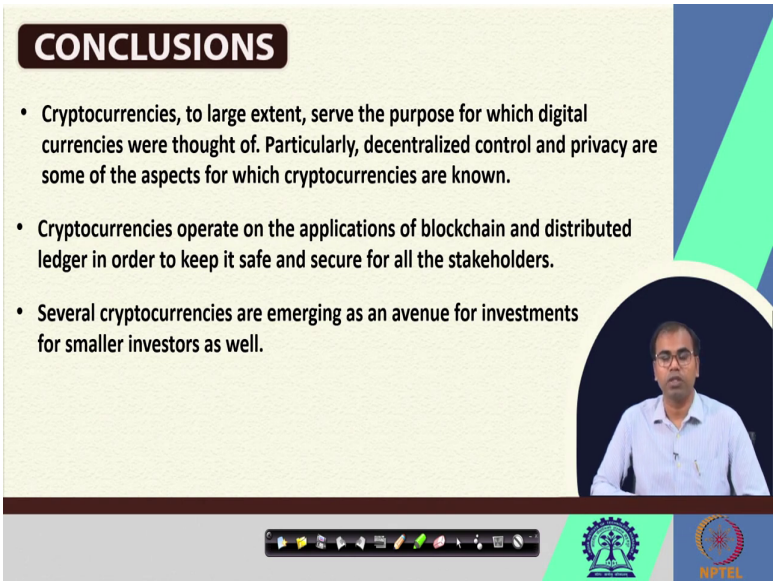
So, with all these four features, we have seen in terms of the way we transact in Bitcoin particularly or in general any other digital currency or cryptocurrency, we have seen that people making transaction need to start with their digital signature or their private key which is used for including that particular transaction in the block of transactions as on the peer to peer network.

Once it is available and included in the peer to peer network in terms of block of transactions, miners start working on it and some minor, some smart minor might be able to successfully solve the proof of work puzzle. And once it is solved, then it is included as part of the block of transactions which are included in the overall peer to peer network where others, other miners can also see.

And once it is validated by the miner, it is included as part of the successful creation of Bitcoin and the transaction is completed in terms of transferring the fund or transferring the money from the peer to the recipient. And in the process, the one who is the person who is mining, the miner also receives certain amount of cut or commission or some value in terms of percentage of Bitcoin.

With all this, we know that cryptocurrency has been emerging as one of the serious contender of currencies particularly when it comes to digital currencies. It has emerged as an asset class that we will see subsequently.

(Refer Slide Time: 25:01)



But in order to summarize, we know that cryptocurrencies to large extent serve the purpose of any digital currencies that were thought of. We know that currencies or money in general

have to have certain features and digital currencies should overcome the issues that comes with physical form of money.

Particularly, if you look at the issues with physical form of money such as currency notes, we know that there is centralized control where central bank in any country will take care of the issuance of the currency notes and will monitor the exchange of currency notes or money from one person to another person or one place to another place. That issue has been worked upon in terms of when it comes to digital currency.

In we know that particularly in case of digital currencies, decentralized control and privacy are some of the aspects for which cryptocurrencies are appreciated. Cryptocurrency also operate on the applications of blockchain and distributed laser in order to keep it safe and secure for all the stakeholders. Most of the time, all the transactions are anonymous or at least pseudo anonymous where no outsider can easily trace the origin of the transaction or the end of the transaction.

And finally, several cryptocurrencies are emerging as an avenue of investment for small as well as big investors. And we have seen in recent years that people in financial market have been showing keen interest in terms of considering cryptocurrencies as one of the asset classes and they wish to include this asset class as part of their portfolio and we will see that in the subsequent session. That is all for now.

Thank you.