Advanced Financial Instruments for Sustainable Business and Decentralized Markets

Prof. Abhinava Tripathi
Department of Management Sciences
Indian Institute of Technology-Kanpur

Week 11
Lecture No. 32

In this lesson, we start the discussion with the blockchain background of cryptocurrencies. Next we introduce modern monetary and payment systems and explain it with the help of money flower concept. We highlight how cryptocurrencies have emerged as a novel instrument in this money flower taxonomy. Next we discuss the market dynamics and volatility of cryptocurrencies with the help of blockchain example. Subsequently, we discuss the distributed ledger technology and its application in cryptocurrency blockchains. We discuss both the permissioned and permissionless blockchain.

We explain the mechanics of cryptocurrency transactions with the help of a simple example. Next, we discuss the benefits of cryptocurrencies. Then we explain the evolution in market dynamics including historical prices, market capitalization of cryptocurrencies with the help of two major currencies namely Bitcoin and Ethereum. We also compare and draw parallels between cryptocurrency and conventional monetary instruments such as cash and bank deposits.

Lastly, we discuss some of the challenges faced by cryptocurrency due to the limitation of permissionless blockchains. Then we conclude the discussion with a comparison between shared currency and cryptocurrencies. In this video, we will introduce cryptocurrencies with the blockchain background behind them. In the previous lesson, we discussed that blockchains are tamper-evident and tamper-resistant digital ledgers implemented in a distributed fashion often, like without a central repository and usually without a central authority like a bank or government. At their very basic level, they enable a community of users to record transactions, these blockchains, to record transactions in a shared ledger within that community such that under normal operation of the blockchain network, no transaction can be changed once published.

Cryptocurrencies: Blockchain Background

- Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion
- In 2008, blockchain was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority. The first such blockchain-based cryptocurrency was Bitcoin.
- Within the Bitcoin blockchain, information representing electronic cash is attached to a digital address
- Blockchain technology is the foundation of modern cryptocurrencies, so named because of the heavy usage of cryptographic functions

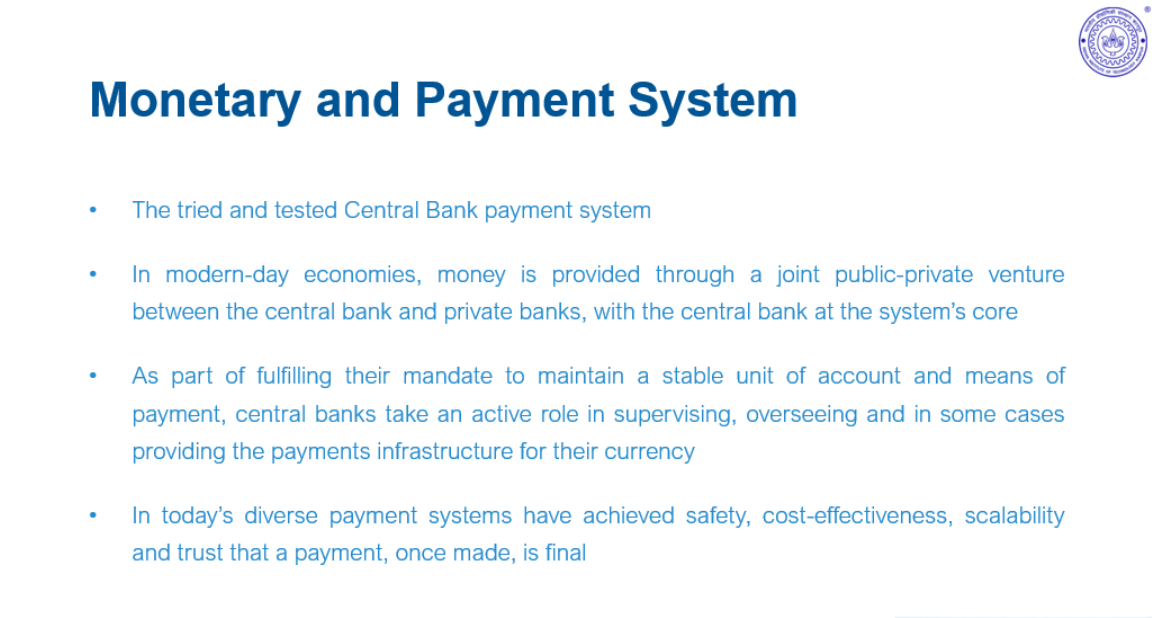
So it's like immutable chain. In 2008, this blockchain idea was combined with several other technologies and computing concepts to create what we call as modern cryptocurrencies or electronic cash protected through cryptographic mechanisms instead of central repository like a central bank. The first such blockchain based cryptocurrency was Bitcoin which is running today. Now within the Bitcoin blockchain, information representing electronic cash is attached to a digital address. Bitcoin users can digitally sign and transfer rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all the participants of the network to independently verify the validity of the transactions.

The Bitcoin blockchain is stored, maintained and collaboratively managed by a distributed group of participants. This along with certain cryptographic mechanisms makes the Bitcoin blockchain resilient to attempts to alter the ledger later, like modifying blocks or forging the transactions or duplicating the transactions. What we have already discussed as double spend problem is an example of it. Lastly, the blockchain technology is the foundation of the modern cryptocurrencies, so named because of the heavy usage of cryptographic functions. Users utilize public and private keys here to digitally sign and securely transact within that blockchain system.

For cryptocurrency based blockchain networks like Bitcoin which utilize mining, users may solve these puzzles using cryptographic hash functions in the hope of being rewarded with the native currency with a certain amount of native cryptocurrency. However, blockchain technology may be more broadly applicable than just simply cryptocurrencies. And this mining process we have already discussed in the previous lessons. To summarize this video, we noted that in Bitcoin and similar systems, the transfer of digital information

that represents the electronic cash takes place in a distributed system. Bitcoin users can digitally sign and transfer their rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all the participants of the network to independently verify the validity of the transactions.

The Bitcoin blockchain is independently maintained and managed by a distributed group of participants. This along with cryptographic mechanisms makes the blockchain resilient to attempts to alter the ledger later like modifying and forging the transactions. And blockchain technology has thus enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum. In this video, we will discuss cryptocurrencies in the backdrop of monetary and payment system. We will also apply the money flower concept to it.



Let us start with the tried and tested central bank payment system. The tried, tested and resilient way to provide confidence in money in modern times is the independent central bank. This means agreed goals, clear monetary policy and financial stability objectives, operational instruments like interest rate and administrative independence, democratic accountability so as to ensure broad based political support and legitimacy. Independent central banks have largely achieved the goal of safeguarding society's economic and political interests in a stable currency, the fiat currency. With this setup, money can be accurately defined as an indispensable social convention backed by an accountable institution within the state that enjoys public trust.

In almost all modern day economies, money is provided through a joint public-private venture between the central bank and private banks with the central bank at the core of the

system. Often, electronic bank deposits are the central or main means of payment between ultimate users while central bank reserves are the means of payment between banks. In this two-tiered system, trust is generated through independent and accountable central banks which backs reserves through their asset holdings and operational rules. In turn, the trust in bank deposits is generated through a variety of means including regulation, supervision and deposit insurance schemes, many of them ultimately emanating from the power of state. As part of fulfilling their mandate to maintain a stable unit of account and means of payment, central banks take an active role in supervising, overseeing and in some cases providing the payment infrastructure for their currency.

Here the central bank's role includes ensuring that the payment system operates smoothly and seeing to it that the supply of reserves responds appropriately to shifting demand including at intra-day frequency i.e. ensuring an elastic money supply. Lastly, thanks to the active involvement of central bank, today's diverse payment systems have achieved safety, cost-effectiveness, scalability and trust that a payment once made is final. Thus, payment systems in modern world or modern economies are safe and cost-effective.

They can handle high volumes and accommodate rapid growth with hardly any abuse and at low cost. An important contributor to safety and cost-effectiveness is scalability. In today's sophisticated economies, the volume of payments is huge, equal to many multiples of GDP. Despite these large volumes, expanding use of the instrument does not lead to a proportional increase in cost. This is important since an essential feature of any successful money and payment system is how widely used it is by both buyers and sellers.

The more others connect to a particular payment system, the greater one's own incentive to use it. In this backdrop, users not only need to have trust in the money itself, they also need to trust that a payment will take place promptly and smoothly. A desirable operational attribute is the certainty of payment or finality and the related ability to contest transactions that may have been incorrectly executed. Finality requires that the system be largely free of fraud and operational risks at the level of both individual transactions and the system as a whole. So strong oversight and central bank accountability both help to support finality and hence the trust.

In this backdrop, while most modern day transactions occur through means ultimately supported by central banks, over time a wide range of public and private payment systems have also emerged. These can be best summarized by a taxonomy characterized as money flower as we can see here. The money flower distinguishes four key properties of the money. This includes the issuer, for example issuer can be a central bank or the system where there is no central authority. The central bank as was the case when the money took the form of a commodity, so one major issuer can be central bank and like we said another

system could be where there is no central authority.

The other system or the other taxonomy is of the form. The form can be physical like metal, coin, paper like banknote or digital like today we have UPI system in India or cryptocurrency. The other is degree of accessibility, so it can be widely accessible like a commercial bank deposit or like a central bank reserve less accessible so that is also there. So accessibility can be very wide high or low. Then you have the payment transfer mechanism, so you can have a payment transfer mechanism one extreme is like peer to peer and other extreme would be like a central bank inter through a central bank intermediary like for deposit.

So each of these four dimensions the accessibility, the digital or not so digital, the central bank, or there is no central authority and peer to peer or there is some intermediary. So all these have two extremes as we discussed. So let's take my instrument, so if you think of cash, cash is widely accessible, the cash is also can be transferred peer to peer. In India, there is a so here we are thinking in terms of fiscal cash but India you have a UPI version of digital cash valets also, but here we are thinking of cash physical cash terms so it is not part of that digital shape. Then it is also central bank issued so it is in this green shape.

Now you have this virtual currency that virtual currency is digital. It is not central bank issued like cryptocurrency is not central bank issued so it is not there it is outside that it is often not widely accessible so it is outside it. So this way you can think of it bank deposits for example if you take bank deposits, so bank deposits are widely accessible. They are issued by private banks so not in the green shape. They're also not peer to peer they are through banks, there is an intermediary.

So in this way each of the instrument can be sort of categorized in all these dimensions like widely accessible digital central bank issued and peer to peer and so on. Lastly, if you think of digital currency, particularly in the permission version of digital ledger, it will be digital so it is in the blue shape. Then it is also peer to peer so it is in the yellow kind of shape. It is not part of central bank. So it is not in the green and also not so much widely accessible so it because to access you need to have certain systems and certain computing power and so on.

So it is not part of that red widely accessible shape. So this way you can under this taxonomy you can define cryptocurrency also. Here while discussing money one needs to make a distinction between two forms of money or two basic technologies called tokens like the cash in a physical form or account based like bank deposits. Now token based money for example bank notes or physical coins can be exchanged in a peer to peer setting but such exchanges rely critically on the pay's ability to verify the validity of the object.

For example with cash you are worried about counterfeiting of notes.

So you would like to have your cash or the physical form of the cash to be unforgeable and valid not counterfeit. In contrast when systems are based on account money like bank deposits they fundamentally depend on the ability to verify the identity of account holder. Now in this case an intermediary like a bank a private commercial bank would verify the entity of account holder and then only the transaction would take place. So to summarize this video we introduced the modern payment systems and we also discussed the money flower taxonomy concept of money across which we can classify various monetary instruments and lastly we discussed how cryptocurrency falls on this money flower taxonomy. In this video we will discuss the rise of a new flower cryptocurrency monetary instrument in our taxonomy of money flower.

To begin with we note that cryptocurrencies aspire to be a new form of currency and promise to maintain trust in the stability of their value through the use of technology. Thus cryptocurrencies consist of three key elements. First a set of rules or protocol that is computer code specifying how participants can transact. Second a ledger storing the history of transaction and third a decentralized network of participants that updates store and read the ledger of transactions following the rules of the protocol. With these three elements they advocate or claim that a cryptocurrency is not subject to potentially misguided incentives of banks and so real fiat currencies.

Monetary and Payment System

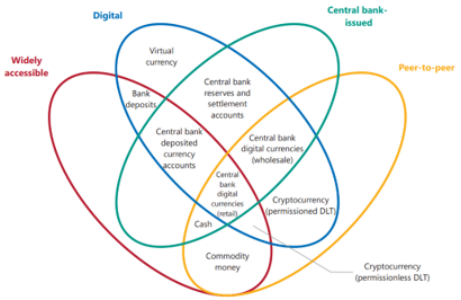
- While most modern-day transactions occur through means ultimately supported by central banks, over time, a wide range of public and private payment means has emerged.
- These can be best summarized by a taxonomy characterized as the “money flower.”
- The money flower distinguishes four key properties of money: the issuer, the form, the degree of accessibility, and the payment transfer mechanism.

Coming back to our money flower taxonomy cryptocurrencies can be identified there with and they combine three key features. First they are digital aspiring to be a convenient means of payment and relying on cryptography to prevent counterfeiting and fraudulent

transactions. Second although they are created privately they are nobody's liability unlike the conventional currencies like cash that is for example dollar rupee so they cannot be redeemed and their value drives only from the expectation that they will continue to be accepted by others. This makes them akin to a commodity money although without an intrinsic value in that sense and lastly these cryptocurrencies allow for digital peer to peer exchange which is very important compared with other private digital money such as bank deposits the distinguishing feature of the cryptocurrency is the digital peer to peer exchange. What it means is that digital bank accounts have been around for decades and privately issued virtual currencies for example as used in the massive multiplayer online games like warcraft and so on they predict cryptocurrencies by more than a decade.

The Money Flower: A Taxonomy of Money

- The issuer can be a central bank, a bank, or nobody, as was the case when money took the form of a commodity.
- Its form can be physical, e.g., a metal coin, paper banknote, or digital.
- It can be widely accessible, like commercial bank deposits, or narrowly so, like central bank reserves.
- A last property regards the transfer mechanism, which can be either peer-to-peer or through a central intermediary, as for deposits.



Source: Central bank cryptocurrencies
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

However in contrast to these the cryptocurrency transfers in principle takes place in a decentralized kind of setting without the need for a central counterparty to execute and verify the exchange. So underlying this setup the three key features the key features of these cryptocurrencies is the implementation of set of rules that aim to align the incentives of all the participants so as to create a reliable payment technology without a centralized strategy. Now the protocol determines the supply of these assets in order to counter debasement for example in the case of bitcoin it states that not more than 21 million bitcoins can exist and in addition the protocol is designed to show that all participants follow the rules of this rules out of self-interest that is they yield a self-sustaining equilibrium. Now like we said there are three key aspects or features associated with this as follows. First the rules entail a cost to updating ledger this distributed ledger in most cases this cost comes because updating requires that proof of work consensus mechanism which is a mathematical evidence as we have discussed in the previous lesson this mathematical evidence that a certain amount of computational work has been done and in turn calling

for costly equipment and electricity consumption.

Since this proof of work process can be likened to a digging up rare numbers via laborious computations it is often referring to as mining in return for their effect these miners receive fees in the form of native currency from the users and if specified by the protocol some newly minted native cryptocurrency. Second all miners and users of cryptocurrency verify all ledger updates which include miners to include only valid transactions. Valid transactions need to be initiated by the owners of fund and must not be attempts to double spend or malicious attempts. So if a ledger update includes an invalid transaction it is rejected by the network and the miners rewards are voided. The verification of all new ledger updates by the network of miners and users is thus essential to incentives or sort of incentivize miners to add only valid transactions.

The Money Flower: A Taxonomy of Money

- The key feature of these cryptocurrencies is the implementation of a set of rules (the protocol) that aim to align the incentives of all participants
- Three key aspects are the following.
- First, the rules entail a cost to updating the ledger.
- Second, all miners and users of a cryptocurrency verify all ledger updates, which induces miners to include only valid transactions.
- Third, the protocol specifies rules to achieve a consensus on the order of updates to the ledger.

So this incentivizes miners to add only valid transactions and lastly the protocol that we discussed specifies the rules to achieve a consensus on the order of updates to the ledger what it means is that this is generally done by creating incentives for individual miners to follow the computing majority of all the miners when they implement updates such coordination is needed for example to resolve cases where communication lags lead to different miners adding conflicting updates that is updates that include different set of transactions. To summarize, in this video we discussed the role of cryptocurrencies as a new flower in the money plot taxonomy. We also noted three very important aspects of the cryptocurrency first the protocol on which they are run second the digital aspect and lastly the peer to peer lending and transaction this peer to peer lending is sort of decentralized network or decentralized nodes and another important aspect is the ledger distributed ledger aspect of these cryptocurrencies which makes them a unique new flower

in the money plot taxonomy. In this video we will briefly introduce cryptocurrencies and discuss their market dynamics. To begin with cryptocurrencies are digital tokens they are type of digital currency that allows people to make payments directly to each other through an online system.

Cryptocurrency: Introduction

- Cryptocurrencies are digital tokens. They are a type of digital currency that allows people to make payments directly to each other through an online system.
- Cryptocurrencies have no legislated or intrinsic value; they are simply worth what people are willing to pay for them in the market.
- There are a number of cryptocurrencies – the most well-known of these are Bitcoin and Ether.
- Just like physical money, such as the United States dollar or Mexico's peso, crypto can buy goods and services.

Source: Coindesk.com

Cryptocurrencies have no legislated or internal value intrinsic value like a fiat currency or any other stock they are simply worth what people are willing to pay for them in the market so there is no intrinsic value. There are number of cryptocurrencies cryptocurrencies particularly the most well known of these are bitcoin and ethereum or ether. Now just like the fiscal money for example dollar for US dollar United States dollar or Mexican PISO crypto can also help you buy goods and services. So we can say that crypto or cryptocurrency is a digital currency that operates slightly differently from the traditional currencies like dollar and PISO just like physical money like dollar and peso you can buy goods and services and cryptocurrency also functions as an investment in the same way like metal goods commodity and as a hedge against ups and downs of government issued money and other assets. However while a centralized government issues fiscal money cryptocurrency money comes from decentralized system of digital record keeping or what we call as distributed ledger system of blockchain where it is not regulated by an official authority.

Activity in the Cryptocurrency markets

- Activity in cryptocurrency markets has increased significantly. The fascination with these currencies appears to have been more speculative (buying cryptocurrencies to make a profit) than related to their use as a new and unique system for making payments.
- Related to this, there has also been a high degree of volatility in the prices of many cryptocurrencies.
- For example, the price of Bitcoin increased from about US$30,000 in mid 2021 to almost US$70,000 toward the end of 2021 before falling to around US$35,000 in early 2022. Rival cryptocurrencies like Ether have experienced similar volatility.

Source: https://www.coindesk.com/price/bitcoin/

Let us briefly discuss the activity of cryptocurrency markets. So activity in cryptocurrency markets has increased significantly in the last 5 to 10 years as we can see on this graph there has been periods of extreme rise then fall then rise and fall like periods of boom and bust. The fascination with these currencies appears to have been more speculative as we can see here with these periods of boom and bust buying cryptocurrencies to make a profit just for speculative reason rather than any fundamental asset behind it or fundamental reason and also more than related to their use as a new or unique system of making payments. So this is less of a case more is being a speculative asset buying to make a profit. Related to this there also been high degree of volatility in prices of many cryptocurrencies.

For example the price of Bitcoin increased from about $30,000 in mid 2021 to almost $70,000 by end of 2021. So you can see how sharp up movements and also falling around to $35,000 in early 2022. Rival currencies like Ether have also experienced similar volatility. This extraordinary interest in cryptocurrencies has also seen a growing amount of computing power used to solve the complex codes that many of these systems use to help protect them from being corrupted like proof of work consensus mechanism and despite the increased level of interest in cryptocurrencies there is also a skepticism about whether they could ever replace the traditional modes of payment or what we call as national fiat currencies. Let us also discuss the briefly the nature of volatile markets in crypto.

So crypto is a rapidly growing market saying that crypto has made queens and poppers. But these wins and losses don't necessarily come from winners picking good coins and losers picking bad ones. It is possible to talk to two people who have both invested in

dodgy coin but one lost money another gained the profit. So whether you win or lose can depend largely on timing. This is so because cryptocurrency is an incredibly sort of volatile topsy turvy investment and all cryptocurrencies experience huge fluctuations in their valuation.

Crypto's Volatility

- "Crypto has made queens—and paupers"
- Cryptocurrencies are famous for exposing investors to wild price changes. Bitcoin, for example, appreciated more than 70 percent during the first quarter of 2021, but on May 19 of that year, dropped by 30 percent in the course of the day
- This question brings up something that we often forget with cryptocurrency: it isn't intrinsically valuable
- There are investors who are interested in crypto not to use it as a currency, but to use it as a hedge against inflation, or as an investment vehicle
- For example, *Vox* cites a fascinating graphic on **"The Musk Effect,"** or the phenomenon of how strongly the value of Bitcoin is affected by Elon Musk's tweets.

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

16

A quality known on Wall Street as volatility. So cryptocurrency is an incredibly volatile investment. In one day Bitcoin value dropped 30% but why such volatility? Cryptocurrencies are particularly famous for exposing investors to wild price changes. Bitcoin for example appreciated more than 70% during first quarter of 2021. But on May 19 of that year dropped by 30% in the course of day before recovering some of its value. Two such dramatic climbs and falls reflect changes in fundamental information about crypto assets or they are driven by investor sentiment.

And as cryptocurrencies become more salient to the financial system, does their price volatility pose a risk to broader financial stability? This question brings up something that we often forget with cryptocurrency that it isn't intrinsically valuable. There isn't any gold or diamonds or anything backing this crypto's value. At no point did the US Treasury or Indian Central Bank say that yes anytime someone wants to bring us a Bitcoin will give them X number of rupees or dollars from our reserves. Not all diehard crypto fans would agree but there is an argument that crypto's value really comes from how much people are willing to trade for it in terms of goods, other cryptocurrencies or dollars. Now there are investors who are interested in crypto not to use it as currency but to use it as a hedge against inflation or as investment vehicle.

But without anything intrinsically valuable backing up the currency, crypto's market value

is based entirely on speculation which is essentially educated guesswork. Investing in something that is speculative is a guaranteed way to introduce volatility in your portfolio. It means that investment value isn't very grounded which makes its price incredibly sensitive to even slight changes in investors' expectations and perceptions. For example, the Musk effect or the phenomena of how strongly the value of Bitcoin affected by Elon Musk tweets. As Elon Musk tweets go, so goes the crypto market up and down.

And this is true for many such currencies. To summarize, in this video, we briefly discussed the properties of cryptocurrencies and focused on market dynamics of Bitcoin. We also noted that these cryptocurrencies unlike other fiat currencies or traditional commodities or assets have nothing backing them and a major motive to invest in these currencies is not as a currency or a store of value but for speculative purposes to make profits. And these currencies are often affected by prevailing sentiment. For example, the Elon Musk tweets have led to many currencies fluctuating up and down. So these currencies when you introduce them to your portfolio or buy them, you also exposed to more volatility.

In a series of next two videos, we will discuss the application of distributed ledger technology in the case of cryptocurrencies. Let us start the discussion about distributed ledger technology in cryptocurrencies. The technological challenge in digital peer-to-peer exchange is the so-called double spending problem. Any digital form of money is easily replicable and can thus be fraudulently spent more than once. Thus, digital information can be reproduced more easily than physical banknotes.

For digital money, solving the double spending problem requires at a minimum that

someone keeps a record of all the transactions. Now prior to cryptocurrencies, the only solution was to have a centralized agent do this and verify all the transactions. Cryptocurrencies overcame this double spending problem via decentralized record keeping through what is known as a distributed ledger. This ledger can be regarded as a file, think of it as an excel work file that starts with an initial distribution of cryptocurrencies and records the history of all subsequent transactions. An up-to-date copy of the entire ledger is stored by each of the users and that is what makes it distributed character.

DLT: Permissioned

- To prevent abuse, the ledger can only be updated by trusted participants in the CC – often termed "trusted nodes."
- Thus, while cryptocurrencies based on permissioned systems differ from conventional money in terms of how transaction records are stored (decentralized versus centralized), they share with it the reliance on specific institutions as the ultimate source of trust.

Source: Central bank cryptocurrencies
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

19

Now with a distributed ledger, peer-to-peer exchange of digital money is feasible and each user can directly verify their copy of the ledger whether a transfer took place or that there was an attempt to double spend. Now please note that while all cryptocurrencies rely on a distributed ledger, they differ in terms of how the ledger is updated. For example, there are two broad classes, one is permission and one is permissionless which differ substantially in their operational setup. We will discuss them one by one. Let us start the discussion with distributed ledger technology which is of permission nature.

DLT: Permissionless

- The ledger recording transactions can only be changed by a consensus of the participants in the currency.
- The concept of permissionless cryptocurrencies was laid out for the case of Bitcoin
- Align the incentives of all participants so as to create a reliable payment technology without a central trusted agent

Source: Central bank cryptocurrencies
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Now this class is based on permissioned DLP or distributed ledger technology. Such cryptocurrencies are similar to conventional payment mechanisms that to prevent abuse, the ledger can only be updated by trusted participants in this cryptocurrency often termed as trusted node. So for example, there is some kind of authorization mechanism which authorizes the trusted or the member nodes only. So there is some kind of authorization mechanism and only these trusted nodes can update the information. Now these trusted nodes are chosen by and subject to oversight by some kind of central authority like the firm that developed the cryptocurrency or some kind of central banking system and so on.

DLT: Permissionless

- First, the rules entail a cost to updating the ledger
- Second, all miners and users of a cryptocurrency verify all ledger updates, which induces miners to include only valid transactions
- Third, the protocol specifies rules to achieve a consensus on the order of updates to the ledger

Source: Central bank cryptocurrencies
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Thus, while cryptocurrencies based on permissioned systems differ from conventional

money in terms of how transaction records are stored, for example centralized versus decentralized here it is decentralized because there are number of nodes but they share with it the reliance on specific institutions as the ultimate source of trust. So whether a node is to be trusted depends on the authority that is given to it by some kind of central authority. To summarize, in this video we discussed the distributed ledger technology DLD in the context of cryptocurrencies. We discussed one method which is permissioned approach to distributed ledger technology application in cryptocurrencies. In the next video we will discuss the permissionless approach to the same.

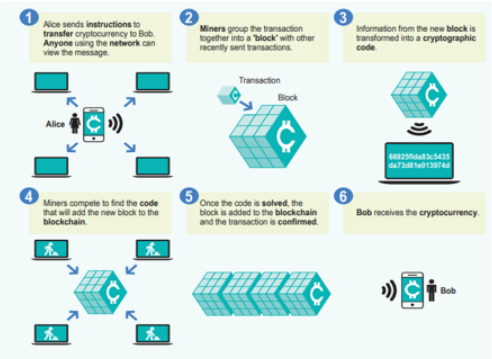
In this video, we will conclude our discussion about cryptocurrencies with respect to distributed ledger technology and permissionless blockchains. In a much more radical departure from the prevailing institutional base setup, a second class of cryptocurrencies or rather more wider class of cryptocurrencies promise to generate trust in a fully decentralized setting using permissionless distributed ledger technology or permissionless DLD. Now the ledger recording transactions here can only be chained by a consensus of the participants in the currency or the blockchain of the currency. While anybody can participate here, nobody has a special key to chain the ledger. So there are a number of member nodes, there is no such authorization mechanism or a central party.

All these are just part of the blockchain. There is no special permission or authorization. Here the concept of permissionless cryptocurrencies started with the case of Bitcoin. It was a white paper by an anonymous programmer or maybe a group of programmers because their identity is not known under the pseudonym of Satoshi Nakamoto. Who proposed a currency which is Bitcoin on a specific type of distributed ledger, the blockchain. Here the blockchain is the distributed ledger that is updated in groups of transactions called blocks.

Blocks here are then chained sequentially via the use of cryptography to form the blockchain. This we have discussed in great detail in the previous lessons. Now this concept has been adapted to countless other cryptocurrencies and blockchain based permissionless cryptocurrencies have two groups of participants. One is called miners who rather act as bookkeepers and users who want to transact or initiate the transaction in the cryptocurrency on that particular blockchain.

How Does a CC Transaction Work?

- Cryptocurrency transactions occur through electronic messages that are sent to the entire network with instructions about the transaction.
- Suppose Alice wants to transfer one unit of cryptocurrency to Bob.
- Alice starts the transaction by sending an electronic message with her instructions to the network, where all users can see the message.



Source: Digital Currencies
https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html

Now at face value, the idea underlying these cryptocurrencies is simple. Instead of a bank centrally controlling the transactions, the ledger is updated by a miner and the update is subsequently stored by all the users and miners on the chain. So there are multiples of users and miners and all the miners and users update their information or ledger on the chain. Now underlying this setup, the key features of these cryptocurrencies is the implementation of a set of rules what you call as protocol that aim to align the incentives of all the participants so as to create a reliable payment technology without a centralized trusted agent like a central bank like RBI. The protocol here determines the supply of the asset in order to counter the debasement. So for example, in the case of Bitcoin, it is stated or the protocol states that not more than 21 million bitcoins should exist 20 million is the maximum bitcoin after which supply would cease.

In addition, the protocol is also designed to ensure that all the participants follow these rules out of self-interest that is some kind of incentive and that yields or results in a self-sustaining endogenous equilibrium. So that results in a self-sustaining endogenous equilibrium on the blockchain transactions. Now this kind of decentralized permissionless mechanism results in three very important aspects and features on the blockchain. First, the rules entail a cost to updating the ledger. In most cases, this cost comes about because updating requires some kind of consensus mechanism like proof of work.

This is like a mathematical evidence. This proof of work is like a mathematical evidence. We have discussed this in great detail in the previous lesson that a certain amount of computational work needs to be done and in turn calling for costly equipment and electricity consumption. Since this proof of work process can be likened to ding up rare numbers via laborious calculations and computations, it is often referred to as mining

process and those who do it called miners on the blockchain. And because of this mining activity in return for their efforts, these miners receive what we call as fees from users. For example, block rewards and transaction fees and if specified by the protocol, this reward is nothing but the newly minted cryptocurrency, the native cryptocurrency from the block.

Second, all miners and users of a cryptocurrency verify all ledger updates which includes miners to include only valid transactions. So valid transactions need to be initiated by the users or owners of the fund and must not be attempts to double spend. If a ledger update includes an invalid transaction, it is rejected by the network and the miner rewards are voided. So then they won't get reward if it is an invalid transaction. The verification of all new ledger updates by the network of miners and users is thus very essential to incentivize miners to add only valid transactions.

So there is an incentive mechanism for the miners to validate the transactions which sort of rewards them for this service or activity. Third, the protocol specifies rules to achieve a consensus on the order of updates to the ledger. Now this kind of consensus is generally done by creating incentives for individual miners to follow the computing majority of all other miners when they implement updates. Such coordination is needed. Recall our Byzantine general problem and such coordination is needed for example to resolve cases where communication lag may lead to different miners adding conflicting updates that is updates that include different set of transactions.

Now with these key key ingredients, it is costly though not impossible for any individual to forge a cryptocurrency. To successfully double spend a counterfeiter would have to spend their cryptocurrency with a merchant and secretly produce a fought blockchain block, a block with the fought information which is incorrect in which this transaction was not recorded. Upon receipt of the merchandise, the counterfeiter would then release the fought blockchain, that is reverse the payment. But this fought blockchain would only emerge as the commonly accepted chain if it were longer than the blockchain, then the rest of the network of miners had to produce in the meantime. Now a successful double spend attack like this requires a substantial share of mining community's computing power, in fact a huge amount of computing power.

Conversely, in the words of the original Bitcoin white paper, a cryptocurrency can overcome this double spend problem in a decentralized way only if honest nodes control a majority of the computing power. To summarize, in this video we discussed how permissionless blockchains or blockchains that are based on distributed ledger technology using permissionless blockchains operate through a set of protocol and rules, how they ensure that even in the absence of a centralized authority the transactions are correctly

verified, validated and miners or the nodes or computers or networks, members on the blockchain they get rewarded and out of this incentive mechanism they act in the best interest of blockchain by validating these transactions by putting computing power and effort. In this video, we will understand cryptocurrency transactions with the help of a simple example. Please note cryptocurrency transactions occur through electronic messages that are sent to the entire network with instructions about the transaction. These instructions include information such as electronic addresses of the parties involved, the quantity of the currency to be traded and a time stamp.

Suppose Alice wants to transfer one unit of cryptocurrency to Bob. Now Alice starts the transaction by sending an electronic message with the instructions to the network where all the users can see the message. So now the transaction is initiated by Alice. Alice sends the instruction to transfer the cryptocurrency to Bob and this signal is transmitted to all the member nodes on the or all the nodes on the blockchain.

Anyone using the network can view this message. So it is available to all public. Now Alice transaction is one of a number of transactions that have recently been sent. Since the system is not instantaneous, the transaction sits with a group of other recent transactions waiting to be compiled into a block which is just a group of most recent transactions. So the miners or the members on this, those who are using or on this network blockchain, they will group the transaction together into a block with the recent transactions. So all the more recently concluded transactions will be added to a block. Now the information in the block is turned into a cryptographic code through hash function and minus compete to solve the code to add the new block of transaction to the blockchain.

So information from the new block is transformed into a cryptographic code of some sort. So this block information that is there is created into some kind of code, cryptographic code through hash function and miners try to solve this puzzle, this kind of mathematical puzzle for them. And the miners, they will compete to find the code and once they perform or compute this mathematical puzzle, the new block will be added to the blockchain. So once a miner successfully solves the code, other users of the network will verify his solution like proof of work mechanism and reach an agreement that his solution or proof of work is valid and therefore the block is verified, the new block of transaction is added to the end of blockchain and else transaction is confirmed. So once the code is solved by the miner, the block is added to the blockchain and the transaction is confirmed and it is verified by all the nodes on the blockchain. So it is added, the new block is added to the block chain, the blockchain elongates, it is added and the transaction is successful.

Now this confirmation of the successful transaction is not instant, it is take time for blocks of transaction to be processed so that users can be certain that their transaction has been

successful and if it is successful, then Bobs receive the cryptocurrency. To summarize, in this video we saw with the help of a simple example how a cryptocurrency transaction works with the help of distributed ledger technology that is blockchain. In this video, we will discuss the benefits of cryptocurrencies that have led to the widespread adoption of the same. There are several advantages of using cryptocurrencies over traditional or fiat money. From its ease of use to its availability and security, cryptocurrency has become a viable alternative to traditional money by offering users new and unique features.

Benefits of Cryptocurrencies

1. Very low transaction costs
2. Anyone can use it.
3. No limits on transactions.
4. Sends funds locally and internationally
5. 24/7 access to your money
6. Private and secure
7. Decentralized

Let us discuss some of these benefits and features. First, very low transaction costs. The blockchain that supports cryptocurrency replaces traditional payment processes that verify payments and transfers. By removing these middlemen such as banks from the equation, crypto allows users to make purchases with much lower fees than actual currency. Next, anyone can use it. Cryptocurrencies hold a great value for people who lack access to banks or unbanked population. Unlike setting up a bank account, which often requires several layers of identification and documentation, users need only a smartphone or access to the internet to use cryptocurrency.

No limit on transactions. The lack of centralized authority and control means that no one can impose limits on crypto transactions. Crypto users are free to use their assets as often as they like without any restrictions on the number of purchases or withdrawals. One can send funds locally and internationally also. Because crypto exists online only, there are no boundaries, it is easy to transfer money 24x7 anywhere, you can access your money, you can send it to anybody.

So another advantage is 24x7 access to your money. Crypto doesn't keep bankers' hours, there are no intermediaries. The publicly available record is viewable all the time and users do not have to wait to access their funds. It is private, secure and provides quasi-anonymity. The technology that powers cryptocurrency, the blockchain distributed ledger, ensures that users stay anonymous.

And advanced cryptography practices ensure that additional currency is safe from thieves. Bitcoin has never been hacked to date. However scamming and fraud are common in the crypto space as with all the currencies. Lastly and most importantly, it is decentralized. Cryptocurrencies do not need a government or company to record transactions, issue new currency or record investments.

No bad economic policy or bank breakup can directly affect their value. To summarize, in this video, we discuss the key features and properties of cryptocurrencies. First low transaction costs, widespread usage, no limits on transactions, one can send funds locally and internationally across borders, 24x7 access to your money, private and secure, anonymity and decentralized peer-to-peer access. In this video, we will understand the trading activity of Bitcoin and its evolution with the help of changes in market cap and pricing. The most well-known cryptocurrency is Bitcoin. It was launched in 2009, a year after the report that described the Bitcoin system and was released under the name Satoshi Nakamoto.

The system was designed to electronically mimic features of a cash transaction. It was designed to allow peer-to-peer or person-to-person transactions without the need to know or trust the other person in the transaction and to occur without the need for a central party such as Central Bank. Unlike conventional national currencies such as dollars which get part of their value from being legislated as a legal tender, Bitcoin and other cryptocurrencies do not have any legislated or internal value. Instead, the value of Bitcoin is determined by what people are willing to pay for it in the open market and in theory its value could very well fall to zero at any time. Now one feature of the Bitcoin system is that of its supply. It increases as a certain predetermined rate and is capped at around 21 million after which the supply will stop.

Bitcoin

- The most well known cryptocurrency is Bitcoin. Bitcoin was launched in 2009, a year after a report that described the Bitcoin system was released under the name Satoshi Nakamoto
- One feature of the Bitcoin system is that the supply of Bitcoins increases at a pre-determined rate and is capped at around 21 million
- The integrity of the Bitcoin system is protected by 'cryptography', which is a method of verifying and securing data using complex mathematical algorithms

https://en.wikipedia.org/wiki/Bitcoin#/media/File:Bitcoin.svg

Also each Bitcoin is subdivided into 100 million satoshis or what you can say is 10 to the power minus 8 fraction which relationship is sort of similar to rupee, passe and dollar cent. Because of this, the supply of Bitcoin has been commonly compared to the supply of a scarce commodity like gold because of this limited supply of 21 million. The Bitcoin system allows transactions to occur directly from person to person without requiring a central party or counterparty to verify or record the transactions. This is unlike most conventional payment methods such as electronic bank transfers which rely on a central party to keep and update record of transactions. For example, commercial banks maintain a record of their customers' account balances, deposits and withdrawals.

Instead, the Bitcoin system uses blockchain technology as we have been discussing in previous lessons to record transactions and the ownership of Bitcoins. This is essentially the technology that connects group of transactions or what we call as blocks and connect these blocks together over time in the form of a chain what we call as blockchain. So blocks connect it and make blockchain. Each time a transaction occurs, it forms part of a new block that is added to the chain and as a result, the blockchain provides a record or database of every Bitcoin transaction that has ever occurred.

And is available for anyone to access and update on a public network. This is often referred to as a distributed ledger or DLT that we have discussed in the previous lessons. Lastly, the integrity of this Bitcoin system as we have discussed is protected by cryptography, which is a method of verifying and securing data using complex mathematical algorithms or computer codes. Now, this makes the system very difficult to correct. Bitcoin transactions are verified by other users of the network and the process of compiling, verifying and confirming transactions is often referred to as mining. In

particular, complex codes need to be solved to confirm transactions and make sure that the system is not corrupted.

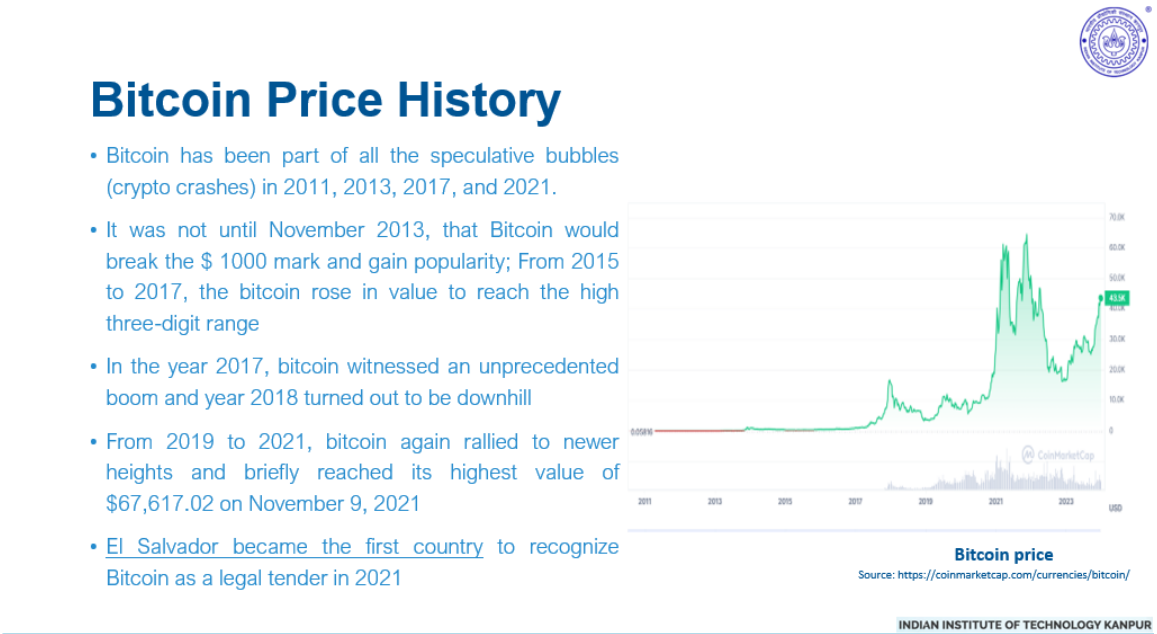
Thus, the Bitcoin system increases the complexity of these codes as more and more computing power is used to solve them. A new block of transactions is compiled approximately every 10 minutes and miners want to solve the codes and process transactions because they are rewarded with new Bitcoins or native cryptocurrency on that particular blockchain. Now, this increase in competition between miners for new Bitcoins has seen large increases in the amount of computing power and electricity consumption, particularly for running the computer systems and cooling requirements. While it is difficult to calculate with precision, some estimates suggest that now the annual energy consumption of Bitcoin system has roughly become equal to smaller countries like Thailand.

Let us discuss the evolution of Bitcoin market cap. As you can see in this diagram, it has witnessed a lot of tumultuous period. There have been periods of boom and bust. Bitcoin is the first cryptocurrency ever introduced and considered as digital gold and it currently has a market cap of 858.77 billion dollars, which is the largest of any variant of cryptocurrency. A unit of Bitcoin can be broken into 100 million satoshis, which is equivalent to the relationship between rupee, paise or dollar set.

Furthermore, the Bitcoin network is so designed that it can only have maximum 21 million units of Bitcoin circulation at any point in time. And this limited availability is a primary component that also sort of limits its supply and drives its prices. Some other important information points are as follows.

Bitcoin had a market cap of 1.2 billion dollar on May 1st, May 2013. It took Bitcoin nearly nine years from the date of its creation to reach the 100 billion mark when it reached 100.1 billion in market capitalization around October 2017. And from October 2017 to 2020, the market capitalization of Bitcoin remained under 250 billion dollar mark. But from November 2020 to February 2021, the Bitcoin grew at an unprecedented rate of 321 percent to reach the 1000 billion dollar capitalization briefly.

And on November 2021 itself, Bitcoin briefly reached its highest market capitalization of 1.28 trillion with a price of around 67,617 per Bitcoin. So it witnessed quite a huge tumultuous up and down but mostly it has been a story of high growth as we can see and that is why it has captivated the investor community. Let us also discuss the pricing history of Bitcoin and like we discuss its market cap, it has been a history of growth but filled with periods of booms and busts. In the history of cryptocurrencies, Bitcoin has played a very pivotal role and emerged as a major cryptocurrency and also it has been part of all the spectrometric bubbles or what we call as crypto crashes.



In 2011, 2013, 2017, 2021 all the crypto crashes. During the initial years, Bitcoin had limited popularity and would occasionally reach the double digit threshold but would soon turn to the single digit price range. So there have been periods of rise and fall and it was not until 2013 that Bitcoin broke the 1000 dollar mark and gained popularity and it briefly attained that $1,127 price around November 2013. Then Bitcoin stayed in the higher three digit range during the first half of 2014 but soon began sliding in the lower three digit range and finally hit the lower of 172 dollars around January 2015. Now from 2015 to 2017 Bitcoin rose in value to reach the high three digit range and managed to reach the

1000 dollar mark for the second time when it reached $1,008 around February 2017.

Next in the year 2017 Bitcoin witnessed an unprecedented boom and managed to cross the 1000 dollar mark. It briefly reached even 17,000 to 50 dollar approximately around December 2017 and the year 2008 turned out to be in the downhill with the Bitcoin value witnessing freefall for the most part of the year and only to stabilize by the end of 2018 reaching and maintaining its value around 3000 dollar mark. From 2019 to 2021 Bitcoin again rallied to newer heights and briefly reached its highest value of around $67,617 in November 2021 and from November 2021 Bitcoin once again dipped in value. So it has been a journey of highs and lows continuously and in terms of adoption El Salvador became the first country to recognize Bitcoin as a legal tender in 2021. El Salvador has been experimenting with the use of Bitcoin as a currency since 2019 and the legislative assembly of El Salvador passed a bill in June 2021 which recognized Bitcoin as a legal currency with El Salvador. In February 2022 Ukraine also announced the legislation of cryptocurrencies with limitations and similarly Central African Republic passed a law in April 2022 legalizing the use of Bitcoin and other cryptocurrencies alongside.

So we can see that gradually country by country the cryptocurrencies and Bitcoin in particular have been adopted. To summarize in this video we discussed the pricing and market cap history and evolution of Bitcoin. We noted that it has been a history filled with booms and busts. However overall Bitcoin has gained from a very small value to value in multiple thousands of dollars. Also gradually as the Bitcoin has gained value more and more countries have adopted and recognized its significance. In this video we will discuss the market activity of a very important cryptocurrency that is Ether which runs on Ethereum blockchain.

Ethereum

- Introduced in 2015, ETH is only second to Bitcoin in market capitalization at about 16%.
- ETH's popularity comes from the platform that the Ethereum ecosystem offers. The platform enables building and working on new tools, DeFi ecosystems, smart contracts, etc.
- From 2015 to January 2021, the market capitalization of Ether remained well under the $200 billion mark, but from February 2021 Ethereum grew at an unprecedented rate and breached the $500 billion market capitalization mark briefly on October 21, 2021.

ETH Market Capitalization

Ethereum Market Cap is at 278B- December 2023

Source: https://coinmarketcap.com/currencies/ethereum/#Chart

Ethereum is a decentralized open source blockchain system that features its own cryptocurrency Ether. Ether works as platform for numerous other cryptocurrencies as well as for the execution of decentralized smart contracts. Almost in 2015 Ethereum is only second to Bitcoin in market cap at about 16%. It witnessed tremendous growth especially during Covid-19 when its market cap almost doubled from August 20 to April 2021. And we can see here from a low value close to zero a sharp rise from 21 onwards.

Though the period has been volatile and tumultuous we can see the booms and busts and then a steady rise again. Ethereum was first described in 2013 in a white paper by Vitalik Butrin. Butrin along with other co-founders secured funding for the project in an online public crowd sale in summer of 2014. The project team managed to raise around 18.3 million in Bitcoin and Ethereum's price in the initial coin offering was around 0.31 win dollar with over 60 million Ethers sold. Now taking Ethereum's price now they sports the return on investment at analyzed rate of around 270% essentially almost quadrupling your investment every year since the summer of 2014. Now Ethereum's popularity comes from the platform that Ethereum ecosystem offers. The platform enables building and working on new tools, DeFi ecosystem, smart contracts among others. Its growth will likely continue as individuals and corporations increase interest and use Ethereum related infrastructure and various blockchain services. The Ethereum Foundation officially launched the blockchain on July 2015 under the prototype name Frontier and since then there has been several network updates like Constantinople on February 2019, Istanbul on December 2019, New York Glacier in January 2020, Berlin in April 2021 and most recently August 2021 the London Hardin Forum.

From 2015 to 2021 the market capitalization of Ether remained well under 200 billion

dollar mark but from February 21 Ethereum grew at an unprecedented rate and breached the 500 dollar billion mark capitalization mark briefly on October 21. Now based on this discussion we can see there has been sort of volatile rise in Ethereum prices and it has created a space for itself. Its own purported goal is to become a global platform for decentralized applications along users from all over the world to write and run software that is resistant to censorship, downtime and fraud. To summarize this video we discussed the historical price evolution of Ethereum and its market cap. We noted that along with, alongside with Bitcoin, Ethereum has also created a space for its own because of, particularly because of the platform or the blockchain of Ethereum on which the Ether currency runs and the feature that blockchain offers, it has successfully grown over last 10 years.

Is Cryptocurrency Money?

To answer this, we can ask whether the characteristics of cryptocurrencies match the key characteristics of money:

1. Widely accepted means of payment
2. Store of value
3. Unit of account

- So, while cryptocurrencies can be used to make payments, currently their use as a means of payment is limited, and they do not display the key characteristics of money,

In this video we will draw a comparison and parallel between cryptocurrency and fiat money. A frequently asked question is whether cryptocurrencies can be defined as money. The short answer is cryptocurrency are not exactly a form of money and to answer this question we can ask whether the characteristics of cryptocurrencies match the conventional key characteristics of money or not. First let us talk about widely accepted means of payment. Can cryptocurrency be used to buy and sell things? Money generally comes in the form of a nation's currency and is widely accepted as a means of payment. While cryptocurrencies can be used to buy and sell things, they are not exactly widely accepted as a means of payment for various goods and services.

And surveys suggest that only a small fraction of cryptocurrency holders use them regularly as a means of payments. The next is store of value. Can the purchasing power of cryptocurrencies, that is their ability to purchase a similar basket of goods and services

be maintained over time? Accounting for inflation. Large fluctuations in the price of many cryptocurrencies mean that their purchasing power or the value is not maintained over time, reducing their effectiveness as a store of value. Lastly as a unit of account, are cryptocurrencies a common way of measuring the value of goods and services? In various countries like US, UK, Australia, the price of goods and services are measured in respective currencies like dollar, pound and so on. While some businesses may accept cryptocurrencies as payment, they are not very commonly used as a measure or unit of account and compare prices.

So while cryptocurrencies can be used to make payments, currently their use as a means of payment is limited and they do not display the key characteristics of money as we discussed here. However, there is one type of digital currency that could be considered money, which is the digital currency issued by a central bank. However, this project is in various stages of infancy across different central banks of different countries. To summarize, in this video, we compared and drew parallel between fiat money and cryptocurrency across three dimensions, which is as a use of modes of payment, store of value and unit of account. We noted while that cryptocurrencies do not exactly fit the bill and can be compared with the conventional form of money, still there is a scope for central banking digital currencies, which are initiated by the respective central banks and in future they may become successful experiments as an alternative to forms of fiat money.

Limitations of Permissionless CCs

Economic limitations inherent in the decentralized creation of trust:

- Trust can evaporate at any time because of the fragility of the decentralized consensus through which transactions are recorded.
- Meaning that a CC can simply stop functioning, resulting in a complete loss of value.
- Moreover, cryptocurrency technology comes with poor efficiency and vast energy use.
- Cryptocurrencies cannot scale with transaction demand, are prone to congestion, and greatly fluctuate in value.
- Overall, the decentralized technology of cryptocurrencies, however sophisticated, is a poor substitute for the solid institutional backing of money.

In a series of next two videos, we will discuss the limitations of conventional form of cryptocurrency mode of operation, that is through permissionless blockchains. We highlight that there are economic limitations inherent in decentralized creation of trust. To begin with, trust can evaporate at any time because of the fragility of the decentralized

consensus through which transactions are recorded. This is so because here trust is being created by actions of miners who are predominantly acting on basis self-interest and there is no such authority where which everybody can place their trust on.

Limitations of Permissionless CCs

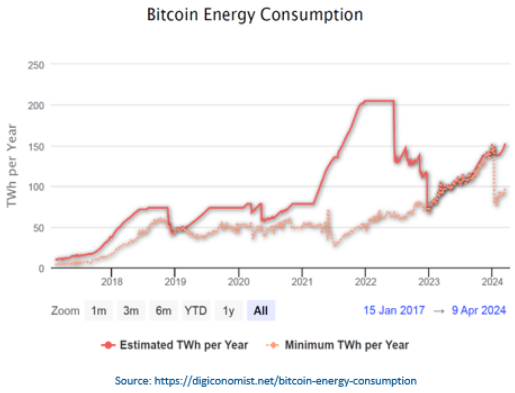
- Cryptocurrencies such as Bitcoin promise to deliver not only a convenient payment means based on digital technology but also a novel model of trust.

1. Does this cumbersome way of trying to achieve trust come at the expense of efficiency?
2. Can trust truly and always be achieved?

It also means that a cryptocurrency can simply stop functioning resulting in a complete loss of value. So if that trust is lost, maybe through some kind of scam, some fraudulent action, if that trust has gone, then suddenly there is a complete loss of value in the system. Moreover, cryptocurrency technology comes with very poor efficiency and vast energy use. So mining process requires heavy energy consumption and as the supply becomes limited, excessive energy consumption levels are witnessed. Also cryptocurrencies cannot scale with transaction demand and are prone to congestion that may greatly fluctuate the value. So as each and the transaction volume increases, the system is designed that with more and more traffic, the blocks may get saturated and extra transactions may have to wait the system and this delay may lead to fluctuations in the value of the transaction itself or the value of cryptocurrency itself because of this delay in transaction.

Cost of generating decentralized trust

- A key potential limitation in terms of efficiency is the enormous cost of generating decentralized trust
- Individual facilities operated by miners can host computing power equivalent to that of millions of personal computers.
- The total electricity use of bitcoin mining equaled that of mid-sized economies such as Switzerland, and other cryptocurrencies also use ample electricity.
- The quest for decentralized trust has quickly become an **environmental disaster**.



Overall, this re-centralized technology of cryptocurrencies, however sophisticated, is a poor substitute, appears to be a poor substitute for solid institutional backing of fiat currency or fiat money. So cryptocurrencies such as Bitcoin promise to deliver not only a convenient payment means based on digital technology, but also a novel mode of trust. But delivering on this promise hinges on some critical assumptions, for example, whether honest miners control the vast majority of computing power and also that users verify the history of all the transactions and that the supply of currency is predetermined by a protocol. Understanding these assumptions is very important for they give rise to two basic questions regarding the usefulness of cryptocurrency. First, does this cumbersome way of trying to achieve trust come at the expense of efficiency, huge consumption of electricity and power? And second, can this trust truly and always be achieved? So as the first question implies, a key potential limitation in terms of efficiency is the enormous cost of generating this decentralized test.

So one would expect the miners to compete to add new blocks to the ledger through the proof of work or some similar consensus mechanism until their anticipated profits go and this leads to exponential rise, exponential rise in power consumption as we can see here over the last five to seven years, there has been exponential rise in power consumption. So the individual facilities operated by miners can host computing power equivalent to that of millions of personal computers. So there is an exponential rise in power and those with large setup can guzzle powers like anything. The total electricity use of Bitcoin mining is related to that of mid-sized economies such as Switzerland and other cryptocurrencies also use huge amount of electricity.

So you can imagine the kind of power consumption that is involved with a consensus or

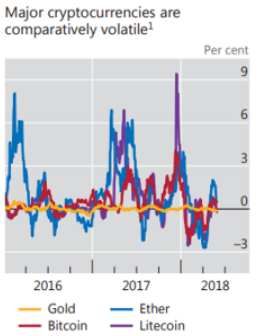
mechanism such as proof of work. Lastly, the quest for decentralized trust has quickly become an environmental disaster. As you can see, these huge energy consumptions, it is completely in contradiction with current requirements of sustainable environment and lower energy and renewable energy consumption. To summarize, in this video, we discussed that creation of trust is one of the most important aspects of decentralized permissionless blockchain-based cryptocurrencies. However, there are two very important questions. One, at what cost this trust is achieved because it requires a lot of energy consumption and even if that is there, can that trust truly be achieved at all times? In the next video, we will answer the second question.

In this video, we will conclude our discussion on limitations of cryptocurrency operations due to permissionless blockchains. Please note, the underlying economic problems with cryptocurrencies go well beyond just the energy issue and they also relate to the signature property of money that is to serve and act as coordination device for economic activity among users. The shortcomings of cryptocurrencies in this aspect lie in three areas particularly. First is scalability, second, stability of value and third, the trust in the finality of payments.

Coordination device for economic activity

The underlying economic problems also relate to the signature property of money: to serve as a coordination device for economic activity.

1. First **scalability**, cryptocurrencies simply do not scale like sovereign money: the more people use a cryptocurrency, the more cumbersome payments become. This negates an essential property of present-day money: the more people use it, the stronger the incentive to use it.
2. The second key issue- **stability of value**- with cryptocurrencies is their unstable value: This arises from the absence of a central issuer with a mandate to guarantee the currency's stability.
3. **Trust in the finality of payments**: This relates to uncertainty about the finality of individual payments, as well as trust in the value of individual cryptocurrencies.



1-Thirty-day moving averages of daily returns.

Source: www.bitinfocharts.com

Let us discuss them one by one. So first, the scalability aspect. Cryptocurrencies simply do not scale like soaring money. At the most basic level, to live up to their promise of decentralized trust, cryptocurrencies require each and every user to download and verify the history of all transactions ever made including amount paid, payer, pay and other details. With every transaction adding a few hundred bytes, the ledger grows substantially over time. Thus, to keep the ledger size and the time needed to verify all transactions with increases in block size. So to keep the time needed to verify all the transactions

manageable, cryptocurrencies have hard limits on the throughput of transactions. But the issue goes well beyond storage capacity and extends to processing capacity and that is only supercomputers could keep the verification of the incoming transactions.

The associated communication volumes could bring the internet to a halt as millions of users exchange files on the order of magnitude of a terabyte. Another aspect of the scalability issue is that updating the ledger is subject to congestion. For example, in blockchain-based cryptocurrencies, in order to limit the number of transactions added to the ledger at any given point in time, new blocks can only be added at pre-specified intervals. And once the number of incoming transactions is such that newly added blocks are already at the maximum size permitted by the protocol, the system congests and many transactions go into a queue. The capacity capped, we store whenever transaction demand reaches the capacity limit and transactions have at times remained in a queue for several hours interrupting the payment process.

This limits cryptocurrency's usefulness for day-to-day transactions such as paying for a coffee or a conferencing, not to mention the wholesale payments. And thus, the more people use a cryptocurrency, the more cumbersome payments become. This negates an essential property of present-day money, that is the more people use it, the stronger it should have an incentive to use it. The second issue is the stability of value. With cryptocurrencies, their values are unstable in nature.

This arises from the absence of central authority, central issuer with a mandate to guarantee the currency stability. Well-run central banks succeed in stabilizing the domestic value of their sovereign currency by adjusting the supply of the means of payment in line with transaction demand. They do so at high frequency, in particular during times of market stress, but also during normal times. And this contrasts with a cryptocurrency that generating some confidence in its value requires that supply be determined by a protocol.

This prevents it from being plastic. Therefore, any fluctuation in demand translates into changes in valuation. This means cryptocurrency valuations are extremely volatile. And the inherent stability is unlikely to be fully overcome by better protocols or financial engineering as exemplified by the experience of die cryptocurrency.

While engineered to be fixed to the US dollar at a rate of 1 to 1, it reached the low of 0.72 dollars, 0.72 dollars just a few weeks after its launch in 2017. Other cryptocurrencies designed to have stable value have also fluctuated substantially. And this outcome is not coincidental. So you can see their fluctuations keeping the supply of the means of payment in line with transaction demand requires a central authority of it. Typically, the central

bank which can expand or contract its balance sheet.

Now, this authority needs to be billing at times to trade against the market, even if this means taking risk onto its balance sheet and absorbing a loss. In a decentralized network of cryptocurrency users, there is no central agent with the obligation or incentives to stabilize the value of the currency. Whenever demand for the cryptocurrency decreases, so does its price. And further contributing to unstable valuation is the speed at which new cryptocurrencies all tend to be very closely substitutable with one another come into existence. Lastly, the third issue concerns the fragile foundation of the trust in cryptocurrencies and this leads to uncertainty about the finality of individual payments as well as the trust in the value of individual currencies.

So this relates to the uncertainty about the finality of individual payments as well as the trust in the value of individual cryptocurrencies. In mainstream payment systems, once an individual payment makes its way through the national payment system and ultimately through the central bank books, it cannot be revoked. In contrast, permissionless cryptocurrencies cannot guarantee the finality of individual payments. One reason is that although users can verify that a specific transaction is included in a ledger, unknown to them there can be rival versions of the ledger. This can result in a transaction rollback. For example, when two miners update the ledger almost at the same time, since only one of the two updates can ultimately survive, the finality of payments made in each ledger version is probabilistic in nature.

The lack of payment finality is exacerbated by the fact that cryptocurrencies can be manipulated by miners controlling substantial computing power. A real possibility given the concentration of mining for many cryptocurrencies. So one cannot tell if a strategic attack is underway because an attacker would reveal the false ledger only once they were sure of success. This implies that finality will always remain uncertain. For cryptocurrencies, each update of the ledger comes with an additional proof of work that an attacker would have to reach to reach.

Yet while the probability that a payment is fine and increases with the number of subsequent ledger updates, it never reaches 100%. Not only is the trust in individual payments uncertain, but the underpinning of trust in each cryptocurrency is also fragile. And this is due to forking. This is a process where a subset of cryptocurrency holders coordinate on using a few version of the ledger and protocol while others stick to the original. In this way, cryptocurrency can split into two subnetworks of users and this forking may only be a symptomatic of a fundamental shortcoming, that is the fragility of different life consensus involved in updating the ledger and with it the underlying trust in the cryptocurrency.

So to summarize, we discussed three key issues which results in fundamental underlying common problems into cryptocurrency. First is the problem of scalability, that is cryptocurrency simply do not scale like sovereign money. Second, issue of stability of value. Cryptocurrencies are sort of uncertain in their value which results or arises from the absence of a central issuer like a government with a mandate to guarantee its value and stability. And lastly, the trust in finality of payments which relates to uncertainty about the finality of individual payments as well as the trust in the value of individual cryptocurrencies.

In this video, we will make a short comparison across different parameters between the conventional fiat currencies and cryptocurrency. In the context of fiat currencies, due to their nature such as physical cash and system of operations such as banking and logistics of movement of cash in physical form, there is inconvenience in terms of transportation and logistics and storing of cash into walls and so on. However, the same aspect of transportation and logistics is much easier in case of cryptocurrency because they are purely digital. In terms of security parameter for fiat currencies, it is taken care of by the central authorities such as central bank. So central bank takes care of security through various measures.

For example, security and secrecy in the printing of money and various other security protocols for digital form of money. For example, for your banking deposits, there is a banking and payment system that ensures security. In contrast, in case of cryptocurrency, there is a cryptographic protocol which includes hash functions and this cryptographic mechanism is employed to safeguard and securitize the transaction details and any other information. The next parameter is record keeping. Here for every transaction, there is a maintenance of record in the books of some central authority. This includes the central bank like RBI in India and also when there is a transfer or some kind of transaction across deposits, then that particular bank which is taking taking care of the payment system.

So it is driven by the instructions from that authorized central party how the transactions are recorded. In contrast, in the context of cryptocurrency, the record keeping is pretty much automatic. There is no central authority and on the blockchain on which the transaction has taken place, there are nodes or users and miners and on each of these parties, each of these parties on the blockchain, they have their own ledger. This is called distributed ledger technology.

So everybody has own ledger and each of the ledger is updated automatically by the blockchain mechanism. The next aspect is counterfeiting. So in the context of fiat currency, it is feasible and sort of inevitable nuisance as every time there is a new form of

currency in different shapes and designs, there is a possibility of being counterfeited by malicious elements because this is sort of man versus man and technology versus technology kind of thing where it is there is always a challenge of counterfeiting. In case of cryptocurrencies, counterfeiting becomes next to impossible because of the cryptographic mechanism, hash functions and other security details which is automatically driven, it is next to impossible and requires huge amount of computing power and also again all the consensus mechanism and other such similar cryptographic details, they ensure that counterfeiting is impossible and more particularly the problem of double spending is not there. Next is the issue of issuance. The issuance of currency in case of fiat and conventional form is taken care of by the central authority under the given demographic and political system.

So there is a democratic and political system in conjunction with central bank, they ensure how the issuance of currency takes place. In contrast, in the case of cryptocurrency, there is a fixed set of predetermined rules that were determined at the very beginning, which ensures how supply of the currency will take place. For example, in case of Bitcoin, the maximum supply is limited as 21 million and that ensures and there are set of fixed rules and codes and algorithms that determine how the concisions will take place.

Next is the payment clearing. In case of fiat currency, the clearing is done in a centralized manner. For example, if I am transferring my money across deposits, this is done by the bank. If a bank is clearing its deposits or transacting across banks, the clearing is done at the central bank level. So, banks maintain certain reserves with the central bank. So essentially every transaction is authorized or sort of clearing mechanism is done in a centralized manner, there is an authorized central party, which sort of approves or authorizes the transaction. In contrast to this, the payment and clearing takes place through a distributed ledger technology mechanism in cryptocurrencies where there is an entire system of chain which starts in a cryptographic manner where the transaction is announced, then the miners mine the block, they solve the cryptographic puzzle successfully once a block of information is mined, successfully verified, it gets added to the blockchain and transaction is completed.

So there is a sort of endogenous mechanism, which is based on distributed ledger technology and it does not require the presence of central counterpart. Coming to the authentication part, so in terms of authentication, there is a trusted counterparty in case of fiat currency. Across every transaction, there is either the central bank, central bank like India it is RPI or if it is between two individuals through bank deposits, then the bank who is acting as intermediary act as a trusted counterparty, which does sort of things like KYC and other takes a lot of details of the depositors and whatever transaction is happening, they have this two step security mechanism, they have done your KYC, they have your

mobile number, Aadhaar card and so on. So there is a trusted counterparty on which both the parties rely.

In case of cryptocurrency, there is no such KYC mechanism. The authentication is a built-in mechanism, which is done through a cryptographic process. There are well established cryptographic protocols through which for example, we discuss the consensus mechanism and the rule of miners who sort of process the block, solve the mathematical puzzle, verify and then all the nodes on the blockchain verify the node, update the ledger and so on. So there is a built-in cryptographic protocol to authenticate any transaction. Next the problem of double spending that a money given set of coin or money or cash is not spent twice. So here in fiat currency, there is always a central authority like central bank or an intermediary between two parties.

If it is bank deposits, then it is the banking commercial bank who takes care of this authorization and verification that double spending is not there. So there is a central authority in which both the parties across both the legs of transaction, both the parties they trust. In contrast, cryptocurrency transactions takes place on a peer-to-peer network on blockchain. And this thing is resolved by the entire cryptographic mechanism as we discussed through consensus mechanism, rule of miners, solving a mathematical puzzle. And all those steps are taken to ensure that a given coin is not spent twice and there is a sort of trust and trust across parties is created through this cryptographic mechanism. Miners are incentivized through a fee to verify all the transactions and through a majority consensus more than 50%, maybe 51% or more kind of consensus is built to verify the transaction and ensure that there is no double spending or a malicious attack.

So it is sort of inbuilt cryptographic mechanism. In terms of privacy, this is a strong aspect of cryptocurrency. In fiat currency, if you are part of the banking payment and monetary system and economy, the banks will do your know your customer KYC forms and all details will be taken for you so that there is no anonymity, all your transactions back accounts will be known, all the income tax filings and everything will be there. So your identity is very well known in the system, you cannot do any fraudulent transaction or any such, even if you want to maintain anonymity for different reasons is difficult. In case of cryptocurrency, it is like pseudonymous, it is not that open only if you recall our discussions only your public key is open. So your exact real identity is hidden behind your private key, only your public key is known which is not exactly your real identity so we are calling it as pseudonymous.

So the transaction you transact through your pseudonym which is your public key and it is not so much open. So this cryptocurrency transactions give you the benefit of anonymity but there are two sides to it. Some people say that this anonymity also leads to money

funding towards terrorism and all sort of not so good activities the cryptocurrency can be used there. So it has its both sides, pro and cons for having excessive anonymity in cryptocurrency transactions. So to summarize, we compared and contrasted fiat conventional currencies and with cryptocurrencies on these parameters related to logistics and transportation, security, record keeping, counterfeiting, issuance, payment clearing, authentication, double spending and privacy.

To summarize this lesson, we noted how blockchain technology with its tamper evident and tamper resistant digital ledgers facilitates secure transactions in cryptocurrencies. We noted how modern day economies employ monetary and payment systems which are regulated by central banks. This system can be explained with the help of money flower taxonomy with the following key dimensions namely digital, widely accessible and third role of central banks and lastly peer to peer lending. In this backdrop, cryptocurrencies have emerged as a new flower following in the peer to peer digital dimensions without the intermediation of central authorities such as central banks. In the last 5 to 7 years, there has been a considerable rise of interest among the investor community about cryptocurrency assets.

This has reflected in periodic boom and bust in the market cap of major crypto assets such as bitcoin and ether. Moreover, crypto assets have been found to be extremely speculative with prices fluctuating due to attention grabbing events. For example, Elon Musk tweets, we highlighted two kinds of distributed ledgers including permissioned and permissionless cryptocurrencies. Cryptocurrencies predominantly employ permissionless blockchain models to solve the double spending problem.

A simple cryptocurrency transaction would involve the following steps. First, a user initiates the transaction and the same is announced over the network. This information is added to the block. The miners on the network rush to mine the block through proof of work or some other consensus model. The first miner to process the block gets the block in her name and the block is added to the blockchain and thus the transaction is confirmed. These cryptocurrencies come with several benefits as low transaction cost, no central authority and in turn no regulations related to transaction as would be customarily observed in the conventional fiat money. Privacy and security to transfer funds freely across jurisdictions, these are some of the important benefits.

We also discussed two major cryptocurrencies including bitcoin and ether and noted the sharp rise in prices over the years coupled with price fluctuations. We also noted that a number of countries have adopted these currencies. Also when compared with the fiat money on several parameters such as means of payment, store of value and unit of account, these cryptocurrencies have still long way to go. Moreover, the fact that these crypto assets

work on permissionless blockchain in the absence of a central authority, some extra efforts are required to generate trust. Often this trust creation process is a costly and less efficient affair than the conventional fiat money. Thank you.