Cryptocurrency

UNIT 3

Dr. S. Santhosh Kumar
Professor
School of Management Studies
Cochin University of Science and Technology
Kochi, Kerala, India
Email: drsan@cusat.ac.in

Contents of Module 3.3

- What does a cryptocurrency mean?
- What is the ideology behind it?
- How transactions are validated in a cryptocurrency network?
- How new currency creation is made?
- What is the security models used?
- How these currencies are stored?
- How does it get value? and
- What about its acceptance by governments?

Introduction

- Bitcoin came into existence in 2009
- It was founded by Satoshi Nakomoto
- Nearly 60% of the cryptocurrency market capitalization belong to Bitcoin
- All cryptocurrencies are digital currencies
- Digital currencies were proposed in early 1980s and in use since early 1990s
- The first digital currency with the features of independence, anonymity and double spending protection is Bitcoin

Fundamental value of a Currency

- The fundamental value of a currency is its acceptance as a
  - Medium of exchange
  - Store of value
  - Unit of account.

Fundamental value of Cryptocurrency

- If you price your products and services in cryptocurrencies like Bitcoin, you will be put in trouble.
- The trading prices of these currencies are fast shooting up and falling down. So the commodities that track crypto currencies are likely to reflect the same volatility.
- The extreme volatility could be a sign of purchasing them for the purpose of gambling. These gamblers may be expecting that the fundamental value of cryptocurrencies as a medium of exchange will increase significantly in future.
- Moreover the anonymity ensured by cryptocurrencies for the transactions taking place with those currencies also worsens the situation.
- These might be the justifications for the current volatility of Bitcoin and other cryptocurrencies.

Ideology of Bitcoin

- **The ideology of Nakamoto was to have a monetary system without borders, regulation and limitation.**
- **Nakomoto's lack of trust in Fiat currencies and centralized banking system led to the creation of bitcoin**
- **Nakamoto was intending a complete system of production, distribution and management of currency without the involvement of a central authority**
- **This was made possible by him through the Blockchain technology**
- **Through blockchain technology, Nakomoto ensured anonymity in transactions, independence by peer to peer management and also double spending attack protection.**
- **Remember, the very ideology of bitcoin may be to dismantle the central banking system all over the world**

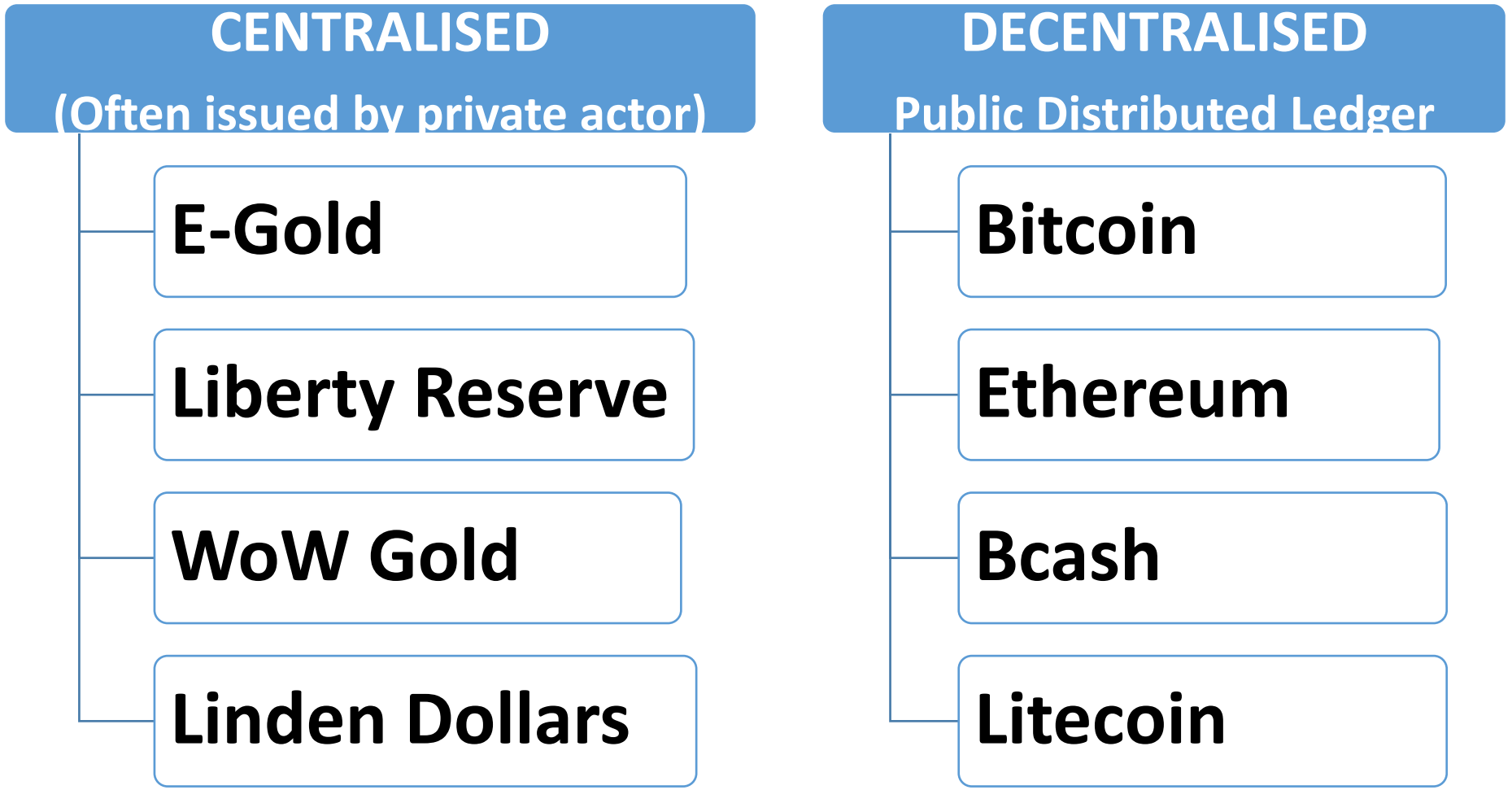
Electronic money

- Electronic money is the money which exists in banking computer systems and is available for transactions through electronic systems.
- Its value is backed by fiat currencies like US Dollar or Indian Rupees.
- It can be exchanged into physical form. However its uses are often more convenient electronically.
- For example, in my mobile I have my bank's mobile App which displays my account details and my fiat currency holding. I can use it for payments, transfer and withdraw in the form of Fiat currency from different outlets.
- In short, electronic money is the digital equivalent of your Fiat currency holding.

Electronic money Vs Digital currency

- Fiat currencies like US Dollar or Indian Rupees are issued in physical form.
- However, digital currencies are issued electronically and not in physical form.
- Like fiat currencies, digital currencies can also be used for payments and transfer if accepted by the other party.
- However, transferability into fiat currency is not guaranteed by any State.
- Digital currencies may be centralized or decentralized.
- They are centralised in the sense that there will be somebody to control and mange the system.
- But decentralized digital currencies may not have any central authority as they are designed to function as a peer to peer managed one.

Digital Currency



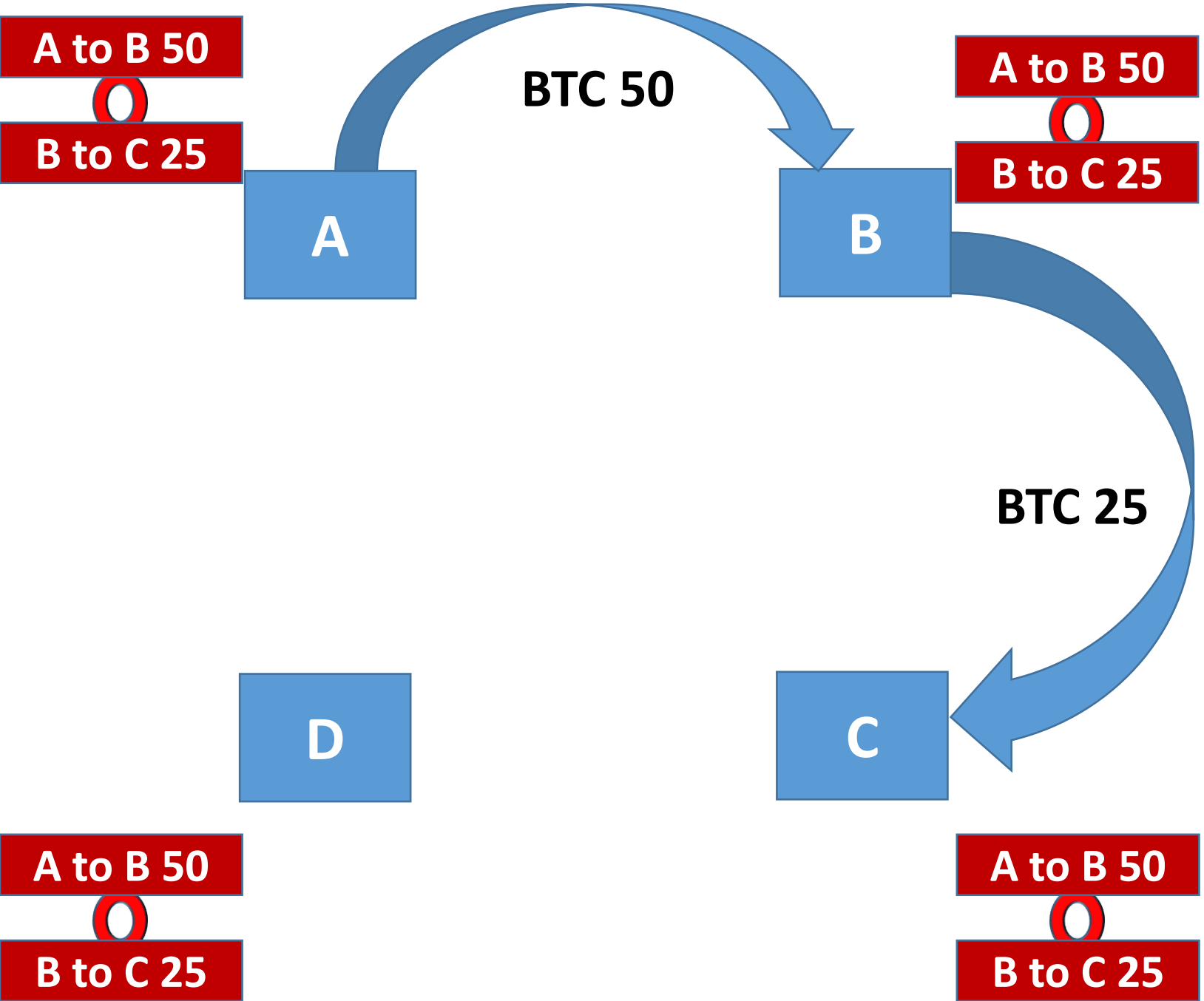
Cryptocurrency

- Cryptocurrency is a digital currency.
- Unlike fiat currencies such as dollar, pound sterling or Japanese Yen, it is not printed.
- It means that it is issued in digital form.
- The security model for new currency creation and validation of transactions in the system are through the science of cryptography.
- The transaction details, the identity of the persons involved and every other relevant information are kept in the system using cryptography.

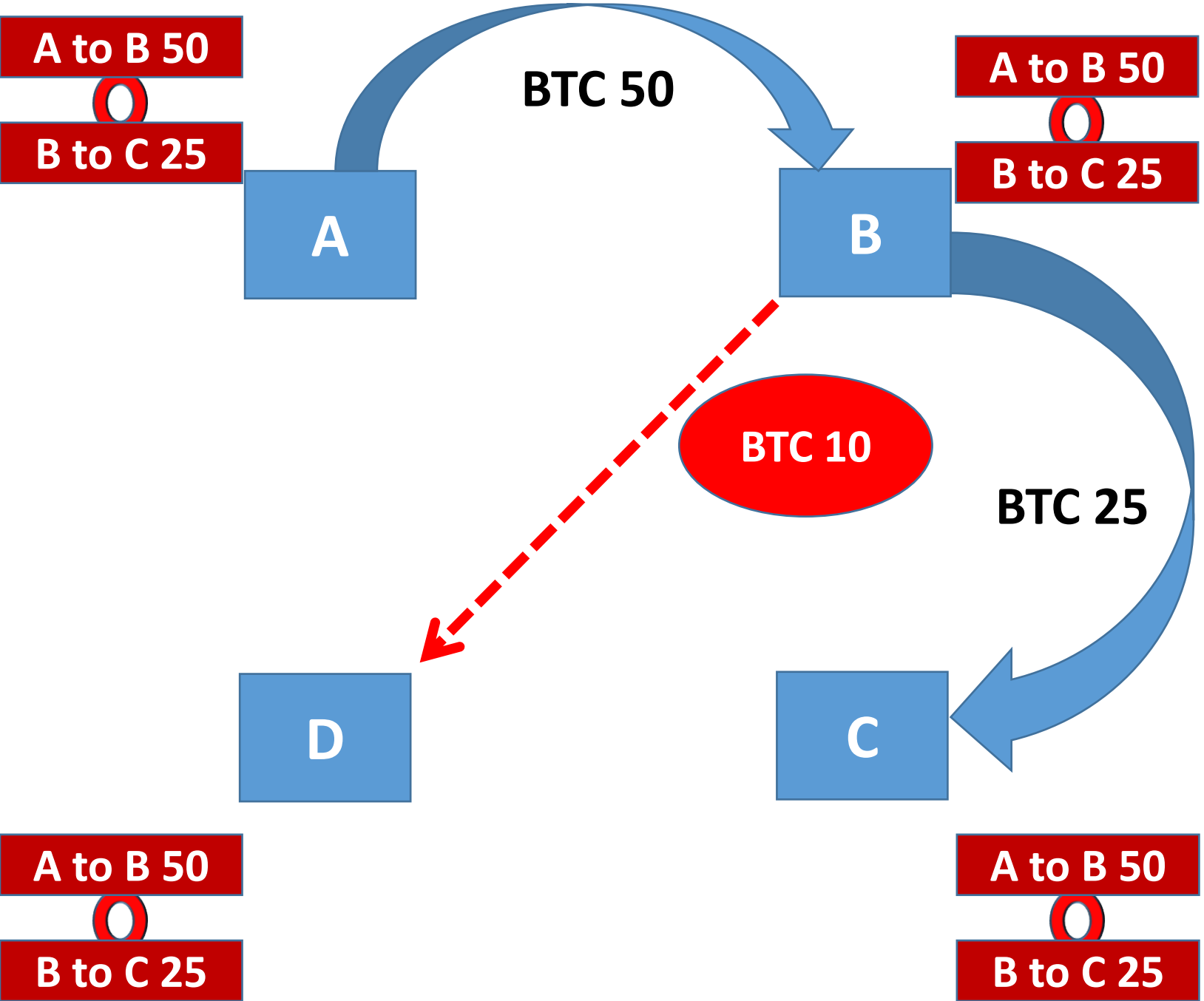
Cryptocurrency…….

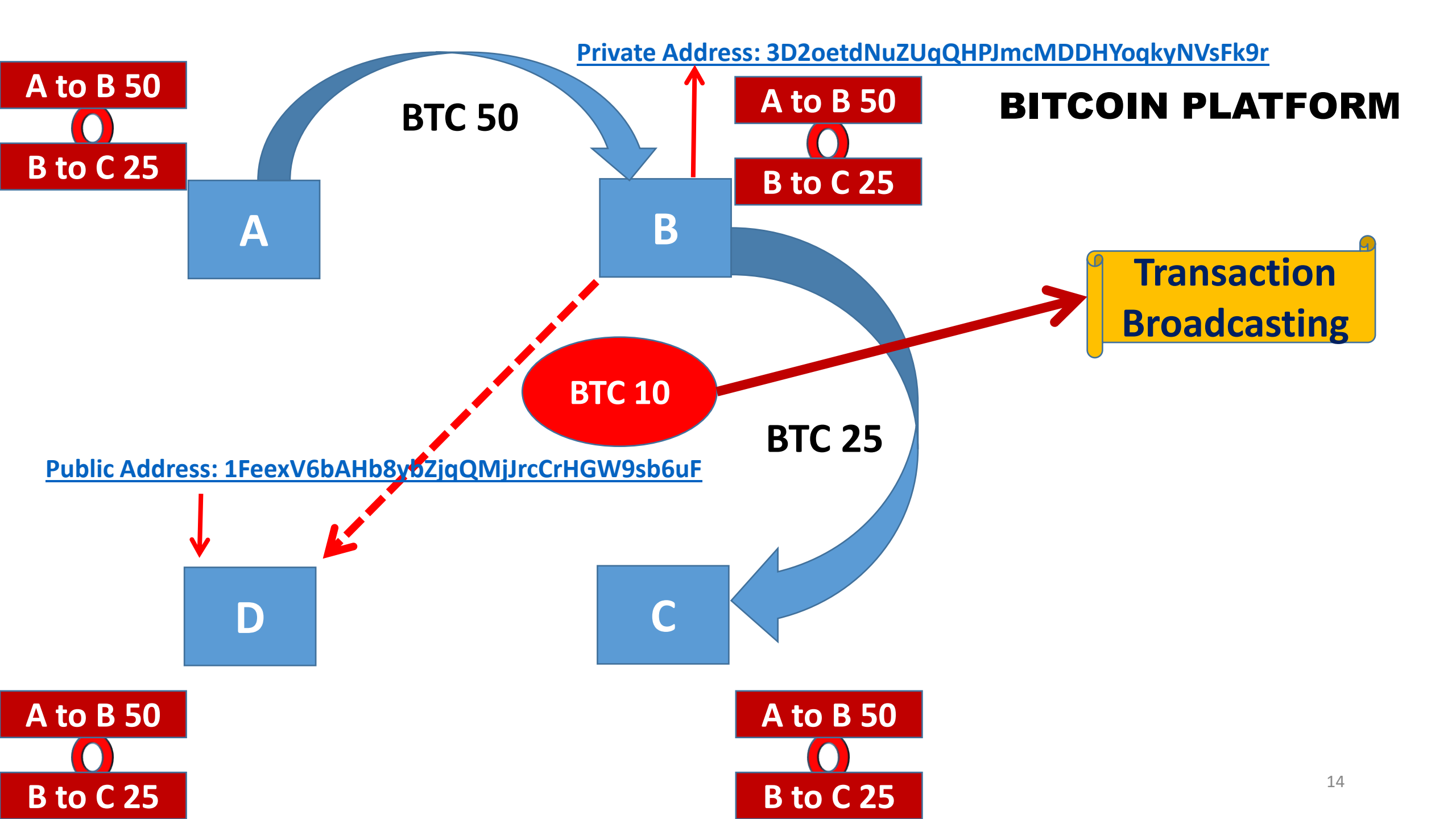
- Jan Lansky, an active researcher and writer in cryptocurrency has given six requirements for considering a particular currency as cryptocurrency.
  - One is that the currency system does not require a central authority.
  - Secondly, the system keeps an overview of cryptocurrency units and their ownership.
  - The third requirement is that the system defines whether new cryptocurrency units can be created, defines the circumstances of their origin and how to determine the ownership of these new units.
  - The fourth requirement is that the ownership of cryptocurrency units must be proved exclusively using cryptography.
  - The fifth one is that the system must allow the owners of cryptocurrency units to frequently change their identity which is maintained in the system using cryptography.
  - And finally, if two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

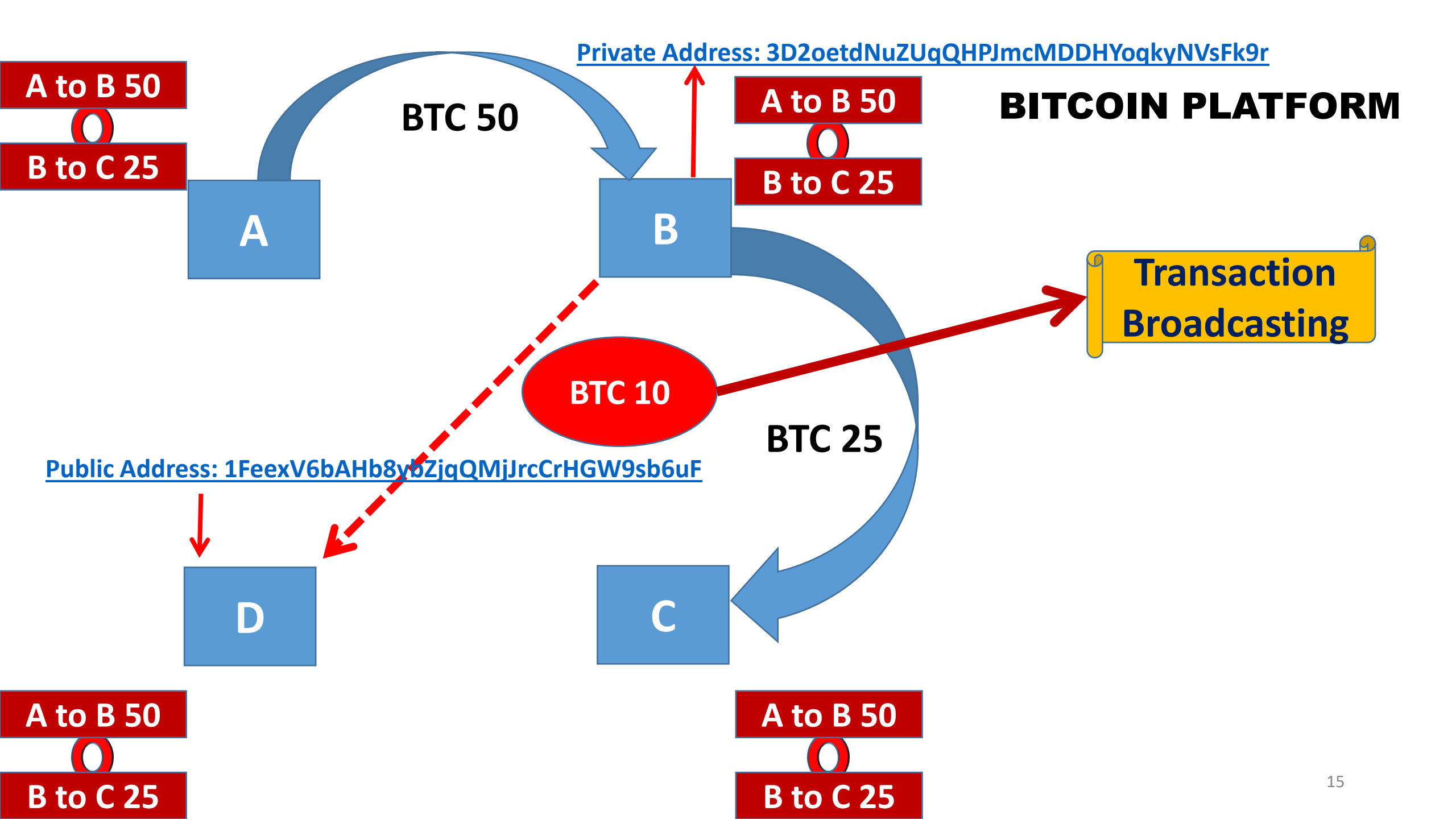
BITCOIN PLATFORM

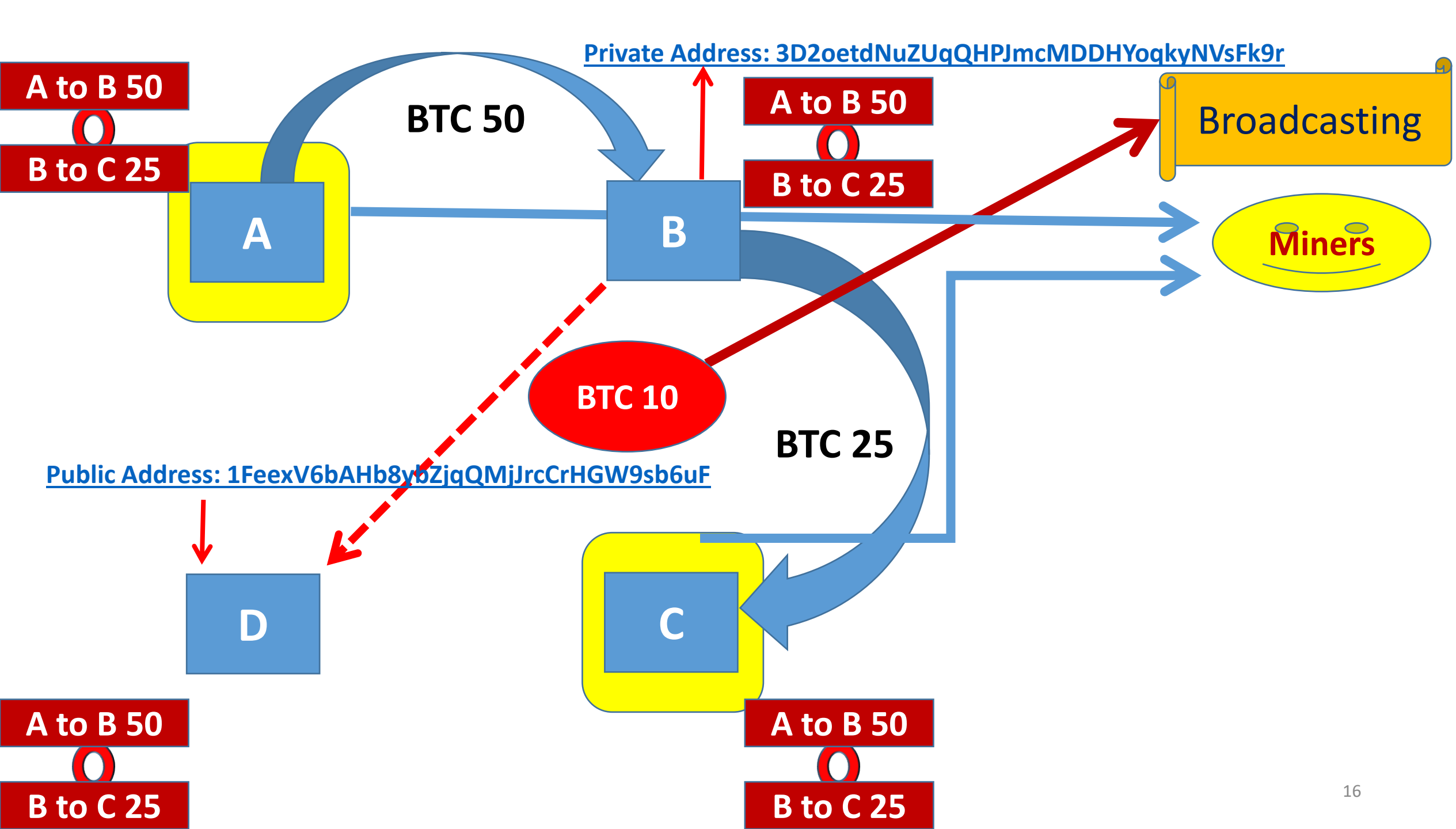


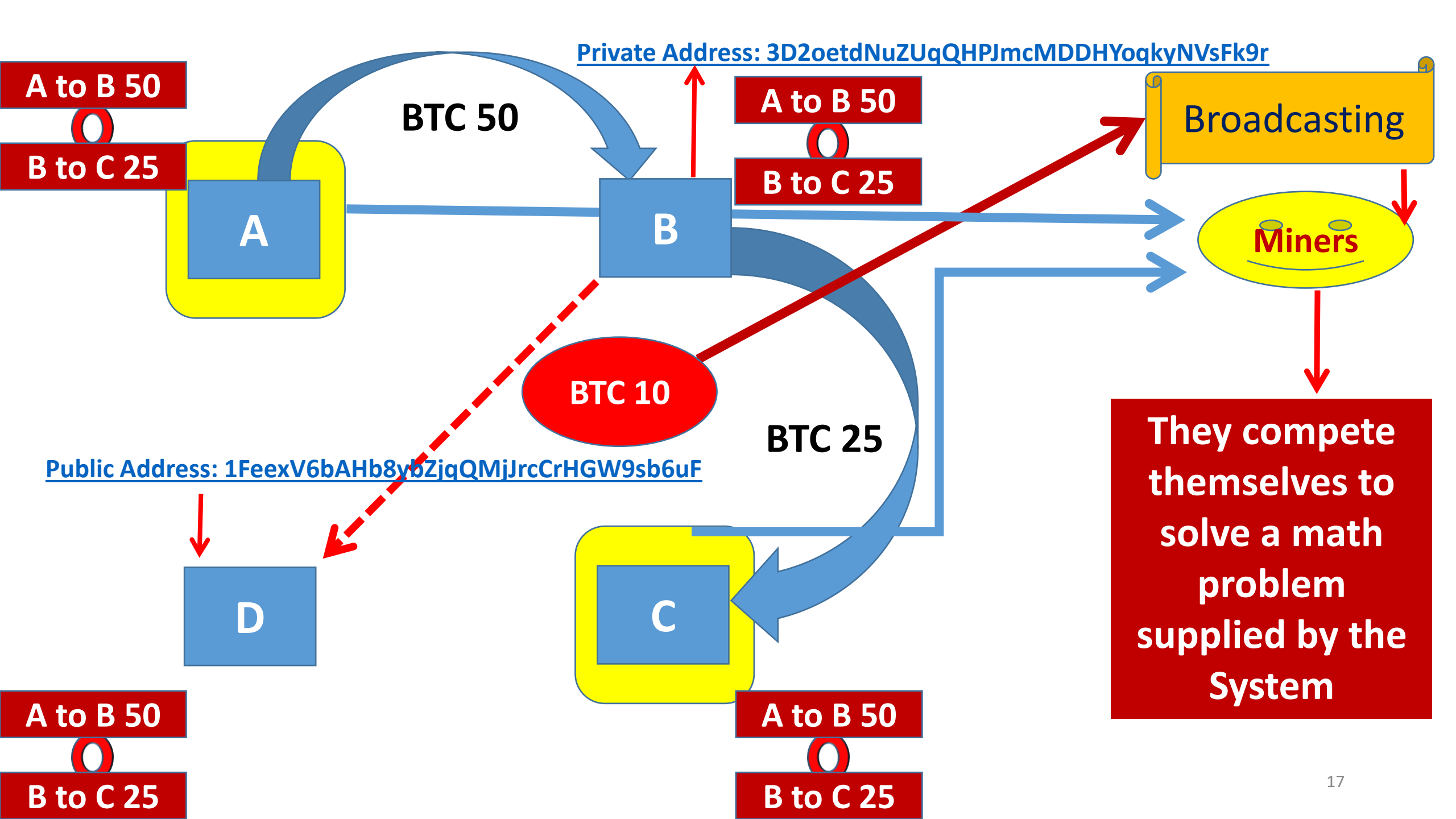
BITCOIN PLATFORM

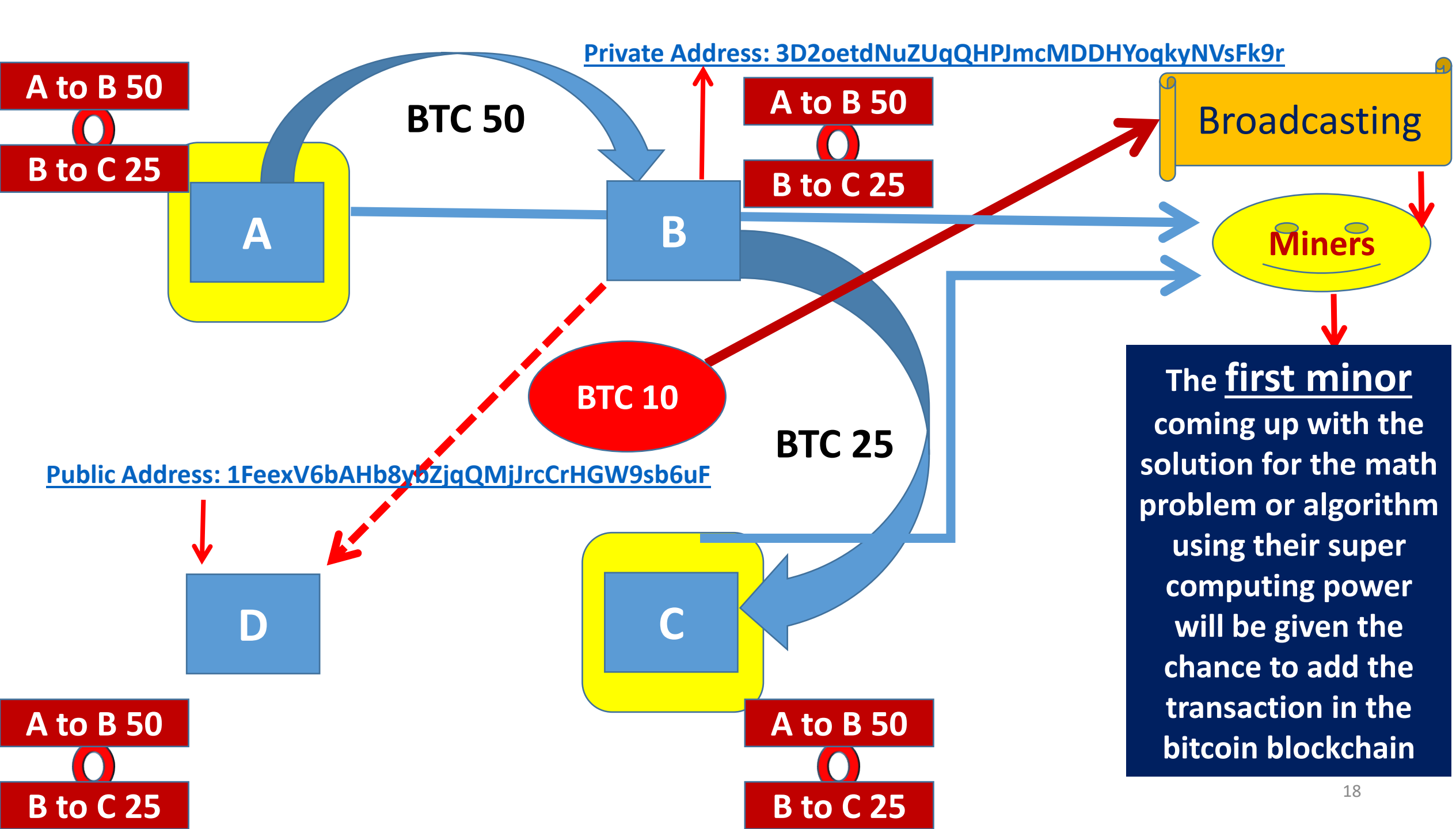


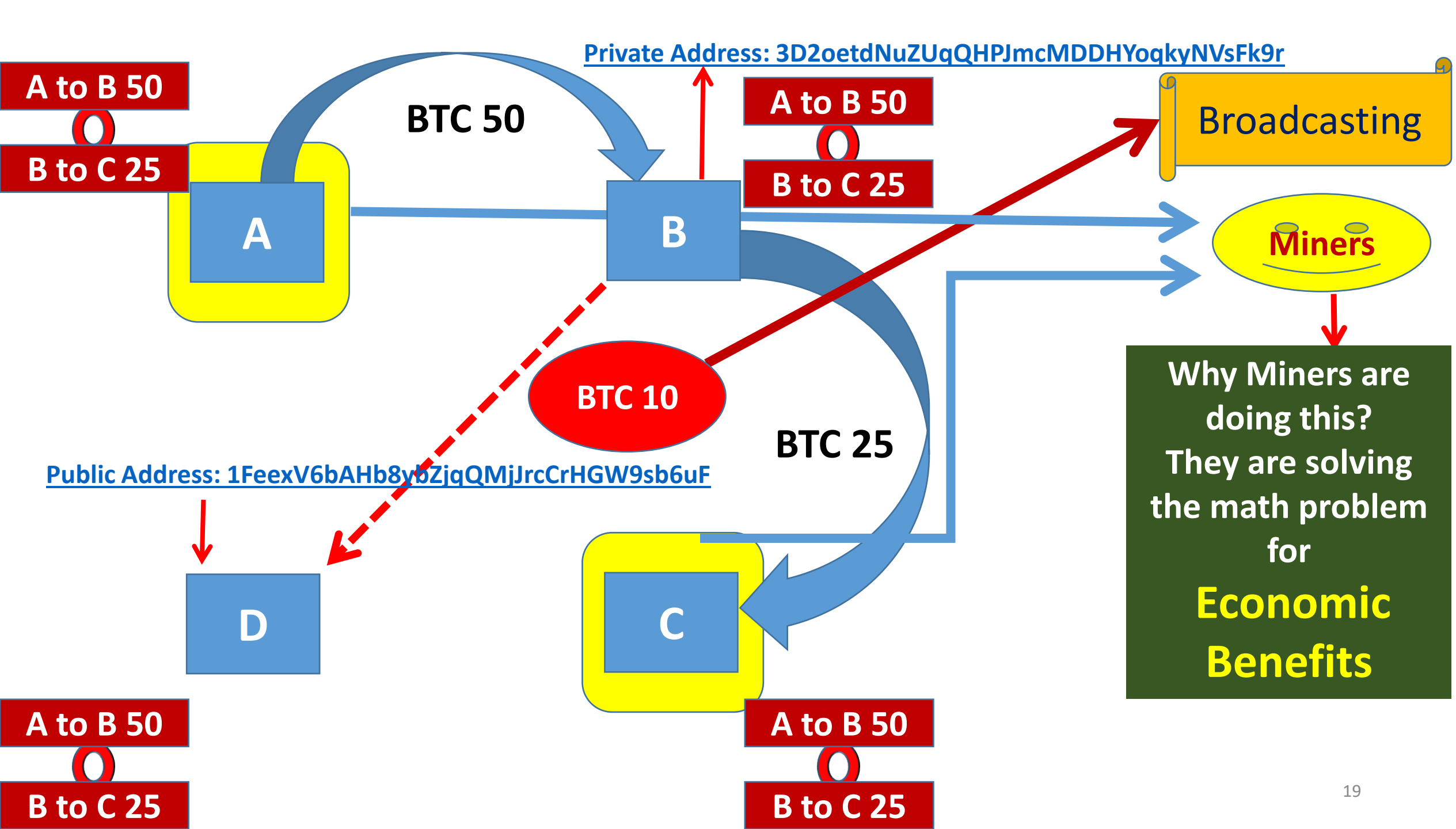

Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
BITCOIN PLATFORM
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Transaction Broadcasting
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
A to B 50
B to C 25
A to B 50
B to C 25

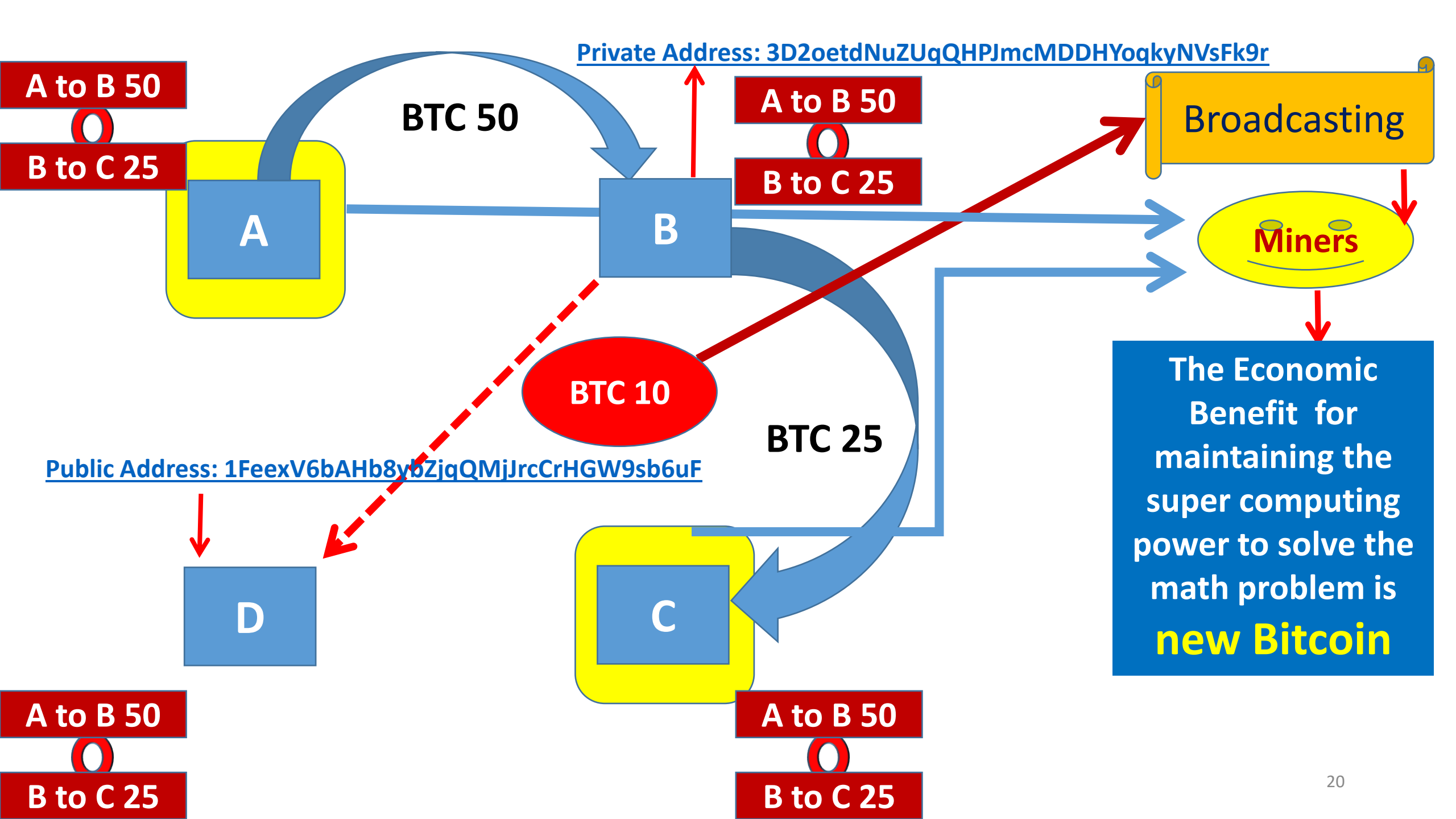

Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
BITCOIN PLATFORM
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Transaction Broadcasting
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
A to B 50
B to C 25
A to B 50
B to C 25

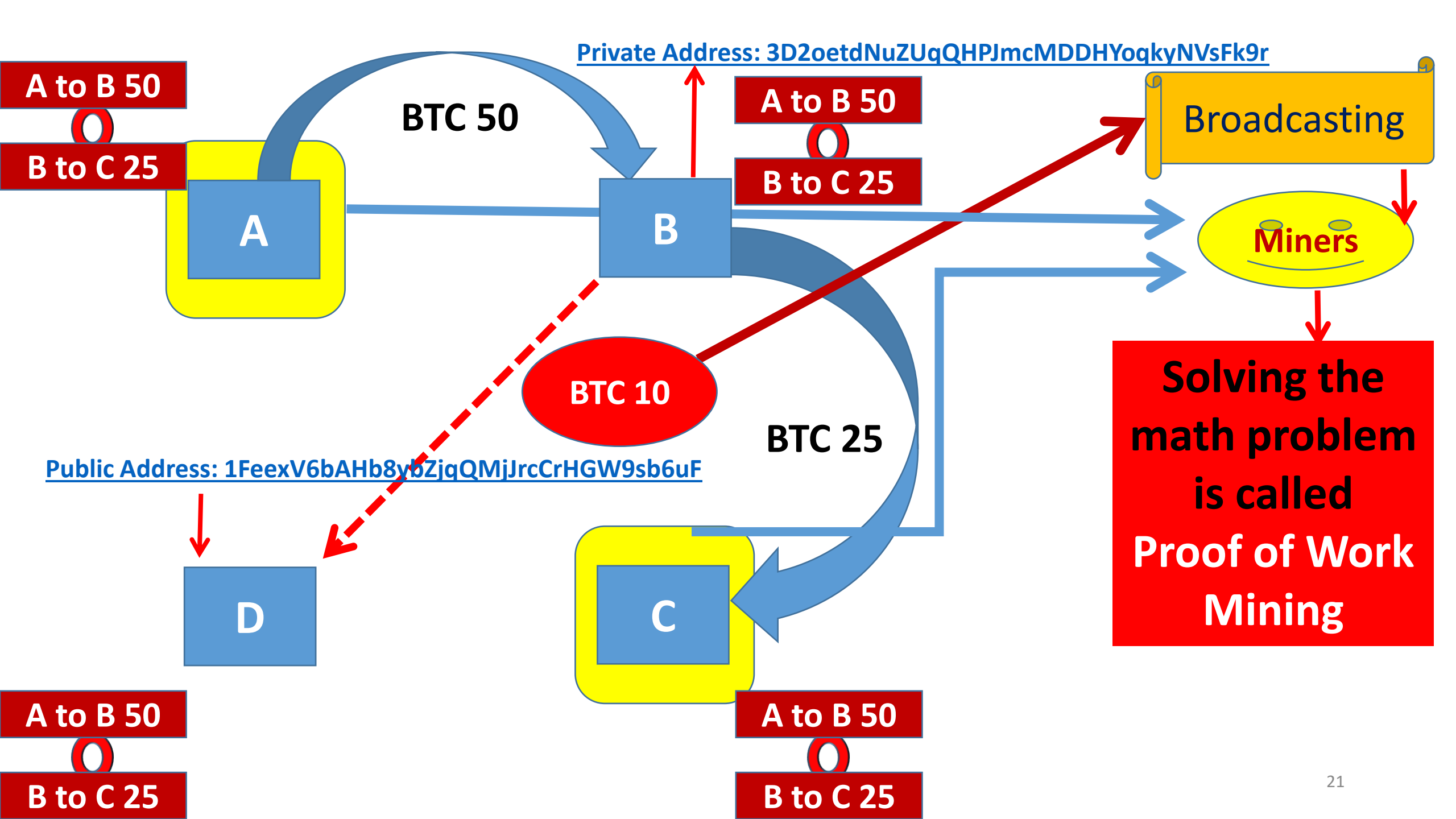

Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
A to B 50
B to C 25
A to B 50
B to C 25

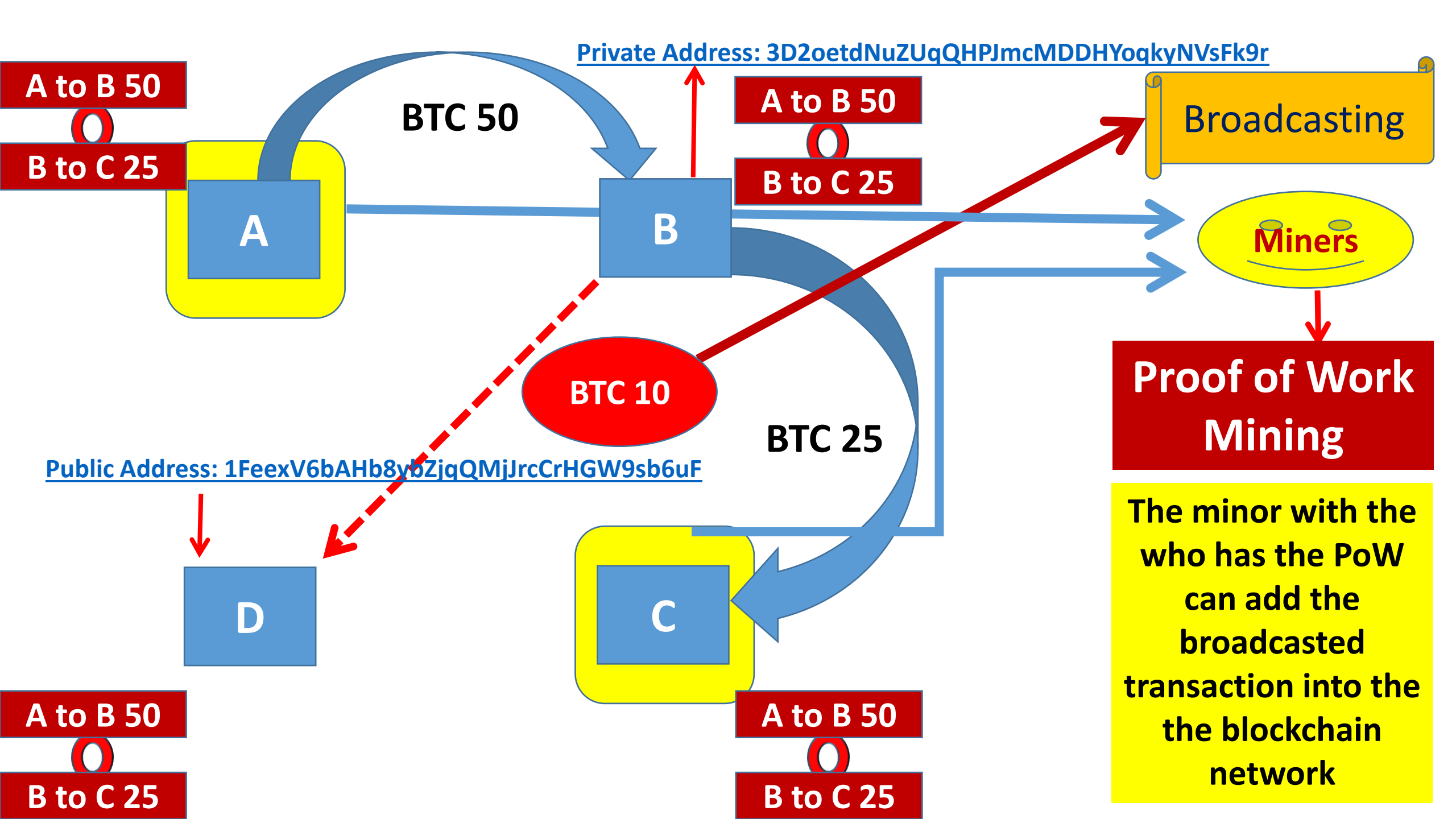

Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
They compete themselves to solve a math problem supplied by the System
A to B 50
B to C 25
A to B 50
B to C 25

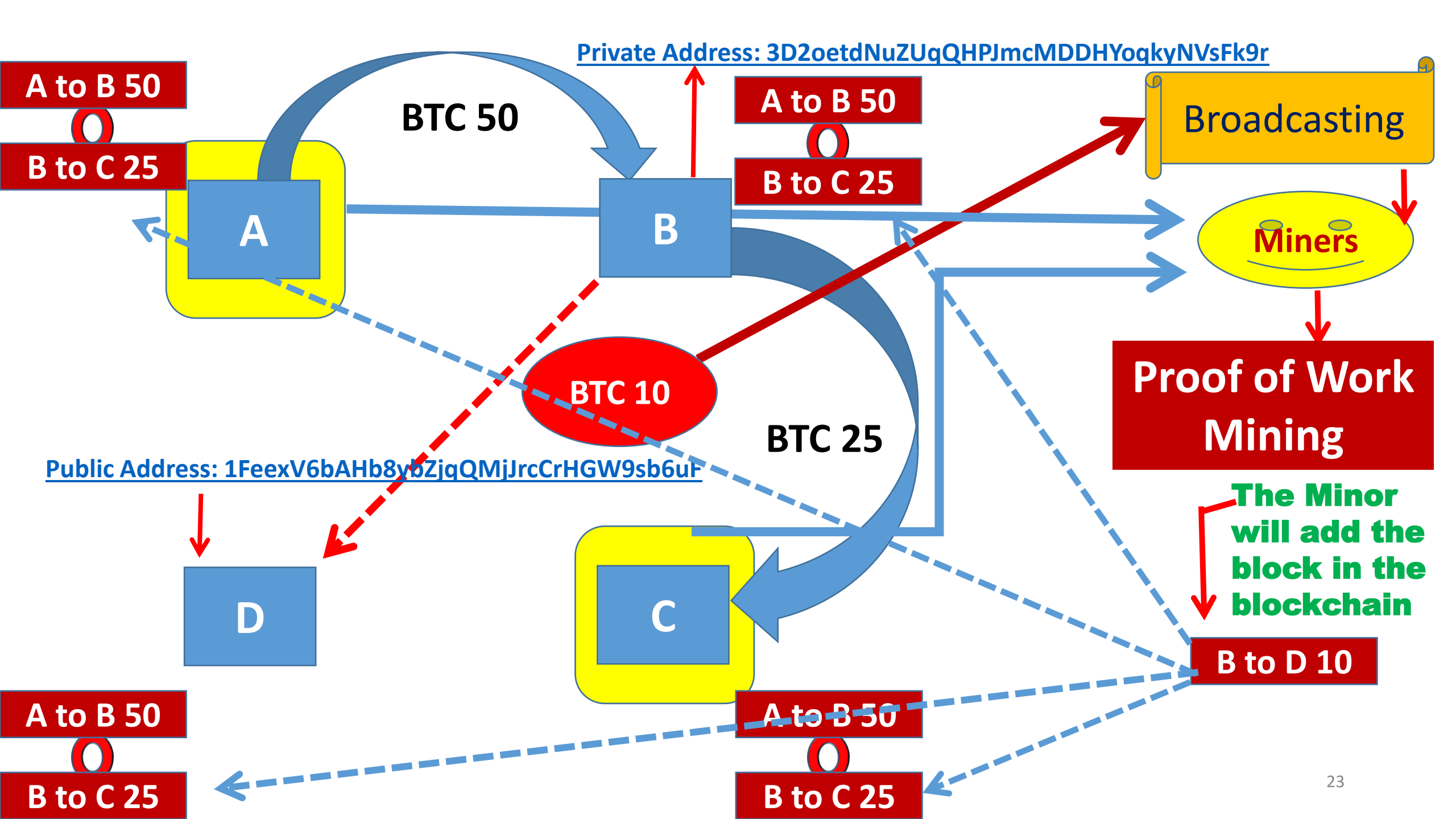

Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
A to B 50
B to C 25
A to B 50
B to C 25
The first minor coming up with the solution for the math problem or algorithm using their super computing power will be given the chance to add the transaction in the bitcoin blockchain


Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
Why Miners are doing this?
They are solving the math problem for
Economic Benefits
A to B 50
B to C 25
A to B 50
B to C 25


Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
The Economic Benefit for maintaining the super computing power to solve the math problem is
new Bitcoin
A to B 50
B to C 25
A to B 50
B to C 25


Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
Solving the math problem is called Proof of Work Mining
A to B 50
B to C 25
A to B 50
B to C 25


Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
Proof of Work Mining
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
A to B 50
B to C 25
A to B 50
B to C 25
The minor with the who has the PoW can add the broadcasted transaction into the the blockchain network


Private Address: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
A to B 50
B to C 25
BTC 50
A
B
A to B 50
B to C 25
Broadcasting
Miners
Proof of Work
Mining
BTC 10
BTC 25
Public Address: 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
D
C
The Minor will add the block in the blockchain
B to D 10
A to B 50
B to C 25
A to B 50
B to C 25

Miners and Transaction Validation

- Miners are computer nodes in the network with super computing power
- The minors will compete to solve a system generated cryptographic puzzle to get a turn to add a transaction block into the bitcoin blockchain.
- The first miner solving the cryptographic puzzle or math problem will get the turn.
- So, whenever a transaction is broadcasted in the bitcoin network, the miners themselves will engage in a competition to solve the puzzle to get a turn for transaction validation.
- This is done by them for getting some economic benefit or reward.
- The reward for miners in the bitcoin network is **Bitcoin.**

Proof of Work Mining

- The process of solving the crypto puzzle or math problem is called Proof of Work Mining.
- A very important point to be noted here is that new bitcoin coins are created in the bitcoin network only through proof of work mining.
- So Bitcoin mining has a two-fold purpose. It allows for the creation of new coins and facilitates the processing of transactions in the network.
- To become a Bitcoin miner, a person first needs a computer and mining software. Moreover, the person must be part of the bitcoin network with a digital wallet.

What is wrong with Mining?

- Mining can be a very lucrative job.
- However, the non-stop attempts by miners for solving the puzzles by constantly running their computers require loads of electricity.
- Moreover, the cost of mining hardware is very high.
- So, proof of work mining is very expensive, labour intensive and environmentally unfriendly.
- The heavy use of electricity for mining makes the process environmentally unfriendly.

Faucets and free bitcoin

- Can you get bitcoin or other crypto free of cost?
- Yes, you can. Faucets will give you free crypto.
- Faucets are very popular in cryptoverse.
- Faucets are a way to earn free cryptos like bitcoin simply by visiting the faucet websites.
- Faucets are allowing you to get your feet wet.
- You visit a faucet website, fill in a captcha and earn satoshis the smallest unit of bitcoin or some other cryptocurrencies.

Wallets

- A cryptocurrency wallet is a secure digital wallet used to store, send, and receive digital currencies like Bitcoin.
- Wallets are softwares which can be used to view cryptocurrency balances and make transactions.
- A wallet has a public address. Public addresses are like cryptocurrency-specific account numbers just like your bank account numbers. They can be used to receive a specific type of cryptocurrency.
- Similarly, each wallet will have a cryptographic private address. You can view crypto balances in a wallet and move funds in a wallet using your private key. It is same as your bank account pin which is not disclosed to others.
- In short, Private address is your ownership proof. If your private key or address is lost everything in the wallet may loose. As the name implies, you can share your public address publicly. However, sharing your private keys and passwords are risky.

Types of Wallets

- Wallets are of different types. They are;
  - Online wallets,
  - Desktop wallets,
  - Mobile wallets, and
  - Hardware wallets.
- Wallet services are usually offered by the crypto exchanges and the promoters of different coins.

How to buy and sell?

- You can buy or sell cryptos through cryptocurrency exchanges.
- This means that you need to create an exchange account and store the cryptocurrency in your digital wallet.
- The cryptocurrency exchanges serves as intermediaries to buy cryptocurrencies against your fiat currencies and also to sell your cryptocurrencies for fiat currencies.
- People do buy cryptocurrencies as an investment or trade in it to book price difference.
- Speculators also tend to create price booms for making gains.

How does it get value?

- Everybody is suspicious about its intrinsic value? It is simple to explain.
- Somebody is ready buy bitcoin at a price somebody is ready to sell. That is all.
- Moreover, by the very structure of bitcoin, its supply is limited.
- The total Bitcoin that can be mined is 21 Million. Almost 70% have been mined. So it is scarce in nature.
- There are many business and non-business entities all over the world that are receiving and paying for goods and services using cryptocurrencies.
- Moreover, there are speculators who are ready to pay for its current price believing that Bitcoin and other cryptocurrencies have some fundamental value as money.
- These are the sources of demand and supply for cryptocurrencies which make their pricing.

Risk of Cryptocurrencies

- European Banking Authority has defined the associated risks.
- One of the risks pointed out by the European Banking authority is the Low Market Capitalisation of cryptocurrencies.
- There are limited numbers of users in cryptocurrency networks and therefore the market capitalization is low.
- Any one user’s trade has a disproportionate impact on market price. Hence, exchange rates of cryptocurrencies against fiat currencies change quickly.
- This volatility offers scope for the operation of speculators.

Risk of Cryptocurrencies……

- **Private Key knowledge is equal to ownership. If the private key of your wallet is known to anyone other than you, it is total risk for you. You can’t stop that person stealing your coins.**
- **The Transaction Irreversibility or immutability feature of cryptocurrencies is also posed as a risk. If you sent some coins by mistake to another party in the network, it cannot be reversed.**
- **Anonymity of the Accounts in the network is another risk. Everybody in the network is known by their cryptographic public address. This pseudo anonymity may give opportunity for money laundering, terrorist funding, illicit trafficking and so on. These are some of the several risks of the cryptocurrencies.**

Future of Cryptocurrencies

- There are two thousand plus crypto currencies across the world.
- One thing is sure; the international acceptance of cryptocurrencies is increasing.
- the cryptocurrencies are claimed to be currency system which can dismantle the existing central banking system all over the world.
- This is the political risk faced by cryptocurrencies for their long-term survival.
- Therefore, the consequences are unlikely to workout in favour of cryptocurrencies.
- It is hard to believe that the Governments voluntarily allow market-based currencies like Bitcoin to out-compete their own Fiat currencies.
- India has not banned cryptocurrencies so far. However, a banking ban is existing in the country in the sense that RBI has blocked transfer money from your bank accounts to the bank accounts of cryptocurrency exchanges and vice versa.
- This blockade has considerably reduced the transaction turnover of crypto exchanges in India.


Thank You