

CREATING
RISK
INTELLIGENT
PROFESSIONALS



GRMI

**GLOBAL RISK
MANAGEMENT
INSTITUTE**

Cryptocurrency Exchange Platform | Chhavi Goel

PROGRAMME
ENDORSED BY



ASSOCIATE
PARTNER



STRATEGIC
PARTNER



ASSOCIATE
MEMBER



STRATEGIC
PARTNER



What is Cryptocurrency?



- A cryptocurrency is a form of payment that can circulate without the need for a central monetary authority such as a government or bank.
- Cryptocurrencies are created using cryptographic techniques that enable people to buy, sell or trade them securely.
- These can be exchanged for goods and services, though they often are used as investment vehicles.
- Cryptocurrencies use block chain technology.

Related Terms

- **BLOCK**

Every block in a blockchain contains 4 components: a timestamp, a reference to the previous block, a summary of the included transaction and the Proof of Work that went into creating the secure block.

- **NODES**

Nodes are distributed computers in the network that all have a copy of the entire blockchain. The data is not controlled by a singular node or network.

- **NETWORK CONSENSUS**

A blockchain is always stored on multiple computers across a network. It also uses consensus algorithms to establish agreement regarding which blocks are to be added to the chain and which nodes are valid.

- **CRYPTOGRAPHY**

Blocks are linked together by cryptography – complex mathematics and computer science. Any attempt to alter data disrupts the cryptographic links between blocks, and can quickly be identified as fraudulent by computers in the network.

▪ **PRIVATE KEY**

In Private key, the secret key is used for encryption and decryption. A private key can be used to decrypt a message that is symmetrically encrypted using the corresponding public key. Private keys are kept secret from anyone that isn't the owner. Once a private key is made public, it is useless as a point of authentication.

▪ **PUBLIC KEY**

In Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message.

▪ **MINING**

Mining means adding transaction records to the blockchain ledger after confirming the validity of the transactions. It involves using complex hardware to perform mathematical calculations in order to verify transactions. Once a new hash is created for every secure block, miners are rewarded with incentives like bitcoins and collecting transaction fees for every transaction that they confirm.

▪ **PEER-TO-PEER (P2P)**

Interactions between traders without a central intermediary. P2P networks allow each peer to connect directly to all other peers in the network.

▪ **SMART CONTRACT**

A smart contract is a digital agreement stored on the blockchain that is unalterable, once signed. It defines certain logic operations that have to be fulfilled in order to perform tasks such as deposit money or data.

Smart contracts in blockchains are particularly useful because anyone who processes a function in a smart contract will get the same output as anyone else performing the same function.

▪ **PROOF-OF-WORK (POW)**

A consensus mechanism or a process in which actors race to solve a computationally difficult problem in order to win the ability to produce the next block in a blockchain.

Proof-of-Work's security is rooted in the computational difficulty of the algorithm.

Because it is an essentially random process to find a solution, the probability of solving the problem is related to the actor's processing speed and the acceptance criteria for the solution (the difficulty). Stricter acceptance criteria reduce the speed at which the network finds a solution, and varying the acceptance criteria can allow a network to control the solution rate.

What is a Blockchain?

A blockchain is a decentralized ledger of recorded data.

This is basically the transaction history for every unit of the cryptocurrency, which shows how ownership has changed over time.

This works by recording transactions in 'blocks', with new blocks added at the front of the chain while the oldest lives at the bottom, known as the 'genesis block'.

Each block contains 'hash' of the previous block, linking them together in a chain.

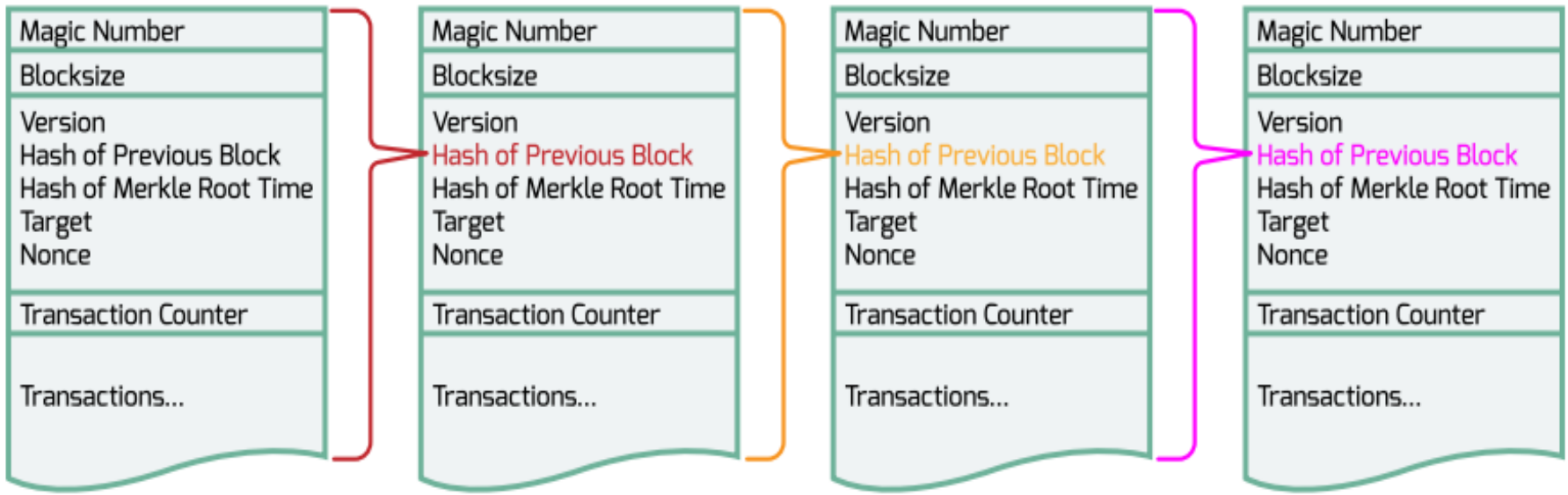
The technology offers a secure way for individuals to deal directly with each other, without an intermediary like a government, bank or other third party.

Each transaction is independently verified by peer-to-peer computer networks, time-stamped and added to a growing chain of data. Once recorded, the data becomes permanent.

The technology cryptographically chains blocks in chronological order, and allows the resulting ledger to be accessed by different servers.

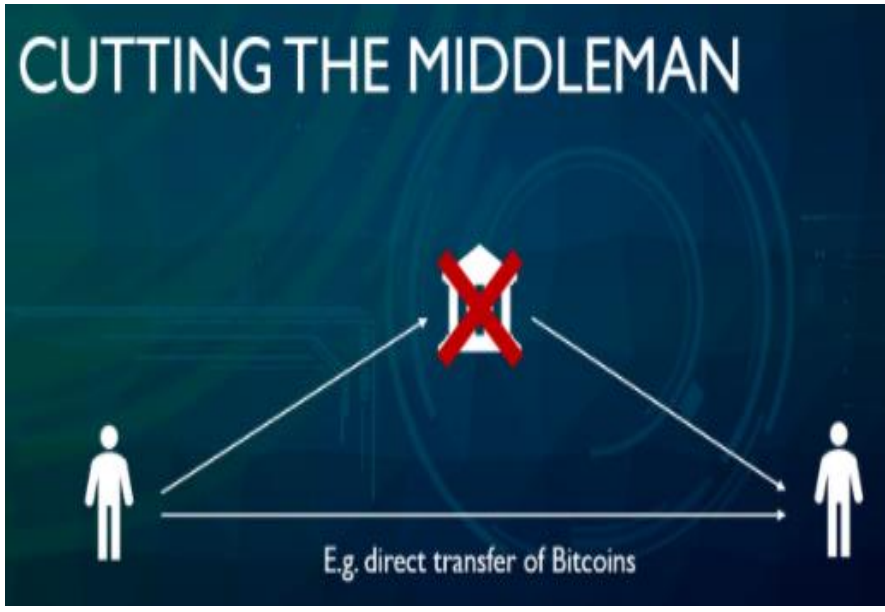
It is maintained by a network of computers in a way that makes it difficult to hack or alter.

What makes it unique is that there is no central authority in charge of the blockchain file or the data it contains.

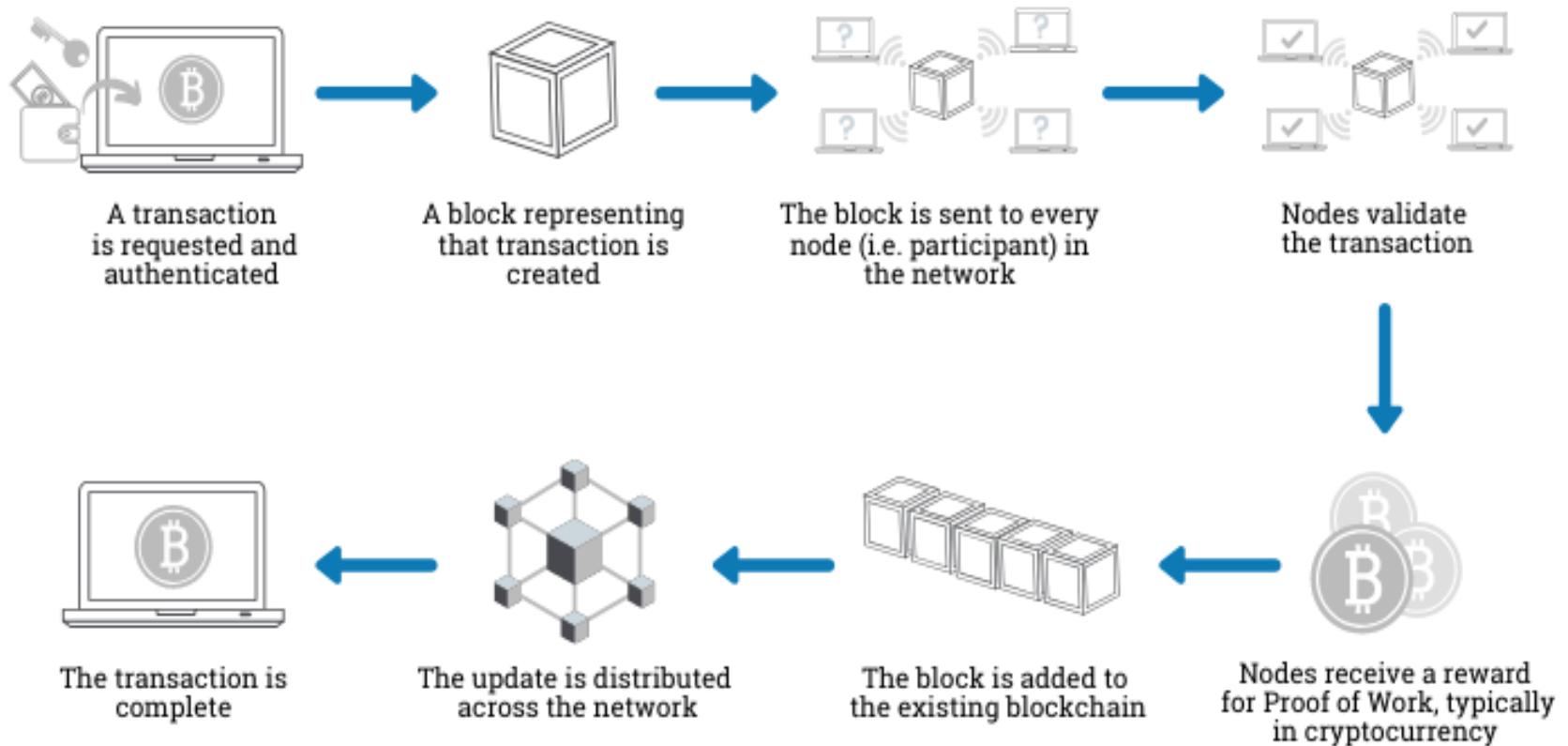


GENESIS BLOCK

LATEST BLOCK



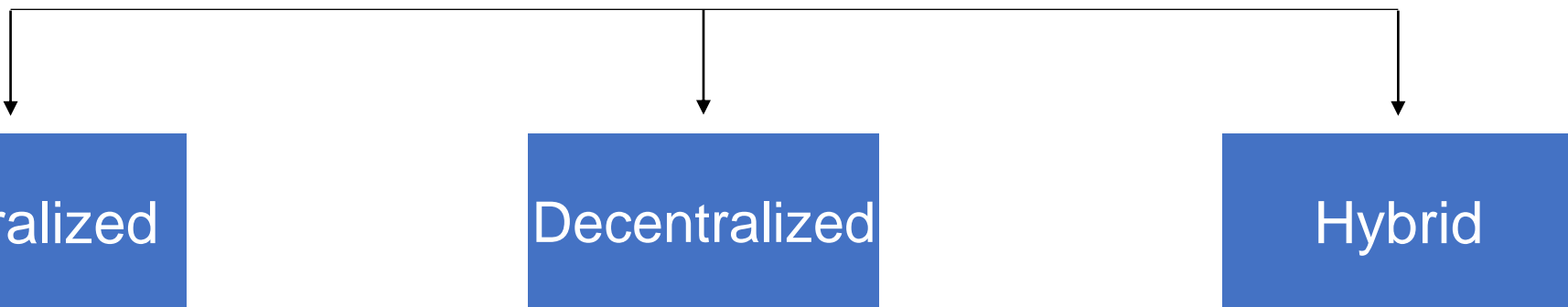
How does a transaction get into the blockchain?



© Euromoney Learning 2020

Cryptocurrency Exchange Platforms

- Crypto Exchange Platforms facilitate cryptocurrency trading in exchange for digital and fiat currencies. They act as an intermediary between a buyer and a seller.
- There are various approaches to the crypto-exchange business. Some exchanges focus on ease for the customer, others offer low trading fees, some try to educate their customers from the very beginning, and on the other hand, there exist those who are oriented on the professional traders.
- Broadly, there are three types of exchange platforms:



Features

- It allows a buyer to deposit money using several methods like direct bank transfer, UPI, using debit or credit cards, etc.
- It charges a set commission or fee for every transaction done using its services.
- Depending on the exchange, one can purchase crypto using a fiat currency like the U.S. dollar, or trade one form of crypto for another, for example converting Bitcoin to Litecoin.
- Trader may be able to convert their crypto back into regular currency, leave it in their account for future trades, or withdraw it as cash.
- Available services can vary, depending on the exchange that is used. For example, some services don't allow traders to move their crypto off platform to their own crypto wallet.
- Unlike traditional exchanges that have set trading hours, cryptocurrency exchanges are active 24 hours a day, 7 days a week.

Centralized Cryptocurrency Exchange

- The concept of centralization refers to the use of a middle man or a third party to assist within transactions in a secure manner.
- Both buyers and sellers trust the middle man to handle their properties.
- The centralized exchanges require their users to verify their personal information before using the tools provided by them. The levels of verification may vary from exchange to exchange. These KYC checks are in order to ensure that crypto businesses comply with anti-money laundering measures.
- Approximately 99% of all crypto transactions go through centralized exchanges.
- Examples:



Advantages and Disadvantages of Centralized Crypto Exchange

ADVANTAGES

 User-friendly

 Secure funds

 Reliable

DISADVANTAGES

 Hacking risks

 Transaction fees

Decentralized Cryptocurrency Exchange

- This type of exchange allow users to execute peer-to-peer transactions without the need for a third party or an intermediary.
- Decentralized exchanges do not store users' funds on the exchange rather they are stored on the blockchain.
- These exchanges do not facilitate the trading of fiat currencies for cryptocurrencies.
- In such exchanges the transactions and trades are automated by using smart contracts. There is no possibility of a security breach if the smart contract is well written of course.
- Because no company is responsible for the run of DEX, it's harder for governments and regulators to shut them down.
- Examples:



Advantages and Disadvantages of Decentralized Crypto Exchange

ADVANTAGES



Mitigating hacking risk



Anonymity



Preventing market manipulation

DISADVANTAGES



Complexity



No customer support



Lack of fiat payment



Liquidity Struggles

Hybrid Cryptocurrency Exchange

- Hybrid cryptocurrency exchanges are an attempt to blend the best of both worlds from centralized and decentralized into one exchange.
- Their aim is to give end users the convenience of a centralized exchange while also giving them the security and freedom of a decentralized exchange.
- They allow users custody of their funds even if a third party is involved in the trading.
- Hybrid types are a new generation of the crypto trading marketplace, but still “under development”.
- Examples:

The logo for Nash, featuring a blue equals sign followed by the word "nash" in a bold, lowercase, blue sans-serif font.

The logo for Qurrex, featuring a red hexagonal icon with a white and red geometric pattern inside, followed by the word "qurrex" in a bold, lowercase, blue sans-serif font.

How to trade on a Crypto Exchange?

To begin trading, one needs to fund their exchange account — sometimes called a wallet.

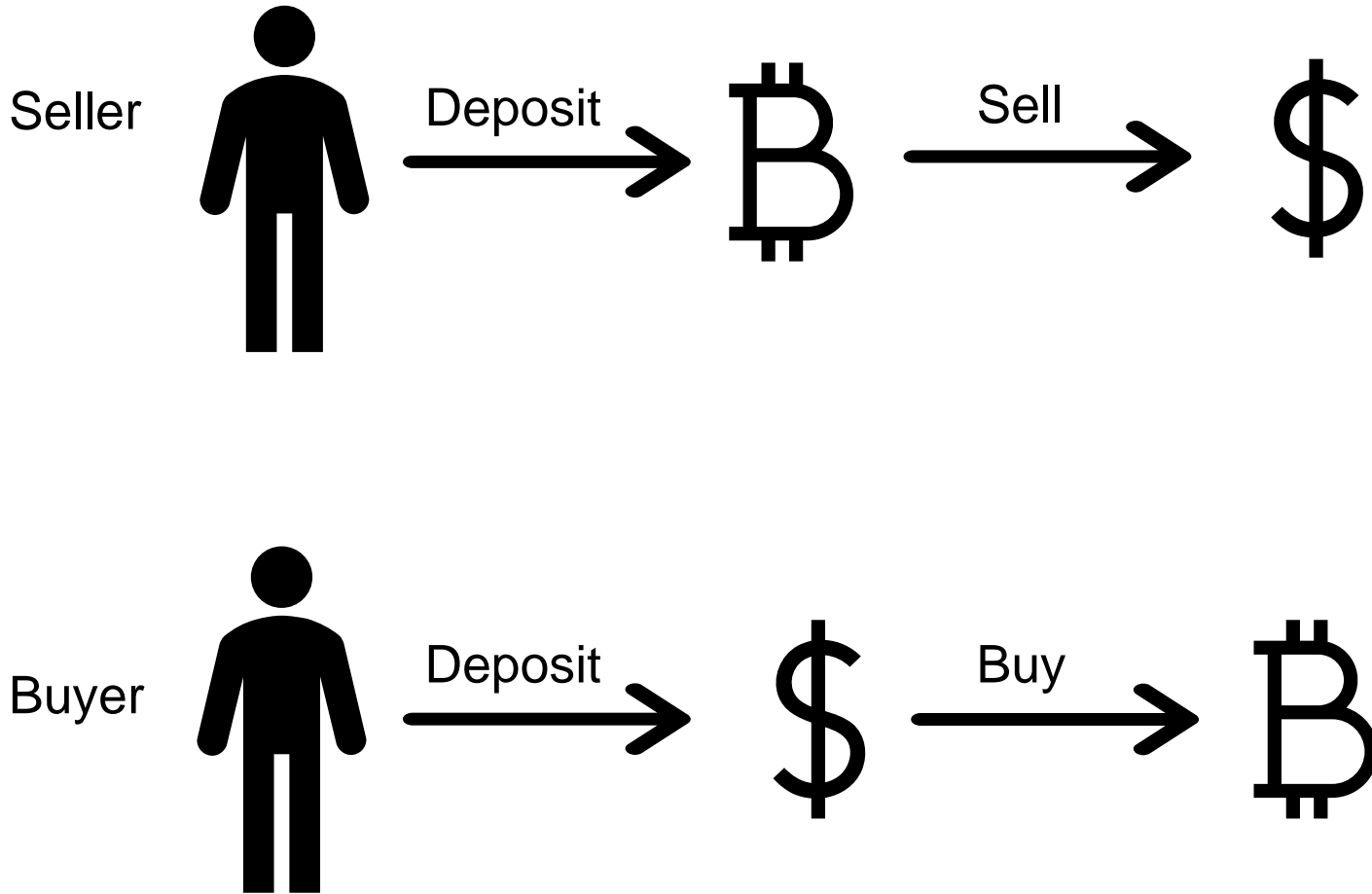
Trader can then view the trading prices of different crypto.

Further, they can place a buy order to purchase crypto, which is then added to the order book along with other buy and sell orders.

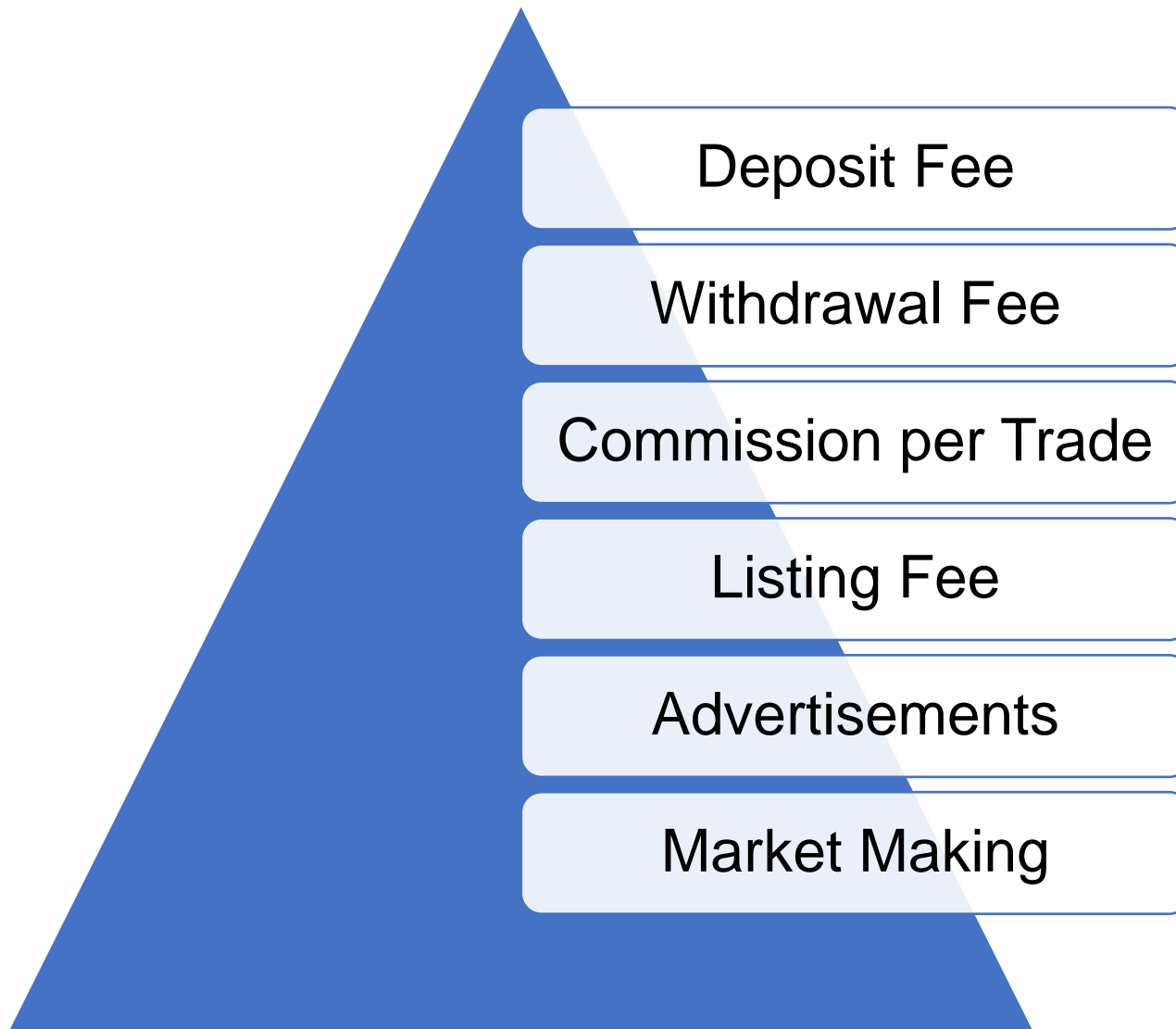
Depending on which type of platform the person is on, the view of exchanges and online brokers generally charge fees for their services.

Once the person has the cryptocurrencies, they can move it from exchange to exchange and wallet to wallet.

Example



How do Crypto Exchange makes money?



How a Crypto Wallet works?

A crypto wallet allows you to access and transact with your crypto via the blockchain.

The wallet software generates pairs of keys, one public and one private, which allow you to send and receive the crypto.

Most wallets accommodate many types of crypto, but not all of them do so.

How Crypto Exchanges and Wallets work together?

Keeping the crypto on the exchange is easier to manage, but it limits the options and can be less secure.

Exchanges are generally unregulated, and few offer insurance in the event of uncertainty. If an exchange goes out of business, one can lose their crypto.

Though using a wallet is a bit complicated, but one can set up their own crypto wallet for more protection.

What to look for in an Exchange?

- Accessibility
- Security
- Liquidity
- Coins offered
- Educational tools
- Storage
- Fees



Risks in Crypto Exchange Platforms

- **Wash Trading:** It is a practice in which the exchanges artificially enhance the trading volume that they report on websites. This is a way of doing business that is unethical and exploits those just starting out trading.
- **Weak Security Measures:** Crypto exchange providers are not specialized cybersecurity firms. Many outsource their cybersecurity tasks, which makes them vulnerable to different attacks if the outsourced provider gets hacked.
- **Single Private Key:** Another risk is that some crypto exchange platforms secure their users' hot wallets using a single private key. If the attacker successfully penetrates the system, it may result in theft and impersonation of user identity to conduct other types of online frauds.
- **Fake Android and iOS Applications:** Another method used by hackers to steal money from cryptocurrency exchange users is distributing fake Android and iOS applications disguised as legitimate trading and cryptocurrency apps.

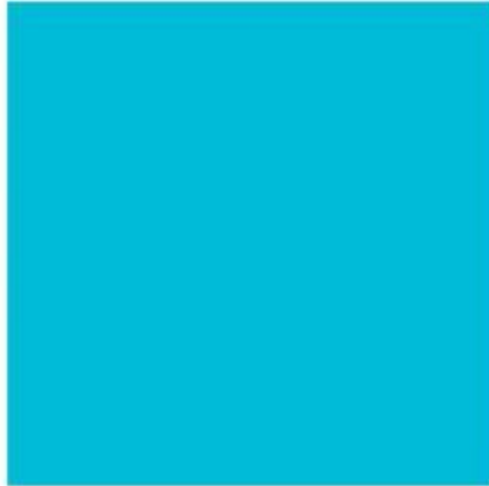
Risks in Crypto Exchange Platforms (contd.)

- **Confidentiality:** No entity stands between the payor and payee in a transaction on the exchange network, and the identity of both remains confidential and participants are difficult to trace. This also makes it a popular method of payment for those engaged in illicit activity.
- **Tax Status:** The tax status of cryptocurrencies might change, and vary by country. In absence of proper regulations in India, it is still unclear whether it is a currency or commodity. While profits gained by investing in cryptocurrencies are subject to an Indian capital gains tax, reporting requirements are still unclear.
- **Regulatory Risk:** One of the major concerns with respect to cryptocurrency is its continued existence in itself. Since, the upcoming bill is different from the earlier one, therefore there is uncertainty as to what new regulations the bill might bring with it.

Takeaways



- A crypto exchange sounds simple but it can be complicated and may require a little more scrutiny from users than traditional stock and bond exchanges do.
- The main thing to remember is that this industry — the coins, the platforms, the blockchains, the exchanges, the wallets — is largely unregulated. That means the consistency users may be accustomed to in the ordinary financial world, in terms of how investments are structured and how investment firms work, is less common in the world of cryptocurrency.
- Thus it's important to invest some extra time to understand basics — like whether a certain exchange can do business in your state or country, what fees they charge, etc. — as well as more complex topics like choosing the right wallet.
- Fortunately, the world of crypto is evolving quickly and a growing number of services are making things easier for investors.



Campus Address :

88, Sector 44,
Gurgaon – 122002

CONTACT US

www.grm.institute

Email :
admissions@grm.institute

Thank you!

