BLOCK-CHAIN TECHNOLOGIES

UNIT-3

UNIT III: Introduction to Bitcoin Bitcoin Block chain and scripts, Use cases of Bitcoin Blockchain scripting language in micropayment, escrow etc Downside of Bit coin mining, Block chain Science: Grid coin, Folding coin, Block chain Genomics, Bit coin MOOCs.

Introduction

Bitcoin is a new type of digital money and, just like with all money, you can store it, exchange it, and make payments with it. The key to what makes Bitcoin different from national currencies like the US Dollar, the Euro or the Japanese Yen lies in its **decentralized** structure and **opt-in model.**

With centralized 'fiat money' (literally money by decree), currency is issued by central banks, and citizens are forced to use the money of their nation. With the exception of cash (which is becoming increasingly rare), transactions are made through intermediaries like banks and payment gateways.

Bitcoin, by contrast, is an opt-in currency that is controlled by the 'consensus' or the will of its users. It consists of a growing network of people who voluntarily agree to the rules of the Bitcoin protocol. They use decentralized infrastructure to make transactions on a peer-to-peer basis and to store value independently of any government, company, or financial institution. There's no need to ask for permission to use Bitcoin, and there's no risk of being cut off from the system.

Entities

The entities involved in the implementation and maintenance of Bitcoins are −

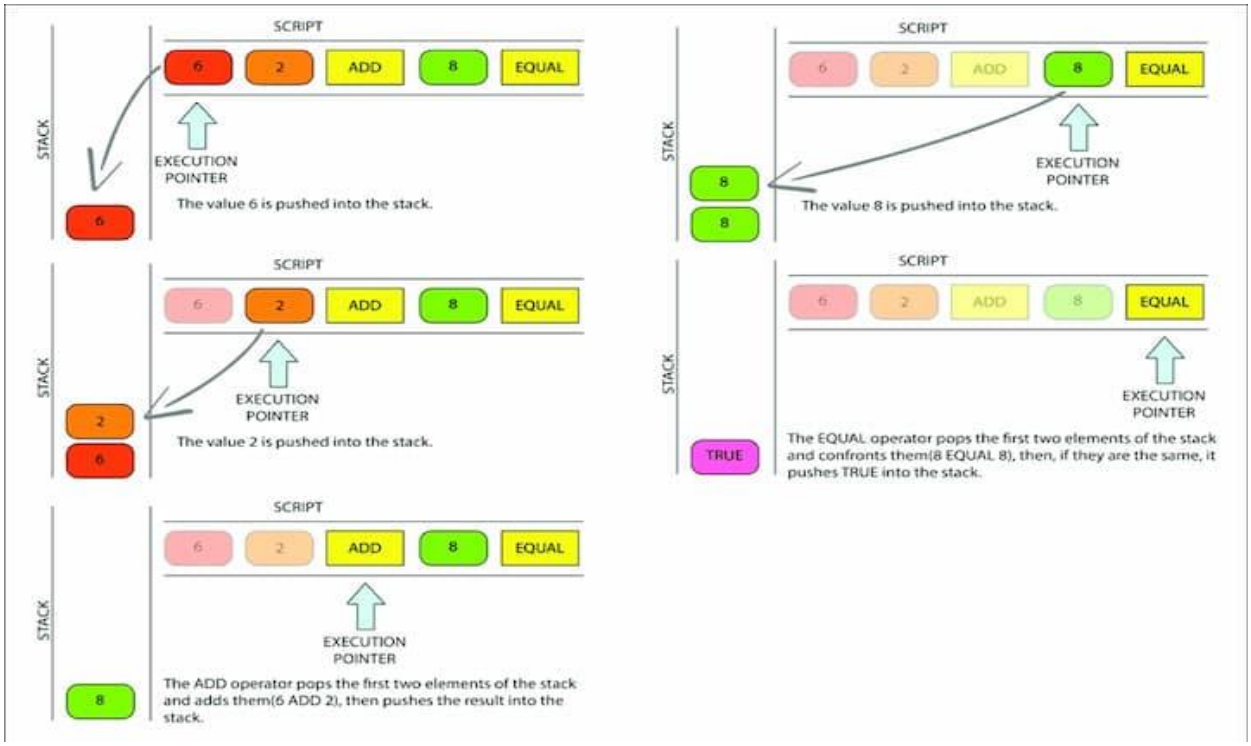
- The Blockchain platform
- Cryptographic algorithms
- Bitcoin miners which are computers or specialized machines that mint the currency and make possible transactions
- People who participate in the transactions and thus help to move the payment system

The philosophy of Bitcoin, and in general, of all cryptocurrencies is that they are distributed systems where there is no central entity that manages the activities such as transactions, among others. It is a peer-to-peer (p2p) system that operates at the level of participants.

BITCOIN BLOCK CHAIN AND SCRIPTS

Bitcoin Script is a simple, stack-based programming language that enables the processing of transactions on the Bitcoin blockchain. To understand more about Bitcoin Script, we'll first look at its characteristics and a basic example of how this programming language works.

Bitcoin Script (also known as Bitcoin Scripting Language or Script) is a simple, stack-based programming language that enables the processing of transactions on the Bitcoin blockchain.



Bitcoin Script - Behind the Scenes of A BTC Transaction

From a very high level, Bitcoin Script can be thought of as a list of instructions recorded with each transaction that describes how the recipient of the funds can gain access to them. Most Bitcoin transactions only require simple scripts, but more complex scripts can be implemented. To understand how Script works, let's breakdown the steps required for a basic Pay To PubKey Hash (P2PKH) transaction.

BTC Script - Basic P2PKH Transaction Example

Let's suppose that Alice wants to send 1 Bitcoin (BTC) to Bob. This transaction is simple with any Bitcoin wallet application, but there is actually a lot of Bitcoin Script code behind the scenes that makes the transfer possible. Each Bitcoin transaction involves at least one locking script and one unlocking script to determine who can spend funds sent to a specific Bitcoin wallet address.

In a P2PKH transaction, Alice does not know Bob's public key. She only knows Bob's address, which is a Base58Check encoded cryptographic hash of Bob's public key. Alice can create the transaction by decoding Bob's address to his "pubkey hash."

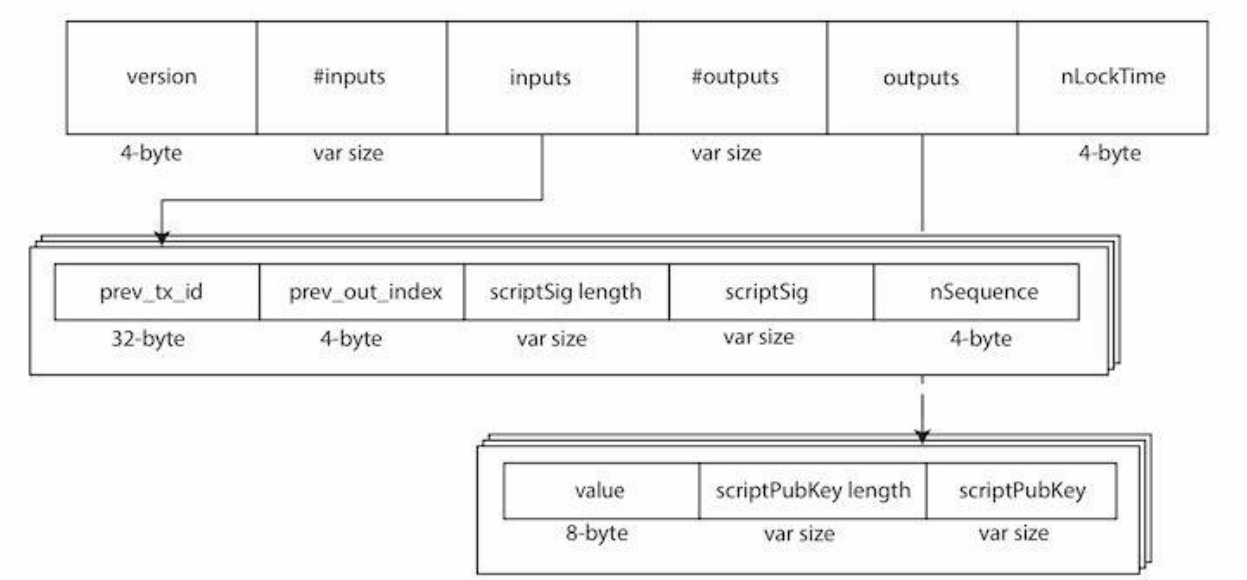
When Alice sends 1 BTC to Bob, a locking script called scriptPubKey is placed on the funds. At that point, the only person who can spend this 1 BTC is the person that supplies the input (i.e., the public key) that produces the pubkey hash to which Alice sent the funds, along with a digital signature from the corresponding Bitcoin private key. In other words, 1 BTC now belongs to Bob, but only if Bob can prove that he is the owner of the BTC address that he provided to Alice

Bob checks his wallet balance and finds that the Bitcoin network has recognized the 1 BTC sent from Alice. Although Bob now technically "owns" these funds, he can't spend them yet. He

needs to verify his true ownership of this 1 BTC to the network before he can send them to someone else.

Let's suppose that Bob wants to send that same 1 BTC to Chris. Before this can happen, Bob first needs to submit an input (UTXO) that meets two requirements. First, the funds Bob is trying to spend must reference the transaction in which he received the funds from Alice by its transaction identifier (TXID). Second, the funds Bob wants to spend must reference the same index number (also called a vector out or vout) as the funds that Alice sent to him in the first place.

Finally, Bob creates an unlocking script called scriptSig (Bitcoin Script Transaction Input) that enables him to spend the funds. As long as Bob provides the scriptSig which matches the conditions set by scriptPubKey (Bitcoin Script Transaction Output), he is able to send 1 BTC to Chris. If Chris wants to send funds to someone else, the cycle of using locking and unlocking scripts continues.



USECASES OF BITCOIN BLOCK CHAIN IN MICRO PAYMENT

Bitcoin micropayments are unlocking new markets and revolutionising online revenue models. By enabling transaction granularity at fractional costs, innovative business opportunities are being made possible.

Micropayments are transactions with a total value below the practical limit for credit card or PayPal transactions, usually under a dollar, while nanopayments refer to amounts less than a tenth of a cent. The revolutionary importance of micropayments lies in their potential to disrupt existing business models, such as subscription-based services or companies that sell user data (e.g. Facebook, Google, Twitter). Micropayments for search could eliminate the need for ads while providing significant revenue. Industries such as e-commerce, gaming, entertainment, and social networking will be significantly impacted by the efficient processing of micropayments.

Use Cases For Micropayments

1. **GCash.**

GCash is a Philippine mobile wallet, mobile payments and branchless banking service. Introduced in 2004. A micropayment service that transforms the mobile phone into a virtual wallet for secure, fast, and convenient money transfer.

GCash is an internationally-acclaimed micropayment service that transforms the mobile phone into a virtual wallet for secure, fast, and convenient money transfer. GCash can be used to buy prepaid load, pay bills, send money, make donations, shop online, and even purchase goods without the need for any cash.

2. **ZipZap**

ZipZap is a payment network enabling consumers to easily buy digital currencies using cash and other payment options. The company's mission is to simplify and democratize payments worldwide. ZipZap promotes digital currencies to create payment solutions.

3. **BitShares**

BitShares Blockchain implements an industrial-grade technology focused on businesses, organizations or individuals, with an amazing eco-system and free-market economy. Based on open-source MIT-licensed Graphene technology, BitShares was launched in its existing form on 13th October 2015, known prior to that as a community project: 'ProtoShares'. Ever since then, the BitShares blockchain and its dApps have been maintained and developed by workers elected via stakeholder consensus, consisting of more than 30 highly skilled professionals.

4. **Logos Network**

The Logos Network is a next-generation crypto network that provides hyper-scalable transaction infrastructure, from micro-transactions to large scale B2B transfers. Its innovative structure overcomes the limitations of the legacy blockchain paradigm and empowers intelligent transfers of value globally. Logos will fundamentally transform what is possible in financial applications, from IoT networks to point-of-sale technology.

Benefits Of Micropayment Transaction Processing Capability

- Automate fractional billing and fees.
- Increase business profitability (depending on the business revenue model).
- Support and offer more subscription tiers for users or customers to access.
- Accommodate fractional transactions for charities.
- Pay-for-what-you-use media streaming through payment channels.
- Capture new markets previously unavailable.
- Create payment schemes with a tithe directed to specific recipients.

ESCROW ETC DOWN SIDE OF BITCOIN MINING

Bitcoin is a form of digital currency or cryptocurrency that is created, held, and exchanged electronically on a decentralized network of computers. The decentralized ledger stores its transactions in the form of blocks, hence, the name “blockchain”.

All transactions are broadcast to the network and are recorded on the blockchain, which acts as a storage for these transactions, encoding them in a way that does not allow them to be changed. The blockchain is maintained by a distributed network of computers called miners that are rewarded for their work with newly generated Bitcoins.

This process of verifying and recording transactions is known as mining. By using the blockchain, Bitcoin users can send and receive payments at a lower cost than traditional networks like banks, which made this technology so disruptive in the first place

What is Proof-of-Work Mechanism?

Proof-of-Work (PoW) is an algorithm used to confirm transactions and produce and add new blocks to the blockchain.

It is a mechanism that requires nodes to solve complex algorithms to validate transactions, which are responsible for the creation of new blocks. Bitcoin uses PoW to mint blocks for its blockchain and secure the network against malicious attacks. It also serves as a way to prevent double-spending and ensure that transactions are both valid and irreversible.

PoW enables Bitcoin to remain decentralized, as the system is powered by miners who compete to process transactions.

What is Escrow?

Escrow is a legal agreement between two parties that is used to protect the interests of both parties. It is a way to facilitate the secure exchange of goods or services. In an escrow agreement, a third party holds onto the property or money until both parties fulfill their obligations in the agreement.

What is Bitcoin Escrow?

Bitcoin escrow is a service designed to act as an intermediary between two parties involved in a transaction.

In a typical transaction, one party sends the Bitcoin to the escrow service, where it is held until both parties agree to the terms of the transaction.

Once both parties have agreed that the stipulated obligations have been fulfilled, the Bitcoin is released to the receiving party. This type of service is particularly useful for those who are buying and selling goods or services online, as it provides a layer of trust and security to the transaction being carried out.

The purpose of using an escrow service is to protect both parties from any potential fraud. By using an escrow service, buyers can be sure that the seller will not take the money and run, while sellers can be sure that buyers are not trying to scam them out of their money. Escrow services also provide a way for buyers and sellers to set rules and conditions for the transaction, and to dispute any potential issues that may arise

Service Providers for Bitcoin Escrow

Paxful Escrow Service

Paxful is an online marketplace that allows users to buy and sell Bitcoins on a peer-to-peer (P2P) basis. The platform provides users with an escrow service that helps to protect their funds and offers an extra layer of security when trading.

The major benefit of using Paxful's escrow service is that it provides a safe environment for trading Bitcoins. The escrow service holds the funds until the trade is completed and the buyer confirms the transaction. This reduces the risk of fraud and ensures that both parties are protected.

In addition, Paxful provides a range of payment methods for buyers and sellers to use, which makes it easier for them to complete transactions. The platform also offers a wide range of currencies, allowing traders to buy and sell Bitcoins in their local currency.

One downside of Paxful's escrow service, however, is that it can take some time for the funds to be released. The platform also charges a fee for each transaction performed, which can add up over time. On the other hand, the platform provides an extra layer of security, a variety of payment methods, and a wide range of currencies to work with.

Final Thoughts

Bitcoin has escrow services available for those who wish to use them. These services are designed to provide an additional layer of trust and security for those engaging in online transactions involving Bitcoin.