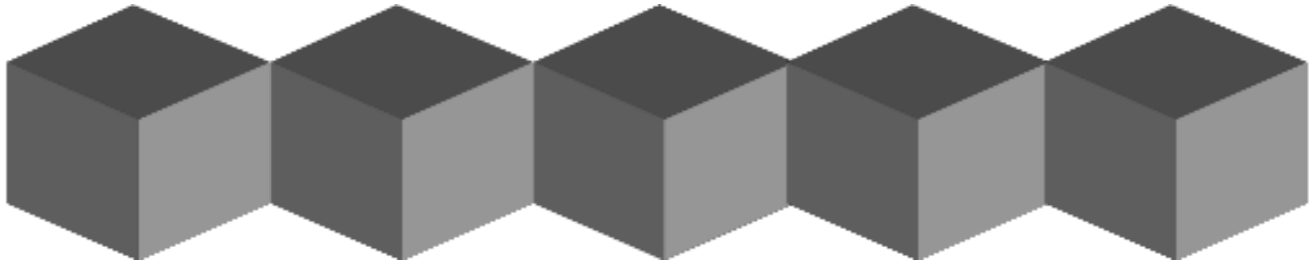
Course Outline

1. Cryptocurrency and Block chain
2. Delving into BlockChain
3. Bitcoin and Block chain
4. Bitcoin Mining
5. Ethereum
6. Setting up private Blockchain Environment using Ethereum Platform
7. Hyperledger
8. Setting up Development Program using Hyperledger composer
9. Create or Deploy our private Blockchain on Multi chain
10. Prospect of Blockchain

IntelliPaat

Bitcoin and BlockChain



Agenda

At the end of this session you will be able to:

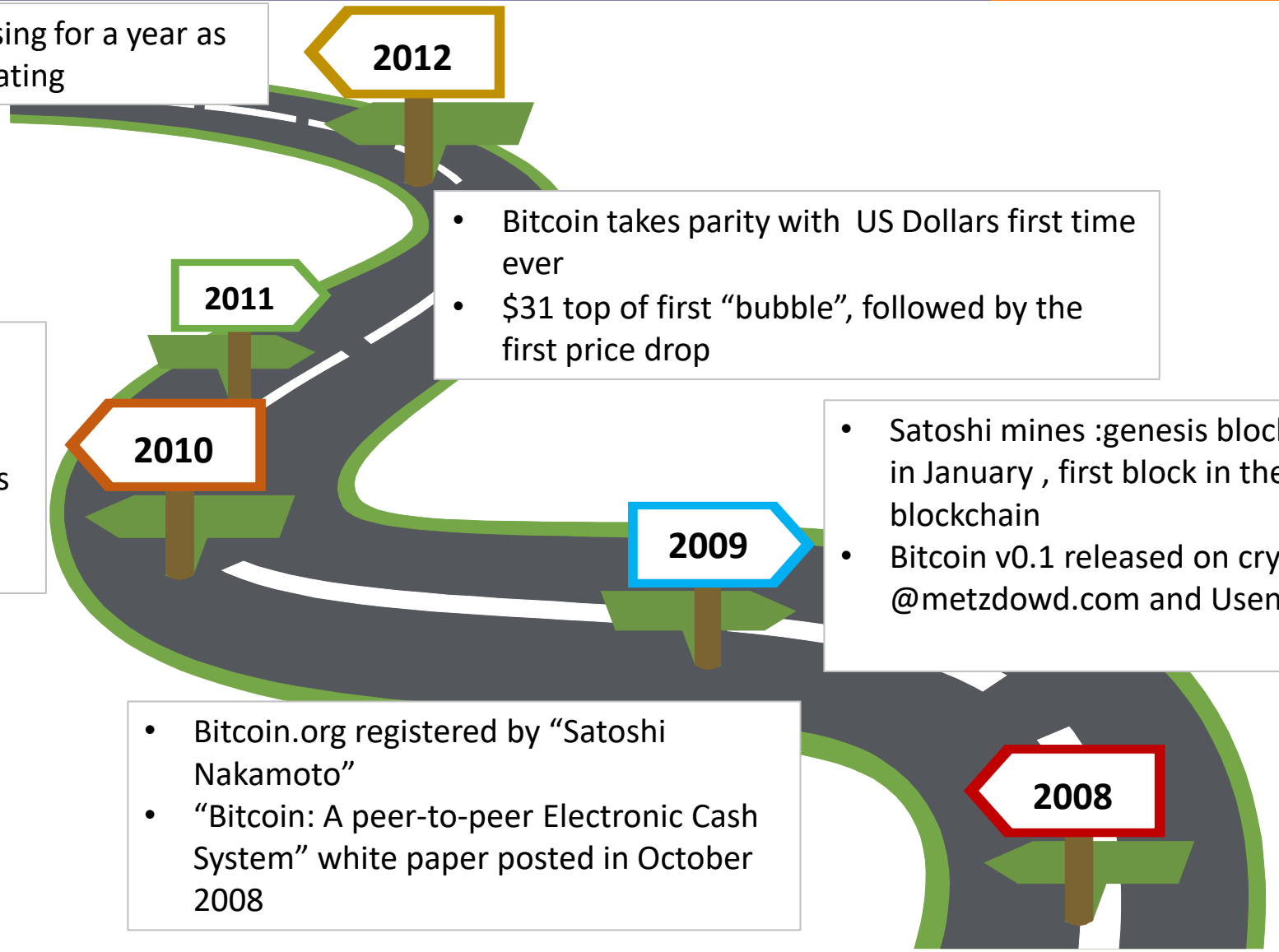
- Identify Bitcoin and its Era
- Understand Where & How to Get Bitcoins
- Identify Bitcoin Wallets
- Identify Jaxx Wallet
- Define Selling Bitcoins
- Compare Bitcoin Blockchain, Transaction & Transaction Script
- Describe Various Transaction Forms in Bitcoin
- Define Scripts in Bitcoin
- List Nodes in Bitcoin Network

Bitcoin and its Era

Bitcoin and its Era

Let’s learn about History of bitcoin and its details of bitcoin.

History of Bitcoin



- Dec: $13, slowly rising for a year as it was really fluctuating

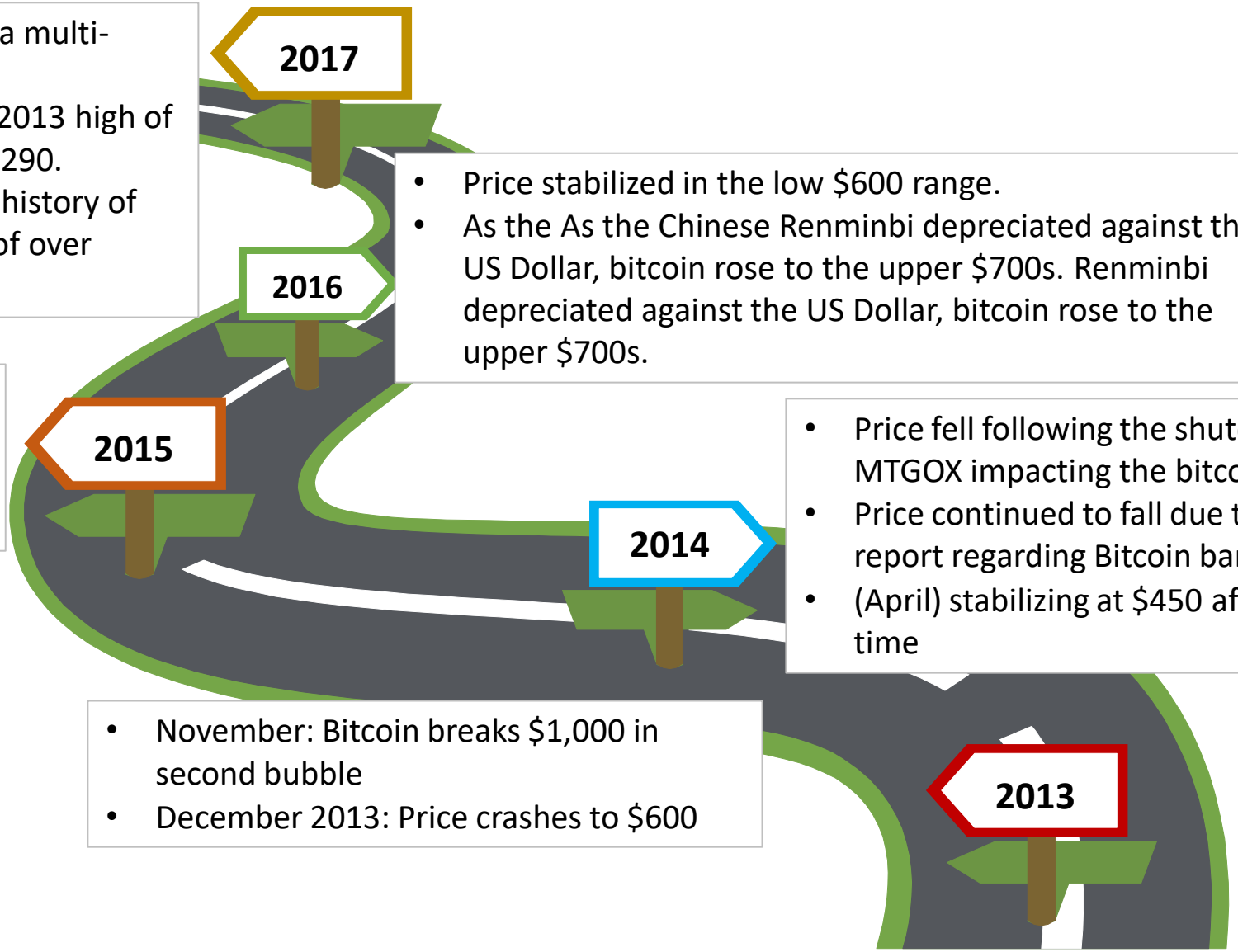
- Bitcoin takes parity with US Dollars first time ever
- $31 top of first “bubble”, followed by the first price drop

- First offline transaction: 10K BTC for two pizzas was done successfully
- First specialized GPU hash miners and pooled mining operations

- Satoshi mines :genesis block” of 50 BTC in January , first block in the bitcoin blockchain
- Bitcoin v0.1 released on cryptography @metzdowd.com and Usenet

- Bitcoin.org registered by “Satoshi Nakamoto”
- “Bitcoin: A peer-to-peer Electronic Cash System” white paper posted in October 2008

History of Bitcoin



- Price fell 30% in a week, reaching a multi-month low of $750.
- Price broke above the November 2013 high of $1,242 and then traded above $1,290.
- Price reached its maximum in the history of bitcoin. Reached an all-time high of over $12,500.

- Price stabilized in the low $600 range.
- As the As the Chinese Renminbi depreciated against the US Dollar, bitcoin rose to the upper $700s. Renminbi depreciated against the US Dollar, bitcoin rose to the upper $700s.

- Price fell through to early 2015.
- Large spike in value from 225–250 at the start of October to the 2015 record high of $504

- Price fell following the shutdown of MTGOX impacting the bitcoin market
- Price continued to fall due to a false report regarding Bitcoin ban in China
- (April) stabilizing at $450 after a long time

- November: Bitcoin breaks $1,000 in second bubble
- December 2013: Price crashes to $600

What is Bitcoin?

The first Blockchain focused decentralized digital currency

Uses consensus to control its creation and management, rather than relying on central authorities

Held electronically in a p2p open ledger called the blockchain

They are not printed. They are produced by people using software that solves mathematical problems

Why use Bitcoins?

01

It's super Fast

Transactions are instantaneous if they are "zero confirmation" transactions, Or, they can take around 10 minutes is a merchant requires confirmation

02

It's really Cheap

Bitcoin transaction fees are minimal, or in some cases free too

03

It's absolutely Decentralized

Because the currency is decentralized, you own it. No central authority has control over bitcoins

04

Never worry about Chargebacks

Once bitcoins have been sent, they're gone. A person who has sent bitcoins cannot try to retrieve them without the recipient's consenunder any circumstances

Why use Bitcoins?

05

Best Payment Security

Transactions don't require you to give up any secret information. They use two key: Public key, and a private one

06

It is not inflationary

Only 21 million will ever be created under the original specification under bitcoin protocol

07

It's really Private

It's like having a clear Its plastic wallet with no visible owner. Everyone can look inside it, but no one knows whose it is.

08

Make your own Money

You can certainly buy bitcoins in the open market, but you can also mine your own if you have computing power

Where & How to Get Bitcoins

Where & How to Get Bitcoins

How we can get BITCOINS?

Where & How to Get Bitcoins

> To buy or sell a bitcoin, customer has to join the network

How do you buy a Bitcoin?

1.To start with, a user must install a virtual wallet onto a PC or mobile device. The wallet keeps track of your bitcoin balance and all transactions

2.Bitcoin can be bought either through online payment company or

3.Once the funds are available, a buyer can place an order for a bitcoin, similar to trading stocks, through various online exchange

4.Bitcoins can also be purchased from third parties , which sends the coins directly into the virtual wallet

Bitcoin and its Client

To join a bitcoin ecosystem and start using the crypto currency, all the users are required to do is download an application or use a web based application.

Full Client

Stores the complete history of bitcoin transactions and manages the users' wallets, and capable of initiating transactions directly on the bitcoin network.

Web Client

Web clients are accessed through a browser and store the user's wallet on a server owned by a third party. They are used by exchanges primarily

Lightweight Client

This type of client Stores the user's wallet but relies on third-party–owned servers for access to the bitcoin transactions and network

Bitcoin Wallets

Bitcoin Wallets

There are various Bitcoin wallets or clients available in the market.

Types of Bitcoin Wallets

Web-Wallets	•Web-wallets are websites or even online exchanges that allow storage. •Example-Blockchain.info, Coinbase, etc
Mobile Wallets	•A smartphone wallets makes it really easy to scan QR codes to make quick payments via phone only. No need to go to web browser for the same. •Example: Breadwallet, Mycelium, AirBitz, GreenBits
Desktop Wallets	•Apps installed on a personal computer like desktop or laptop. •Example: Electrum, Multibit, Armory
Hardware Wallets	•A piece of hardware is used to store the private keys to your bitcoins. •Example: Ledger Nano, Trezor
Paper Wallets	•It is the most secure cold-storage solution •Example: Coindesk, Bitadress,
Multi-signature Wallets	•These wallets require multiple private key signatures to make a transaction •Examples: CarbonWallet, Coinbase, Blocktrail, electrum, CoinKite

Different types of Bitcoin Wallets

Compare Wallets					
Wallet Type	Hot Wallet	Hot wallet	Hardware wallet	Hot wallet	Hot Wallet
Web Interface	✔	✖	✔	✖	✖
Mobile app	✔	✔	✖	✖	✖
Desktop client	✔	✖	✖	✔	✔
Independent wallet	✔	✔	✔	✔	✔
Privacy	Good	Good	Good	Good	Moderate
Security	Good	Good	Good	Good	Good
Newbie friendly	✔	✖	✔	✖	✔

Different types of Bitcoin Wallets

Compare Wallets					
Wallet Type	Hot Wallet	Hot wallet	Hardware wallet	Hot wallet	Hot Wallet
Web Interface	✔	✖	✔	✖	✖
Mobile app	✔	✔	✖	✖	✖
Desktop client	✔	✖	✖	✔	✔
Independent wallet	✔	✔	✔	✔	✔
Privacy	Good	Good	Good	Good	Moderate
Security	Good	Good	Good	Good	Good
Newbie friendly	✔	✖	✔	✖	✔

Comparing different Wallet type

Wallet Type	Safety	Beginners	Convenience	Cost
Web	Unsafe	Easy	Very convenient	Free
Mobile	Unsafe	Easy	Very convenient	Free
Desktop	Safe	Average	Average	Free
Hardware	Very safe	Average	Not convenient	90-400 USD
Paper-Wallet	Very safe	Difficult	Not convenient	Usually free
Multi- Sig	Safe	Difficult	(variable)	Free

Jaxx Wallet

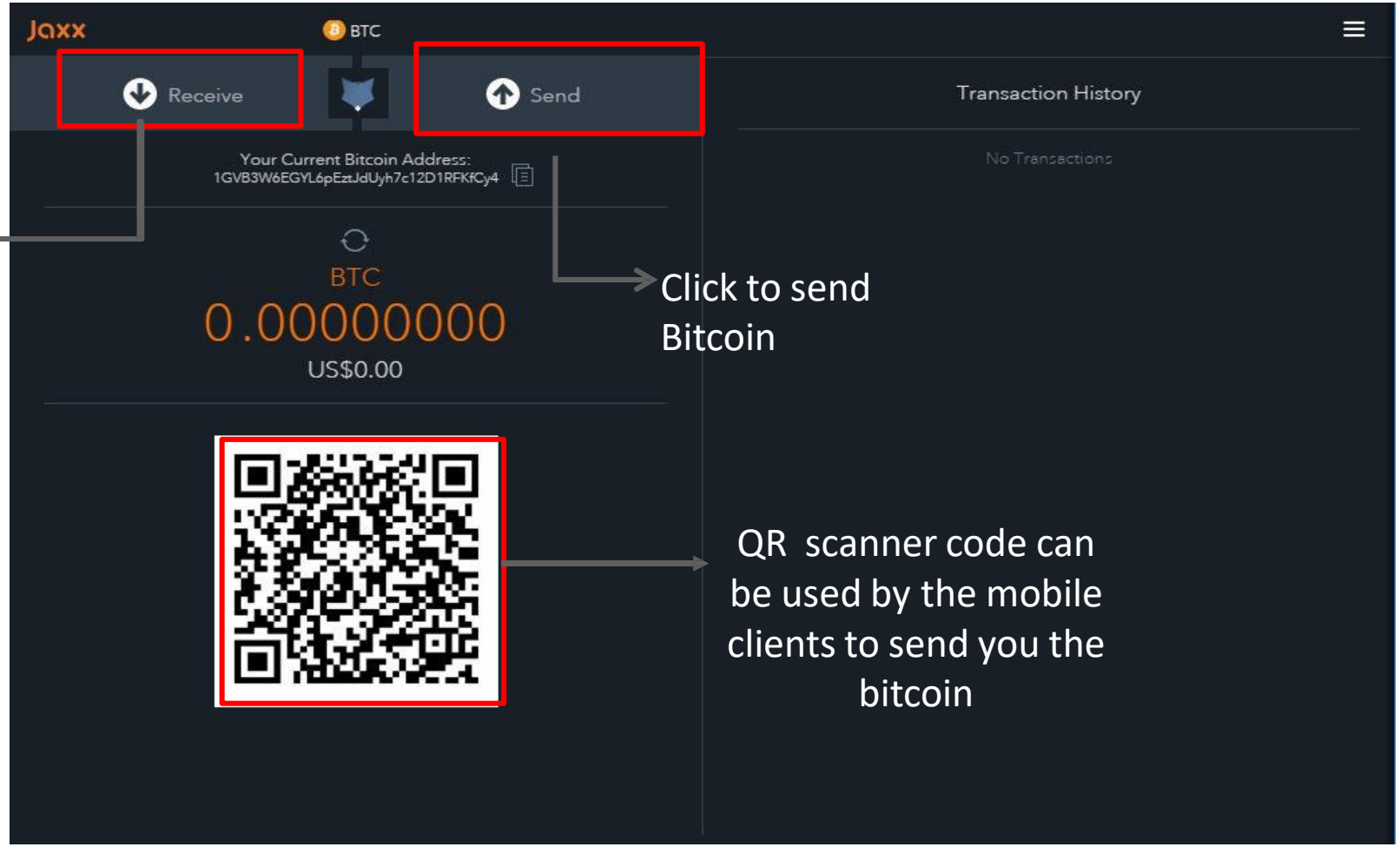
Jaxx Wallet

Now that we have discussed and compared various Bitcoin wallets, lets see a wallet in working.

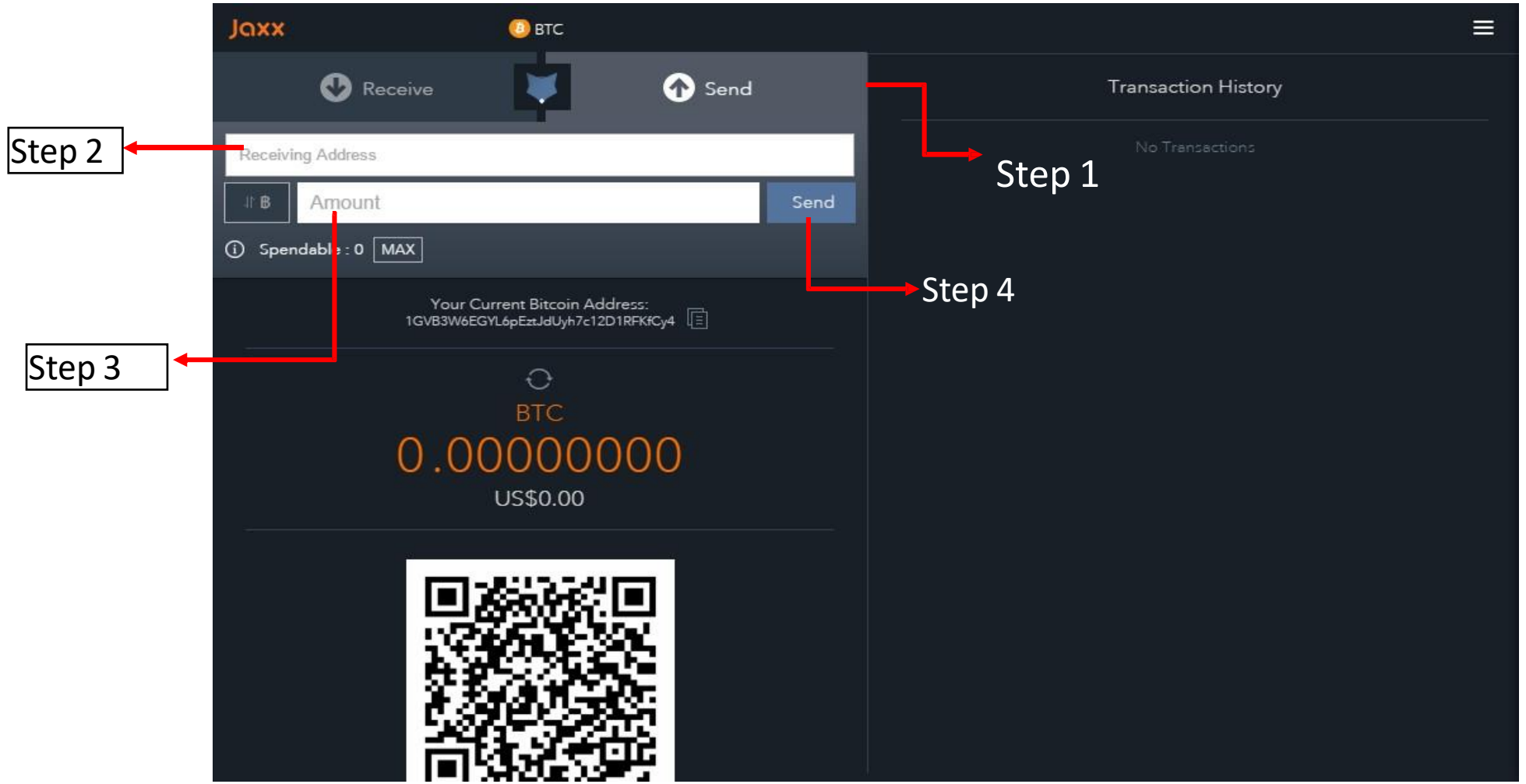
Jaxx Bitcoin Wallet

JAXX wallet home screen

Jaxx Wallet Screen



Sending Bitcoins from Jaxx Wallet



Procedure for Sending Bitcoins

In order to send Bitcoin through Jaxx wallet, consider the following steps:

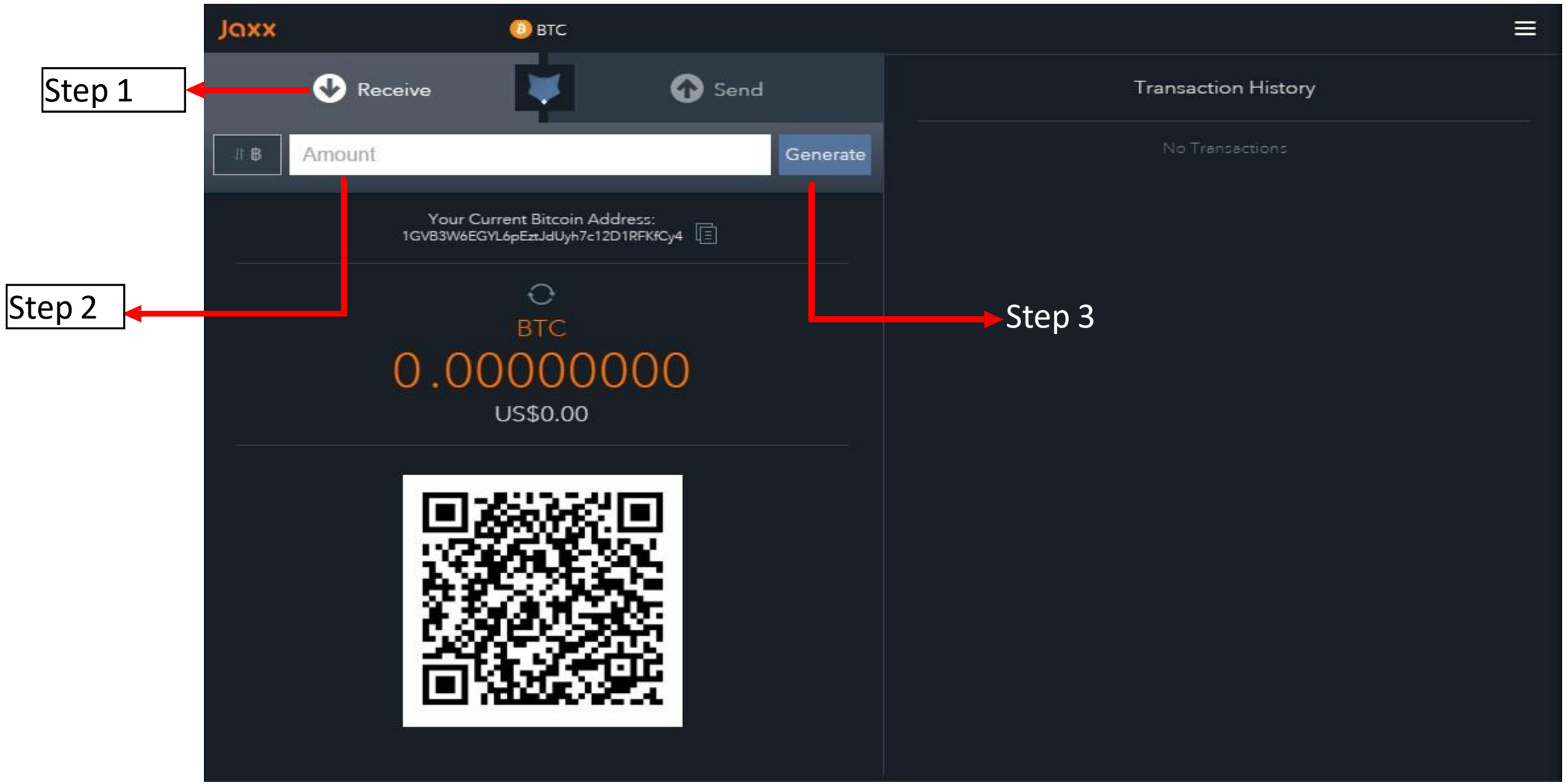
Step 1: Click the send button

Step 2: In the address section, paste the Bitcoin address of the person you are willing to send the Bitcoin

Step 3: In the amount section, enter the amount of Bitcoins you want to send

Step 4: Click on the send icon (in blue)

Receiving Bitcoins through Jaxx Wallets



Receiving Bitcoins through Jaxx Wallets

Procedure for Receiving Bitcoins

In order to receive Bitcoin through Jaxx wallet, consider the following steps:

Step 1: Click the receive button

Step 2: Select whether you want the amount to be in the currency type or the default fiat currency of your choice.

Step 3: In the amount section, enter the amount

Step 4: Click on the generate icon (in blue)

Method to Secure your Wallet

There are multiple ways to make your bitcoin wallet more secure:

Encrypt the wallet

To protect your wallet from prying eyes is to encrypt it. This makes it difficult to access your wallet, but not impossible

Use Multi-sig

Allow multiple parties to partially seed an address with a public key. The required number of signatures is agreed at the start when people create the address

Back it up

Backing up your wallet makes a copy of your private keys, but it's important to back up your *whole* wallet

Take it offline

Cold storage wallets store private bitcoin offline

Buy your first Bitcoins

It is still quite difficult to acquire bitcoins in most countries. CryptoCurrency exchanges are the easiest way to buy bitcoins

A European currency market that supports several currencies including euros (EUR) and US dollars (USD) via wire transfer

A US-based bitcoin wallet and platform where merchants and consumers can transact in bitcoin

Zebpay is the fastest and easiest way to Buy and Sell Bitcoins in India

Coinsecure is the most secure Bitcoin exchange to buy, sell & accept Bitcoins

Selling Bitcoins

How to Sell Bitcoins

- Selling Bitcoins Online
- Selling Bitcoins in Person

Selling Bitcoins Online

These are the three ways to go about selling bitcoin online:

Direct Trade
Involves a trade with another person, directly.

01

Exchange Trades
Involves an online exchange, where your can trade with the exchange rather than another individual or any unknown person

02

Peer to peer trade
Allow bitcoin owners to obtain discounted goods with their bitcoin via others that want to obtain the cryptocurrency with

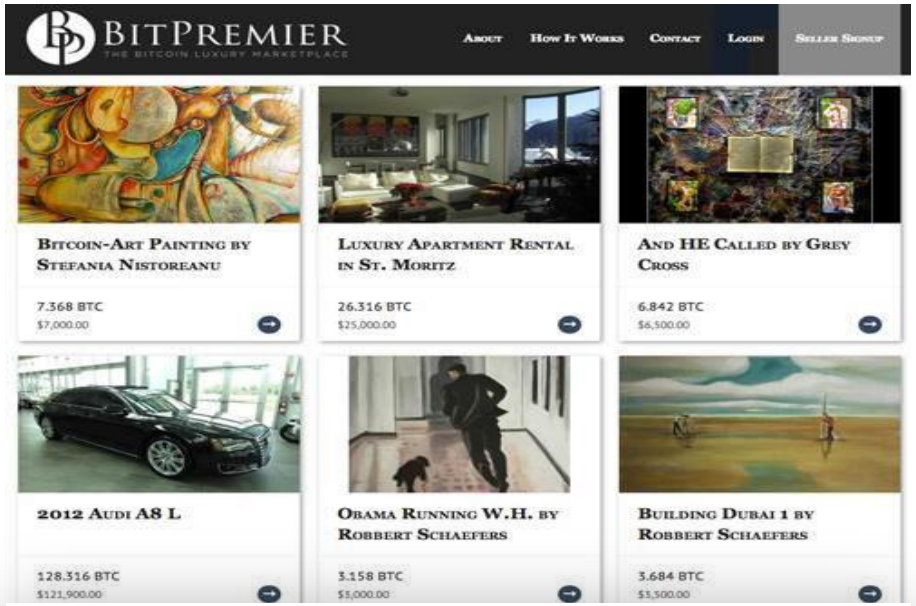
03

Examples of Selling Bitcoins

1. Online with the exchanges
2. Websites that offer this type of selling model include Coinbase and LocalBitcoins in the US, and BitBargain UK and Bittylicious in the UK and many other exchanges across the globe
3. Peer to Peer
4. The marketplace acts as an intermediary, offering users the platform, bitcoin wallet and escrow for transactions.

Places To spend Bitcoins

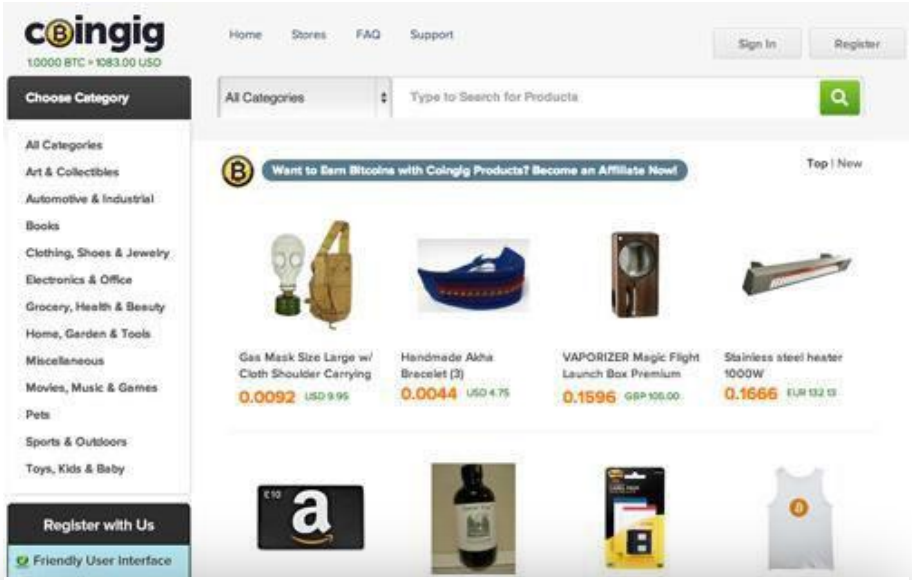
Online marketplace that sells a variety of electronic gadgets



Luxury Bitcoin-only marketplace, where you can find anything from high-performance sports cars to works of art and even real estate.

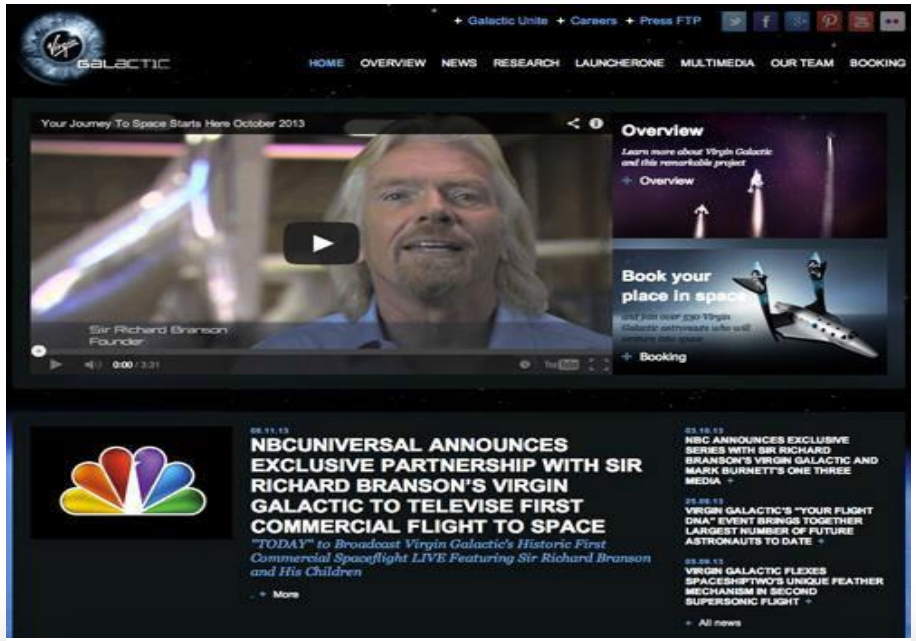
Places To spend Bitcoins

Lets you buy, receive, redeem and send digital gift cards for over 200 retailers, including Amazon, Sears, Target and GameStop



Online marketplace that conducts its transactions solely in Bitcoins. You can find everything from books to t-shirts to gift vouchers on Coingig

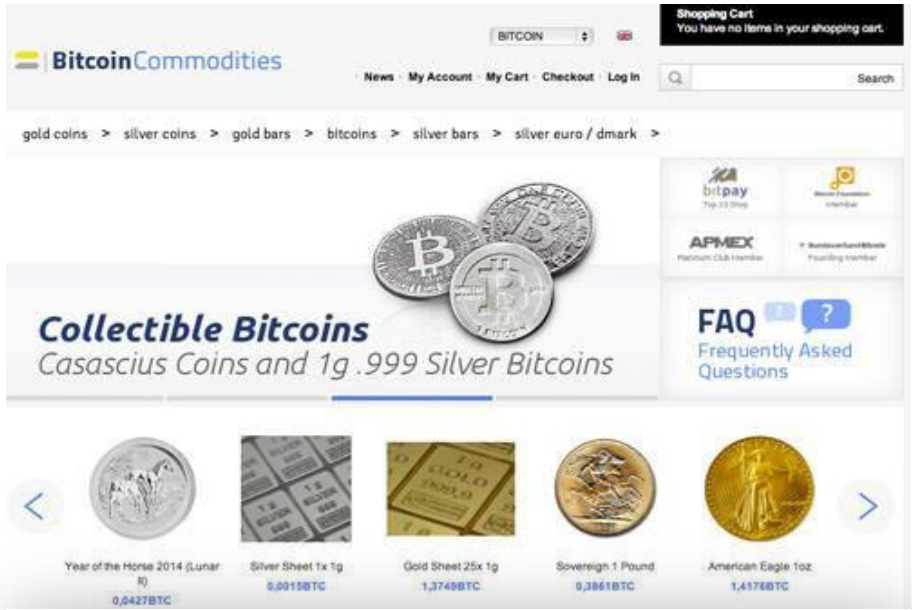
Places To spend Bitcoins



Richard Branson's Virgin Galactic venture, recently announced that it had begun accepting Bitcoins as payment for their suborbital space flights.

CheapAir intends to eventually allow you to book hotels and flights using Bitcoin via their iOS app.

Places To spend Bitcoins



Sells gold and silver coins, bars and sheets. As the name suggests, it accepts Bitcoin payments.

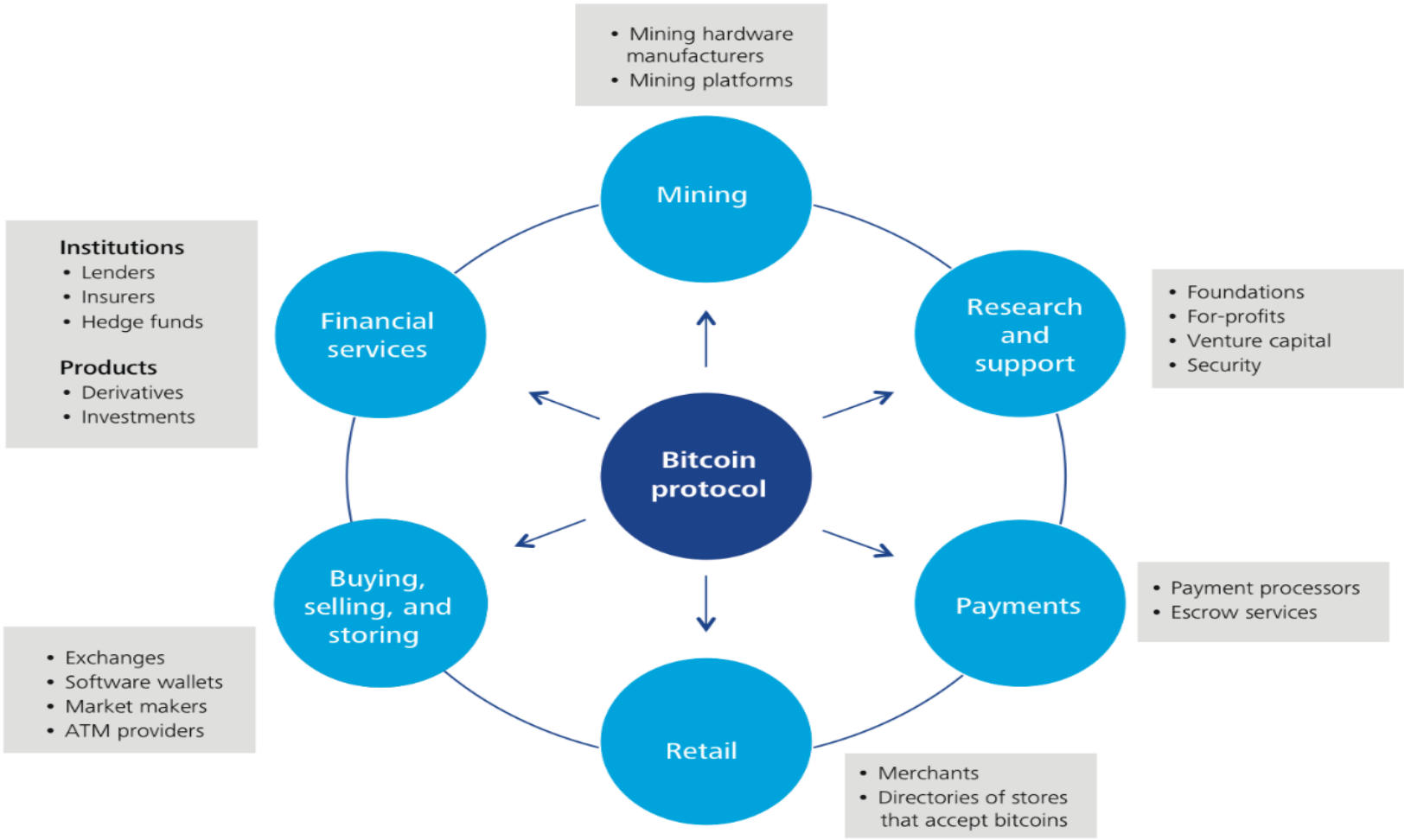
Acts as a middleman between you and travel sites such as Expedia; you pay in Bitcoins to TravelForCoins, who will pay for your flights using standard currency

Bitcoin Blockchain, Transaction & Transaction Script

Bitcoin Blockchain, Transaction & Transaction Script

> Now that we have seen how a bitcoin is used and spent, let's see what exactly happens when a transaction occurs

Bitcoin Ecosystem



Structure of bitcoin Transaction

A transaction contains a number of fields:

Size	Field	Description
4 bytes	Version	Specifies the rules this transaction follows
1-9 bytes(VarInt)	Input Counter	How many inputs are included
Variable	Outputs	One or more transaction outputs
1-9 bytes (VarInt)	Output Counter	How many outputs are included
variable	Outputs	One or more transaction outputs
4 bytes	Locktime	A unix timestamp or block number

Unspent Transaction Output

UTXO or Unspent transaction output is a fundamental building block of a bitcoin

- An Unspent Transaction Output (UTXO) that can be spent as an input in a new transaction.
- The network keep track of all available UTXO currently numbering in the millions

- The first block contained 50 mined BTC in address A (A = 50)
- The second block contained 50 mined BTC in address A, a transaction sending 20 BTC to address B, and putting the change in address C (A = 50, B = 20, C = 30)
- The third block contained 50 mined BTC in address A, a transaction sending the 20 BTC from address B to address D (A = 50 + 50, C = 30, D = 20)

Unspent Transaction Output

So, after three blocks, there are four unspent outputs:

A has two unspent outputs worth 50 BTC each
C has a single unspent output worth 30 BTC
D has a single unspent output worth 20 BTC

And there are two spent outputs:

- the 50 BTC generated in the first block, spent in the 2nd block
- the 20 BTC output created in the 2nd block and spent in the 3rd block

Note that unspent outputs don't merge together. The two unspent 50 BTC outputs at address A are separate, and will remain separate at least until they are spent in a transaction

Bitcoin Transaction Inputs and Outputs

Firstly, four axiomatic truths about transactions:

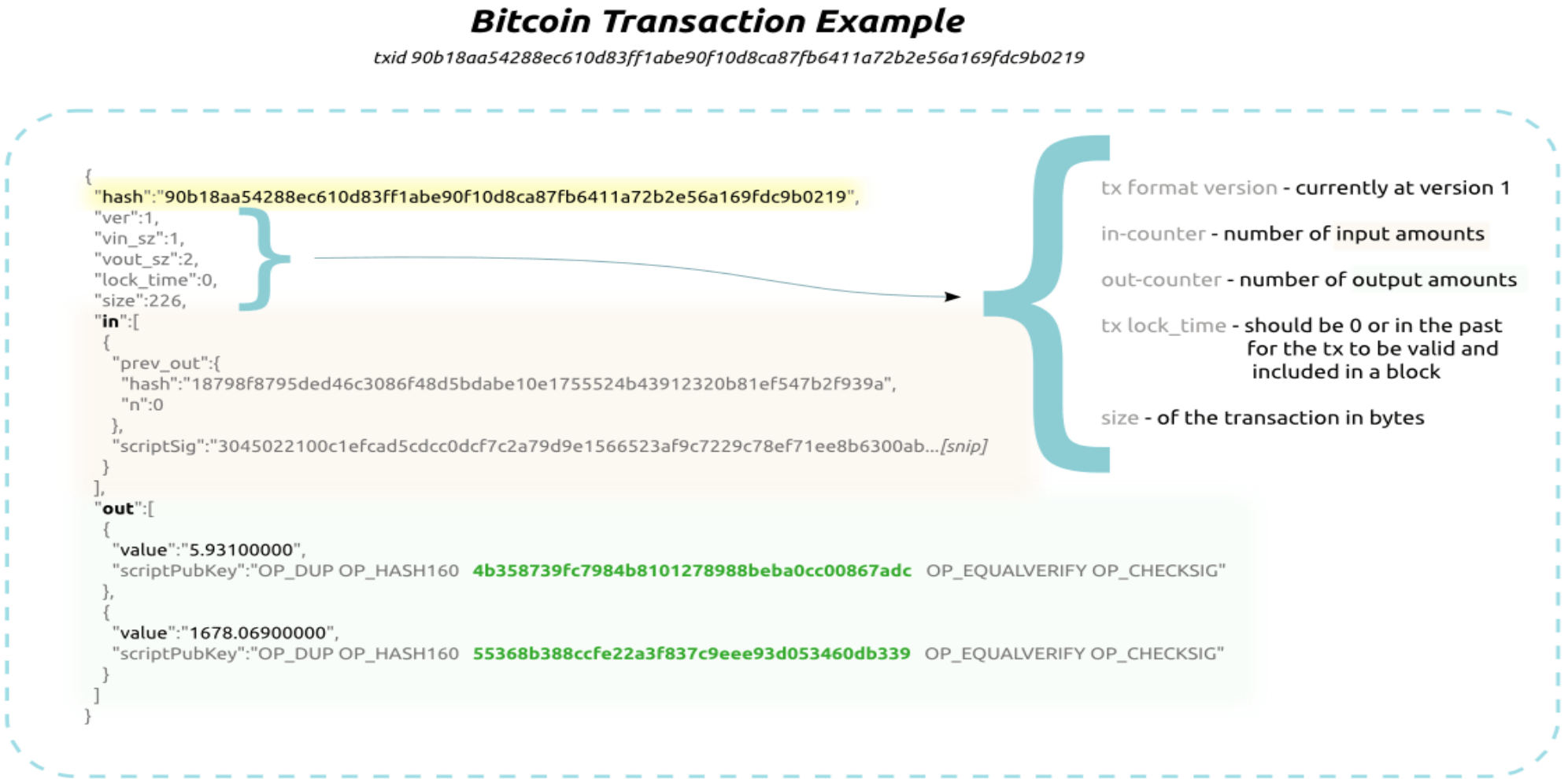
Any Bitcoin amount that we send is always sent to an address.

Any Bitcoin amount we receive is locked to the receiving address – which is (usually) associated with our wallet.

Any time we spend Bitcoin, the amount we spend will always come from funds previously received and currently present in our wallet.

Addresses receive Bitcoin, but they do not send Bitcoin – Bitcoin is sent from a wallet.

Bitcoin Transaction Inputs and Outputs

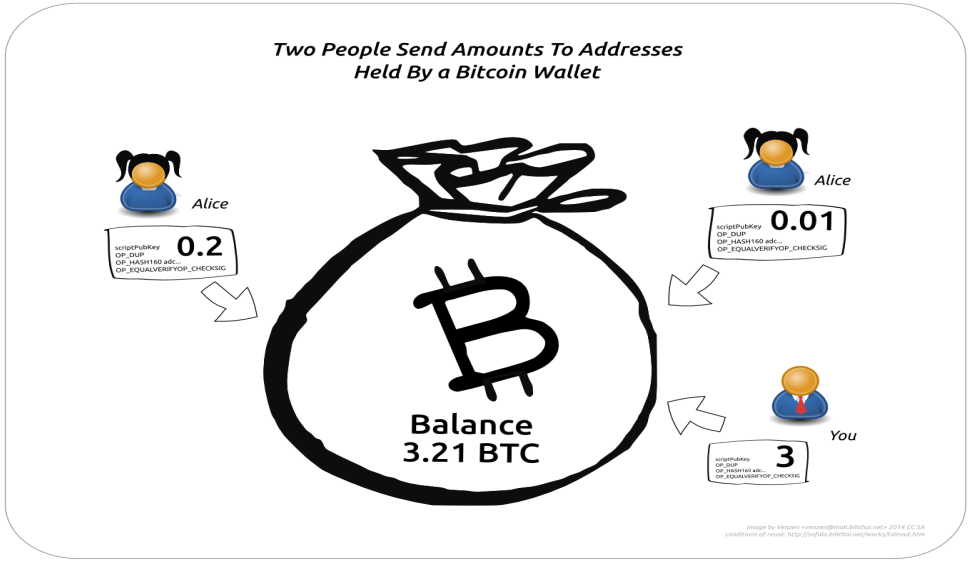


Bitcoin Transaction Inputs and Outputs

> The amounts that go into our wallet are not jumbled like the coins in a physical wallet. Th received amounts don't mix but remain separate and distinct as the exact amounts received by the wallet. Here's an illustration:

Example

You create a brand new wallet and, in time, it receives three amounts of 0.01, 0.2 and 3 BTC as follows: you send 3 BTC to an address associated with the wallet and two payments are made to another address by Alice.

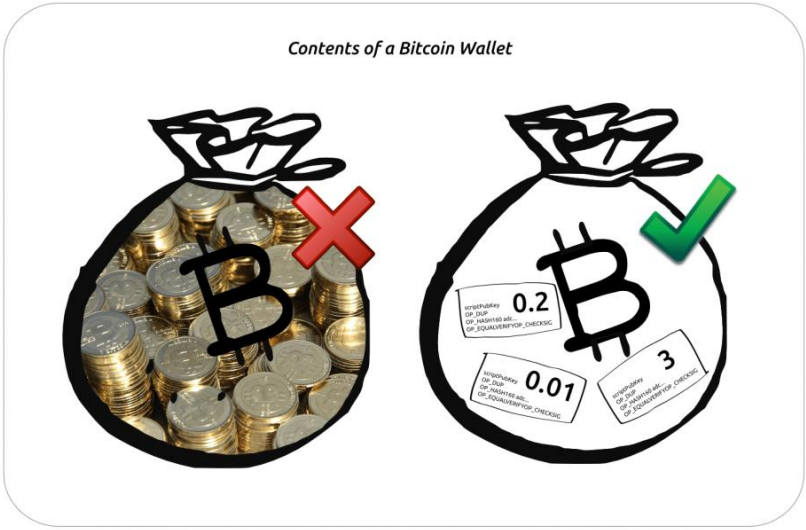


Bitcoin Transaction Inputs and Outputs

> The wallet reports a balance of 3.21 BTC, yet if you were to virtually peek inside the walle you would see – not 321,000,000 satoshi (321 mil satoshi) – but three distinct amounts st grouped together by their originating transactions: 0.01, 0.2 and 3 BTC.

The received bitcoin amounts don't mix but remain separated as the exact amounts sent to the wallet. The three amounts in the example above are called the outputs of their originating transactions.

Bitcoin wallets always keep outputs separate and distinct.



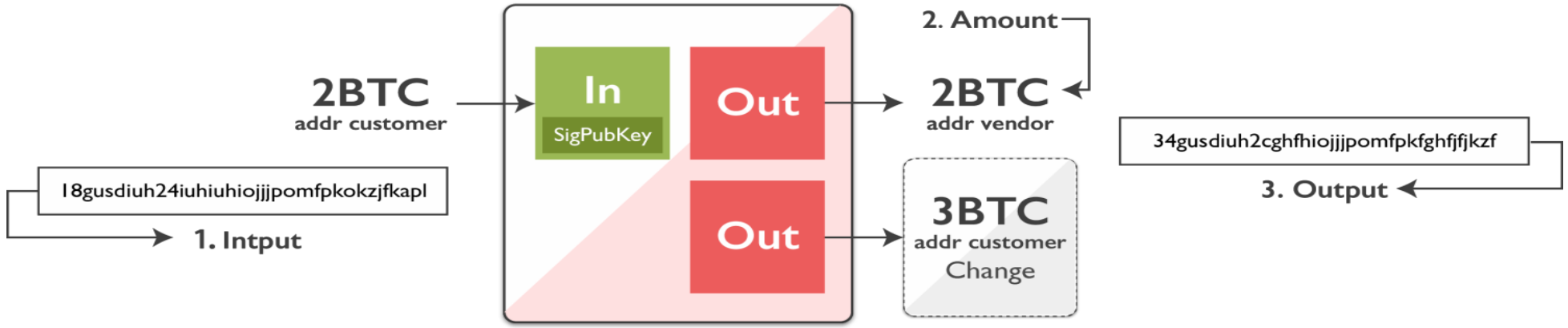
Transaction Inputs

- Transaction inputs are pointers to UTXO
- They points to UTXO by reference to the transaction hash and sequence number
- To spend UTXO, a transaction input also includes unlocking scripts that satisfy the spending conditions set by the UTXO

Size	Field	Description
32 bytes	Transaction hash	Pointer to the transaction containing the UTXO to be spent
4 bytes	Output index	The index number of the UTXO to be spent; first one is 0
1-9 bytes (VarInt)	Unlocking-Script Size	Unlocking-Script length in bytes, to follow
Variable	Unlocking-Script	A script that fulfils the conditions of the UTXO locking script
4 bytes	Sequence Number	Currently disabled Tx-replacement feature, set to oxFFFFFFFF

What does a Transaction look like?

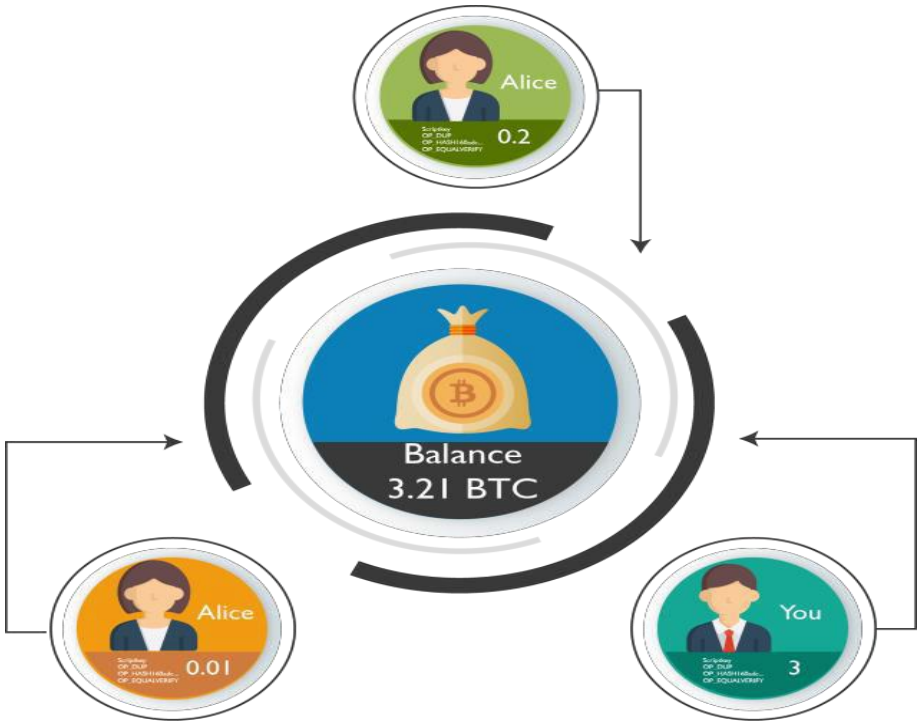
A transaction has three pieces of information:



1. Input: This is a record of which bitcoin address was used to send the bitcoins to customer in the first place
2. Amount: This is the amount of bitcoins that A is sending to Vendor
3. Output: This is Bob's bitcoin address

Example to show the Transfer of Bitcoin

Let's say Andy has 3.21 BTC in his Wallet sent to him at different addresses



Andy's Wallet Balance

The received amount remain separated as exact amounts sent to the wallet

Spending consumes UTXOs and creates new ones

Before Balance 3.21 BTC

sending 0.15 BTC to Bob destroys
Output of amount 0.02 BTC

After Balance 3.06 BTC

... and creates new output of
amount 0.05 BTC

0.15 BTC will be sent to Bob's address and will reside in his wallet as an output- waiting eventually to be spent. The 0.05 BTC is called change and will be send back to your wallet

Transaction as Double-Entry Bookkeeping

With the previous example it is clear that the transaction in Bitcoin is a double- entry bookkeeping

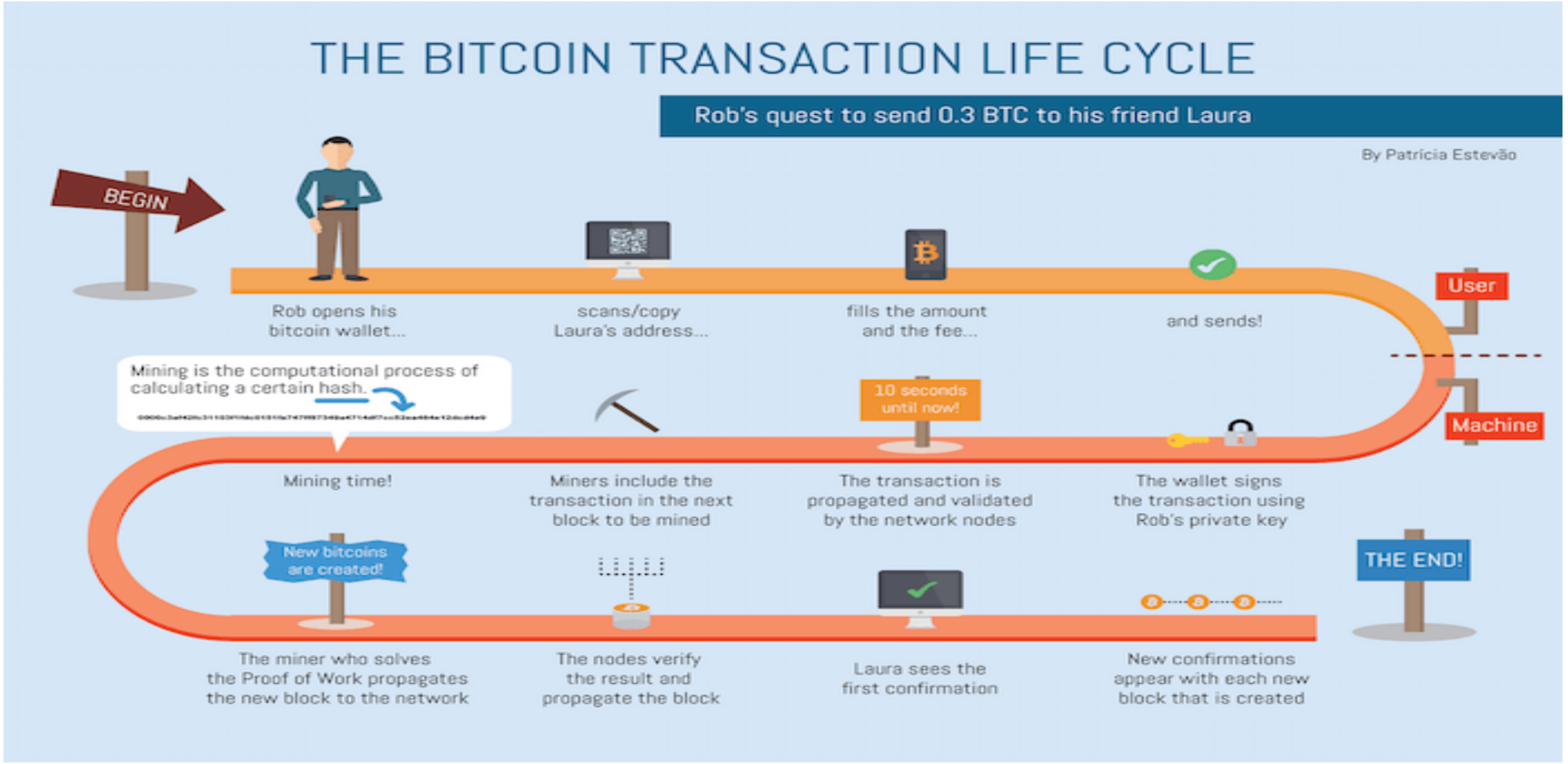
Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

Specimen of a Double-Entry Bookkeeping

Bitcoin transaction life cycle



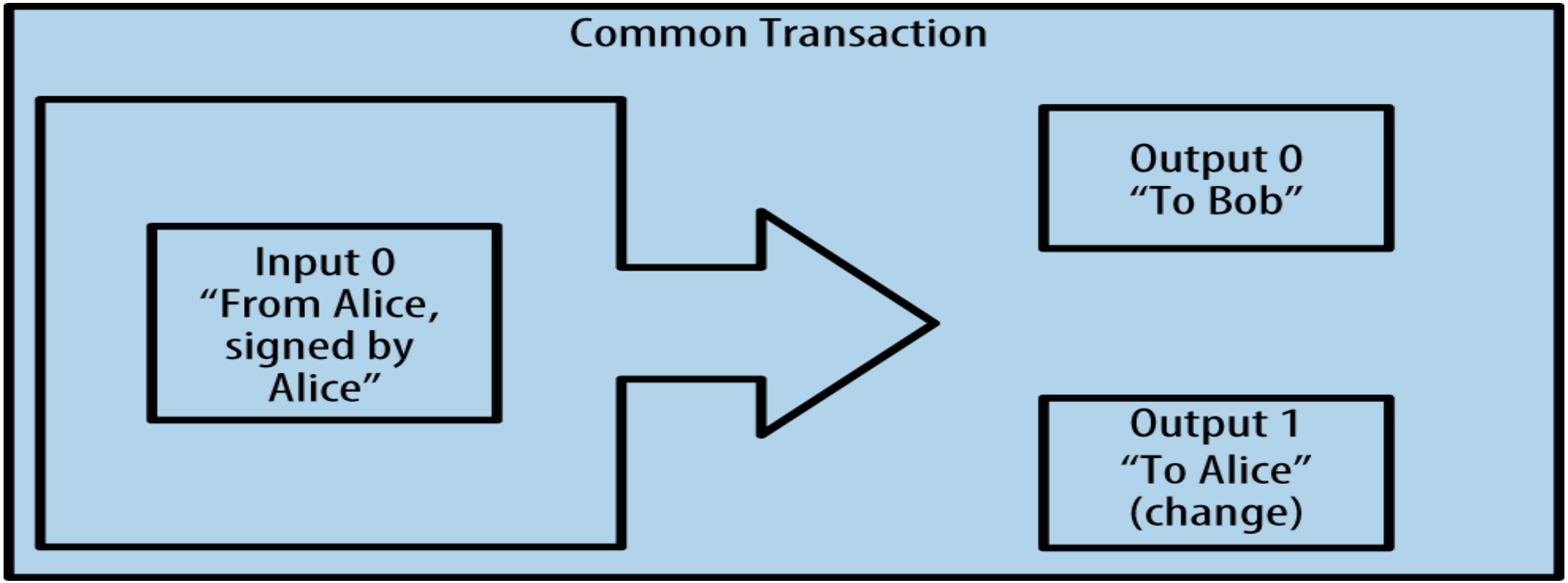
Various Transaction Forms in Bitcoin

Various Transaction Forms in Bitcoin

Let’s see what are the various types of forms used in Bitcoin transactions

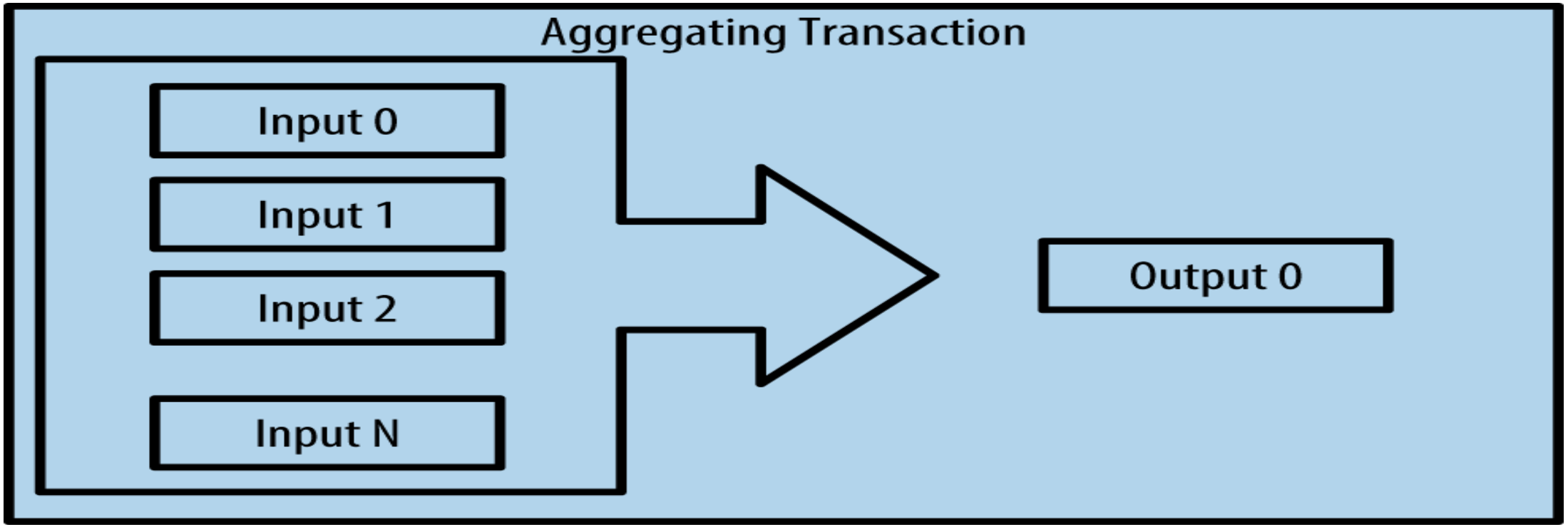
Common Transaction Form

Most common from of transaction is a simple payment from one address to another which includes some “change” returned to original owner



Aggregating Transaction

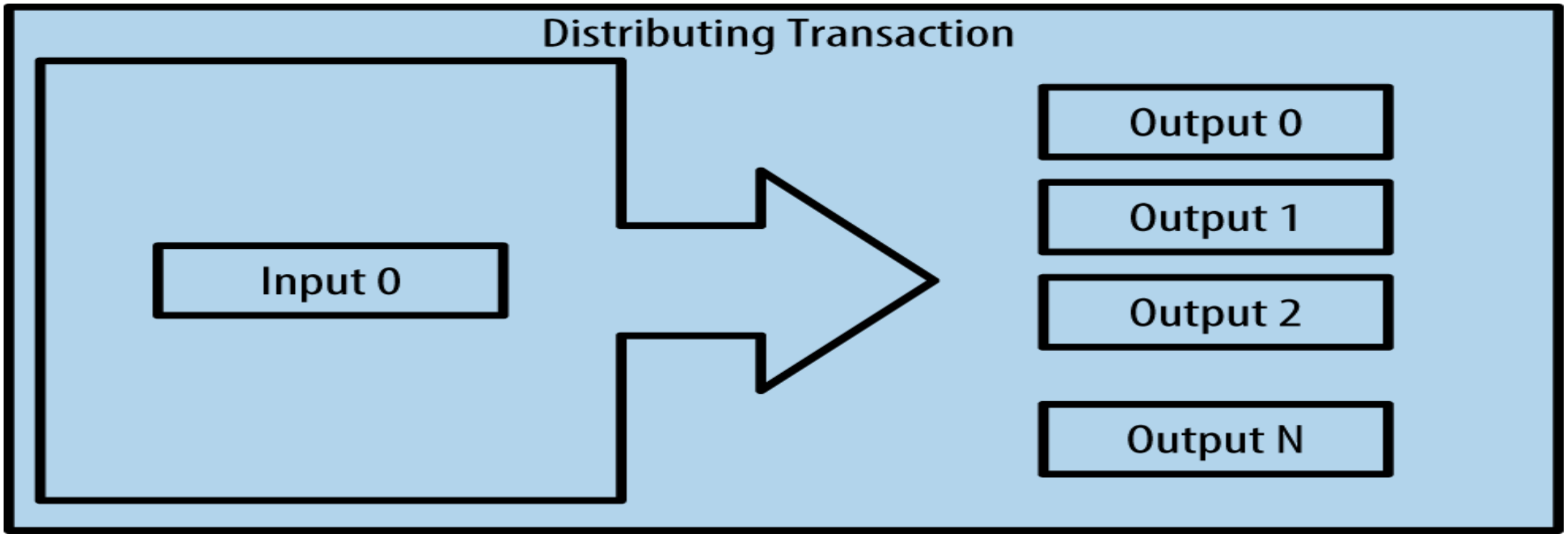
Another common form of transaction is one that aggregates several inputs into a single output



These type of transactions are sometimes generated by wallet applications to clean up smaller amounts that were received as change for payments

Distributing Transaction

Transaction that distributes one input to multiple outputs representing multiple recipients



This type of transaction is sometimes used by commercial entities to distribute funds, such as when processing payroll payments to multiple employees

Scripts in Bitcoin

Scripts in Bitcoin

> Now that we know that the transaction in bitcoin consists of Inputs and outputs. These Inputs and outputs of are nothing but the Scripts.

Bitcoin Scripting Language (“Script”)

All bitcoin transactions have scripts coded into its inputs and output mechanism

Design goals

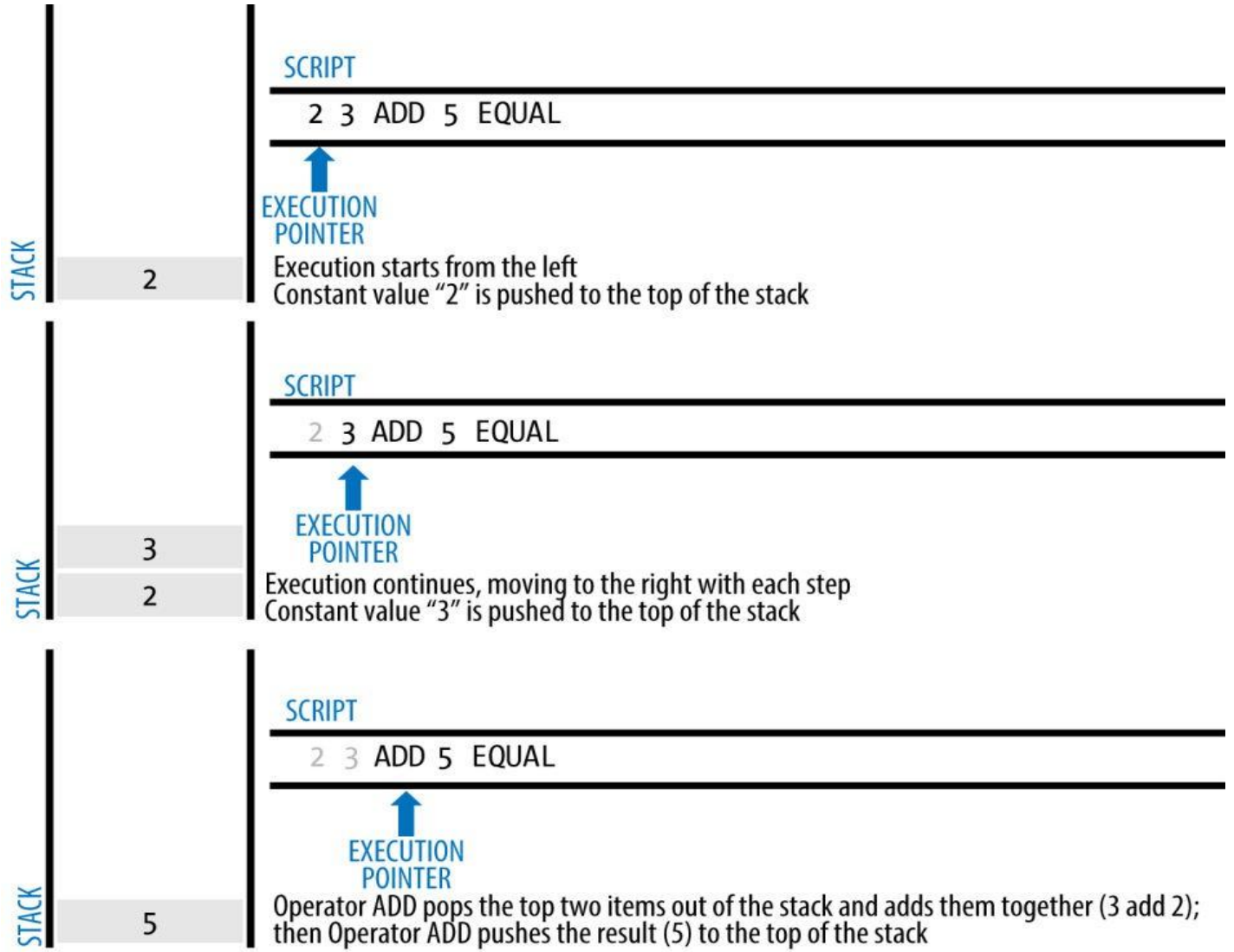
Forth like Programming Language: Old stack based simple programming language

Reverse Polish Notation: Data is pushed onto stack and operation is performed

Composed of OP_Codes: operations in bitcoin is composed of Op_Codes

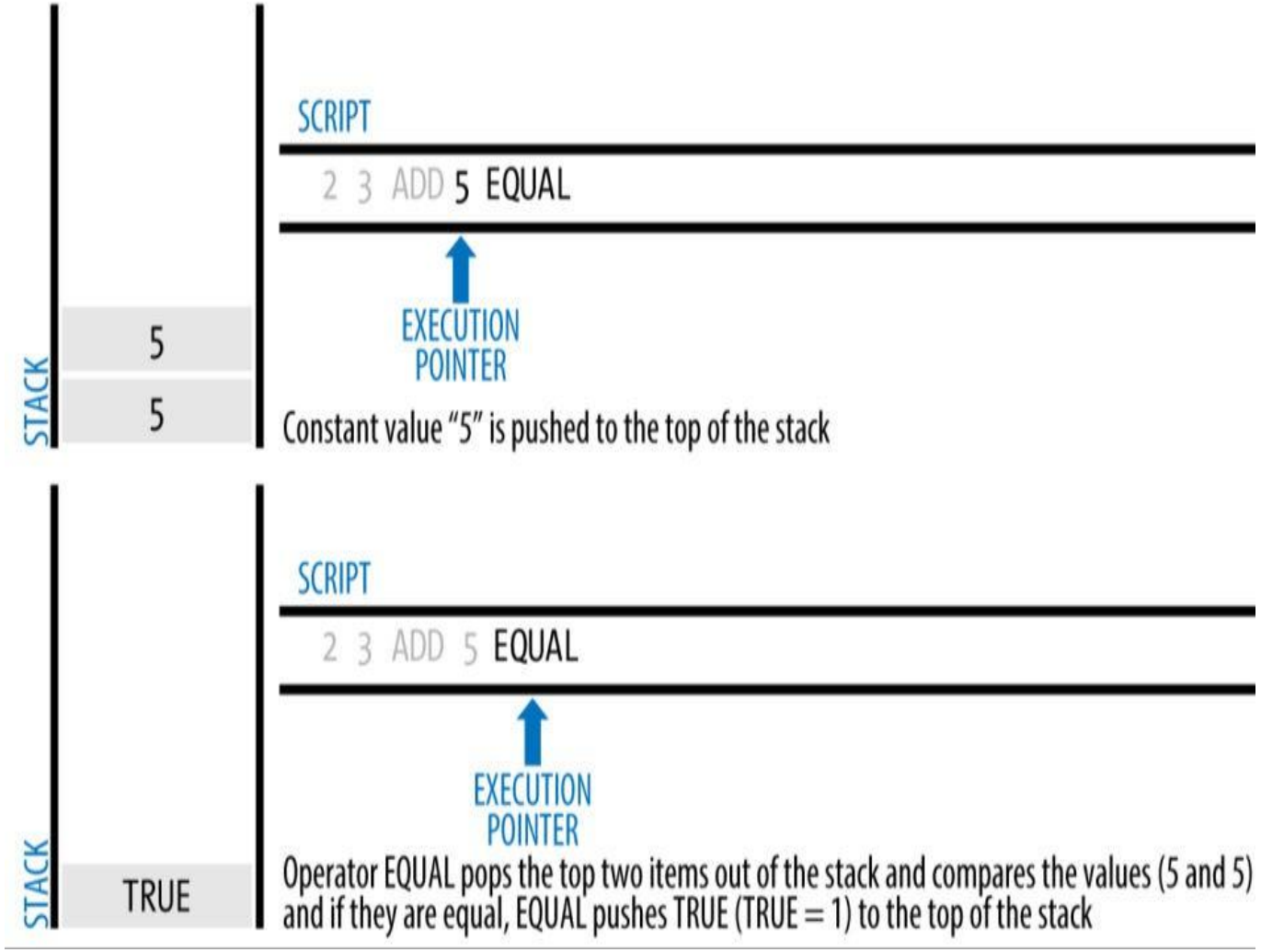
Example of Bitcoin Script

The script shown alongside will execute the values in the stack and will return to true if the equation is valid



Example of Bitcoin Script

When the script shown alongside is executed, the result is OP_TRUE code, making the equation valid



Most common Script types

Pay to Public Key Hash (p2pkh): One of the Most commonly used transaction output script. It is Used to pay to a bitcoin address

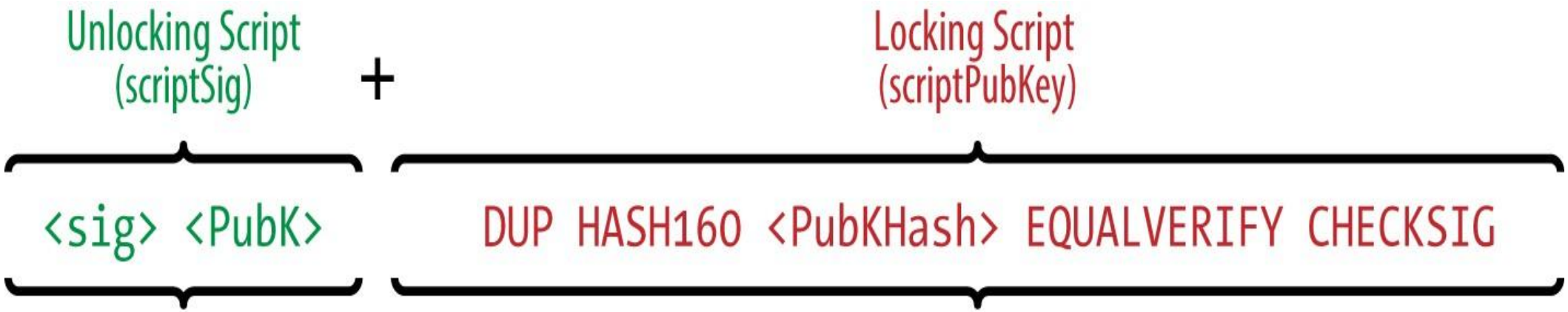
Pay to Public Key (p2pk): This is the simplified form of the p2pkh. This is not commonly used in new transactions anymore because p2pkh are more secure

Pay to Multisig (p2ms): Multisig outputs allow to share control of bitcoins between several keys

Pay to Script Hash (p2sh): scripts that contain the hash of another script, called redeemScript

Script mechanism (Lock + Unlock)

Transaction validation engine relies on two types of scripts to validate transactions:



An unlocking script

A locking script

Combining the output and Input Scripts

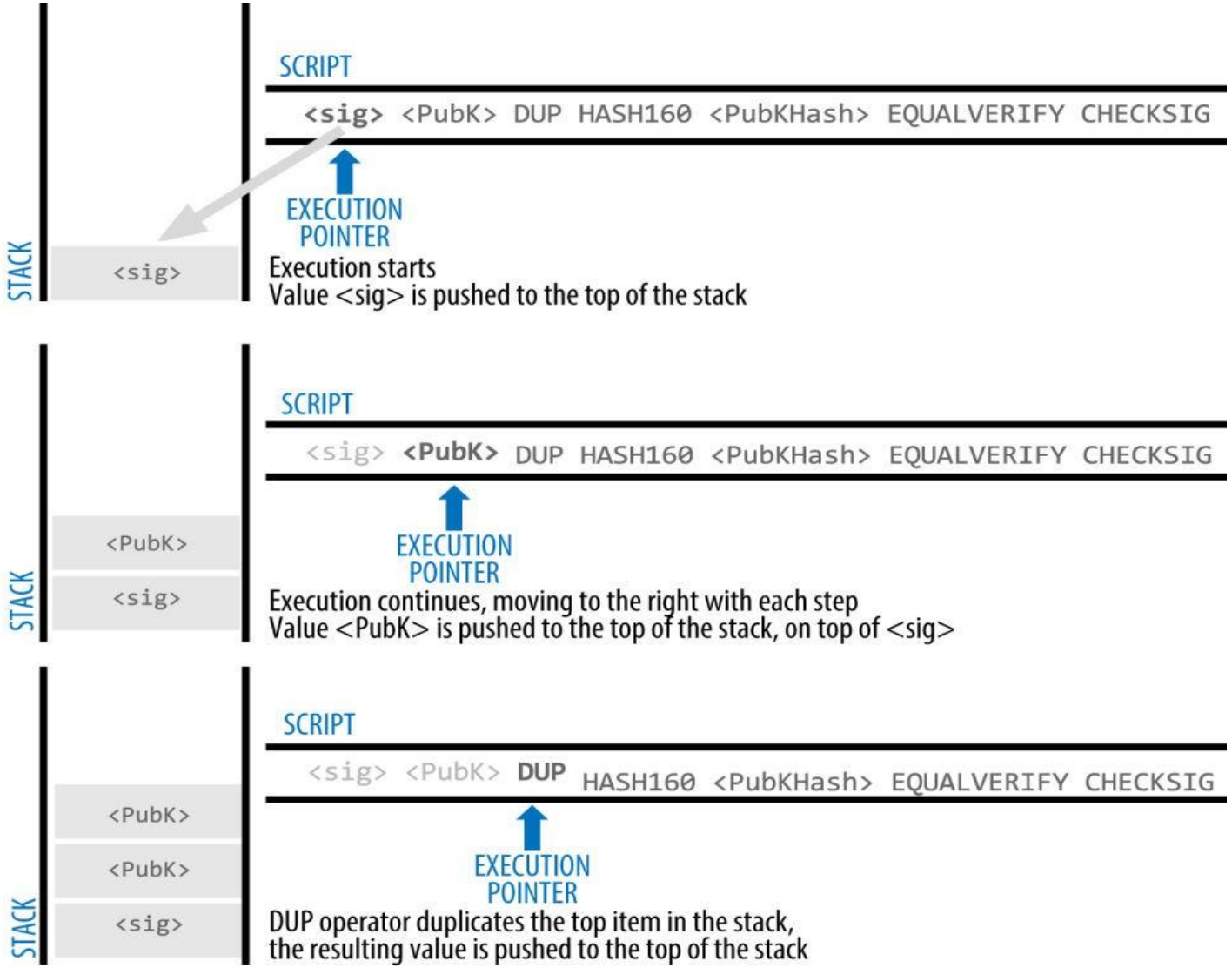
The two scripts together would form the following combined validation script:

```
<Cafe Signature> <Cafe Public Key> OP_DUP
OP_HASH160
<Cafe Public Key Hash> OP_EQUAL
OP_CHECKSIG
```

This Combined script, when executed will evaluate to TRUE if, and only if, the unlocking script matches the conditions set by the locking script

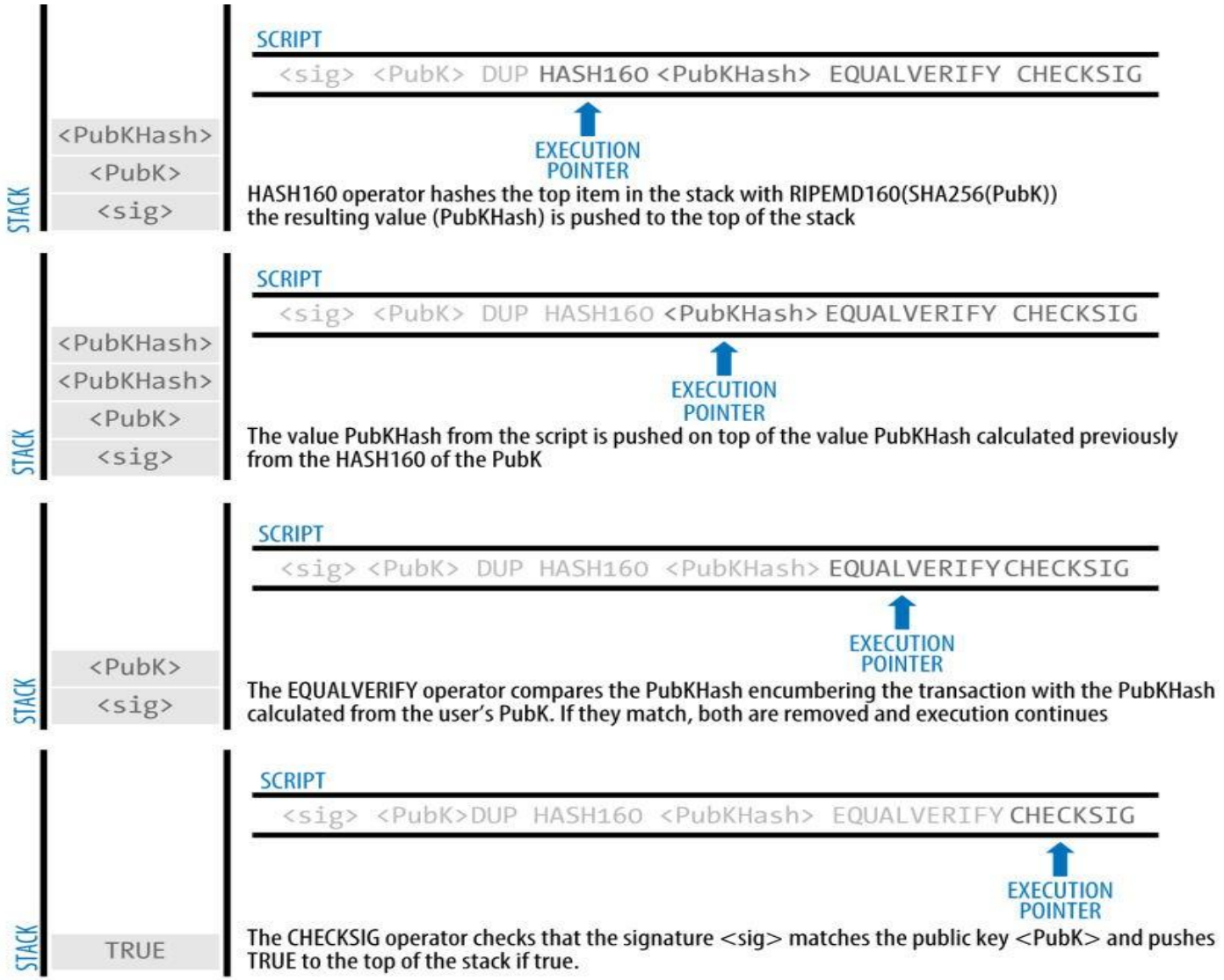
The result will be TRUE if the unlocking script has a valid signature from the cafe's private key that corresponds to the public key hash set as an encumbrance

Evaluation of the Script



A step-by-step execution of the combined script, which will prove this is a valid transaction

Evaluation of the Script



Since the script alongside returns true, thus the transaction is valid

Nodes in Bitcoin Network

Nodes in Bitcoin Network

Let’s see what are the various nodes in bitcoin network

Types of Nodes in Bitcoin

In the bitcoin network, full nodes are the enforcers of consensus rules. But not all full nodes are created equal. There are several different kinds of bitcoin full nodes which exist in the ecosystem.

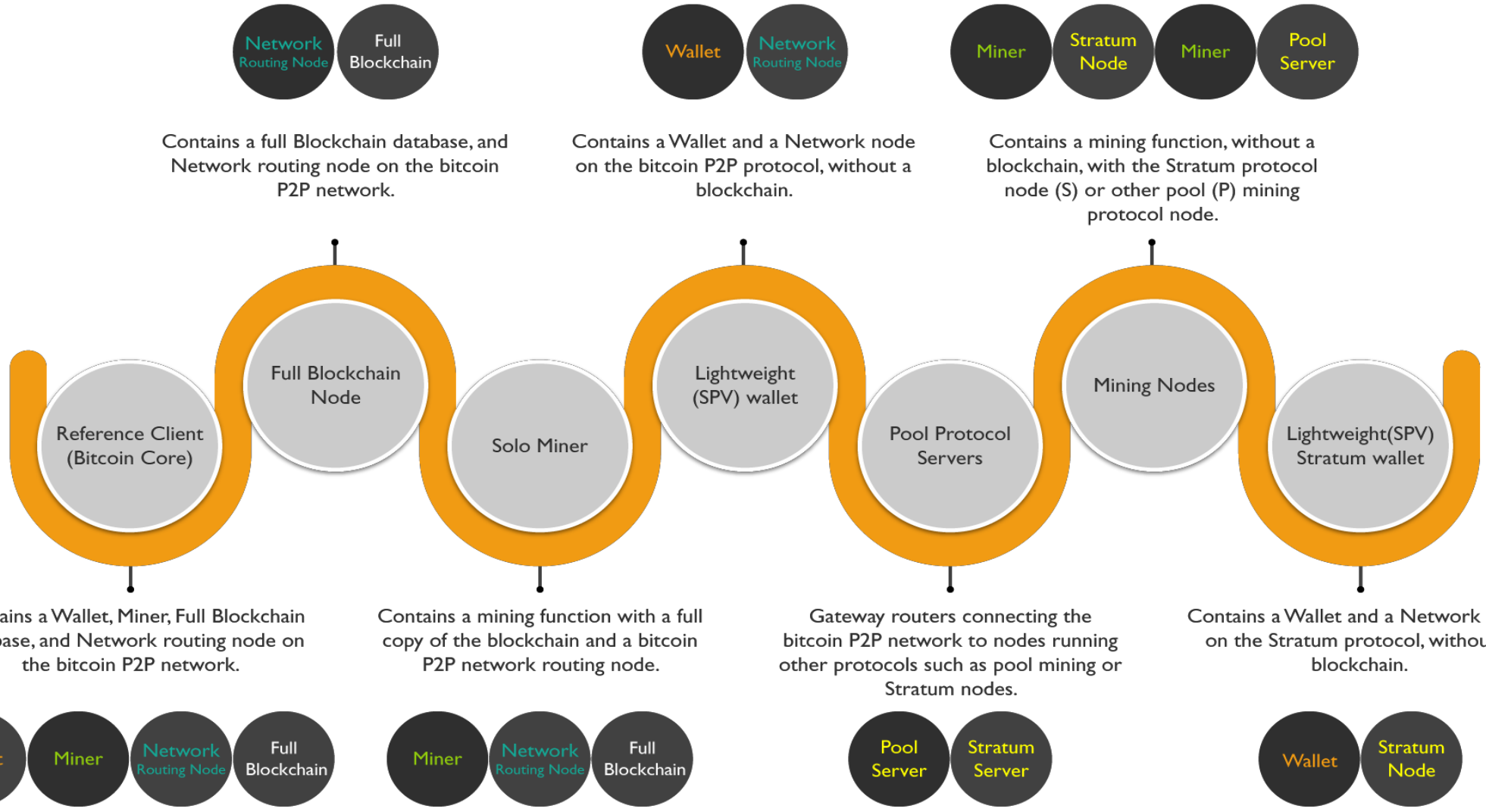
Pruned selfish full nodes

- A pruned node is a full node that “prunes” raw block and undo data by deleting it from disk. This can be achived to save disk space. A selfish bitcoin node is a node that does not upload new blocks or transactions to other bitcoin peers in the network.

Archival selfish full nodes

- An archival node is a full node that stores a complete copy of the bitcoin blockchain data on disk. With this data, the archival node operator can make queries against the blockchain to find information pertaining to particular transactions or addresses

Common Bitcoin Nodes in Bitcoin Network



Thank You

Email us – support@intellipaat.com

Visit us - https://intellipaat.com