Learn Bitcoin and Blockchain

Understanding blockchain and Bitcoin architecture to build decentralized applications

Packt

www.packt.com

By Kirankalyan Kulkarni

Learn Bitcoin and Blockchain

Understanding blockchain and Bitcoin architecture to build decentralized applications

Kirankalyan Kulkarni

Packt

BIRMINGHAM - MUMBAI

Learn Bitcoin and Blockchain

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Commissioning Editor: Sunith Shetty
Acquisition Editor: Divya Poojari
Content Development Editor: Nathanya Dias
Technical Editor: Vibhuti Gawde
Copy Editor: Safis Editing
Project Coordinator: Kirti Pisat
Proofreader: Safis Editing
Indexer: Tejal Daruwale Soni
Graphics: Jisha Chirayil
Production Coordinator: Deepika Naik

First published: August 2018

Production reference: 1280818

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-78953-613-3

www.packtpub.com

Contributor

About the author

Kirankalyan Kulkarni is a determined and highly influential author. He has more than 17 years of experience in various technologies and has more than 9 years experience in hands-on programs, delivery, and account management. He has managed teams of around 125 professionals across global locations, including entry-level developers, project managers, and architects. He researches blockchain and its underlying architecture with Hyperledger and Ethereum variants.

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

Preface

Blockchain is a distributed database that enables permanent, transparent, and secure storage of data. The blockchain technology uses cryptography to keep data secure. This book is the perfect entry point to the world of decentralized databases.

The book will take you on a journey through the blockchain database, followed by advanced implementations of the concept of blockchain. You will learn about the basics of Bitcoin and their technical operations. As you make your way through the book, you will gain insight into this leading technology and its implementation in the real world. You will also cover the technical foundations of blockchain, learn about the fundamentals of cryptography, and see how it keeps data secure. In the concluding chapters, you'll get to grips with the mechanisms behind cryptocurrencies.

By the end of this book, you will have learned about decentralized digital money, advanced blockchain concepts, and Bitcoin and blockchain security.

Who this book is for

This book is for anyone who wants to quickly understand and expand their knowledge of how blockchain and Bitcoin work and how they are applied commercially. No prior knowledge of blockchain and Bitcoin is required.

What this book covers

`Chapter 1`, *Introduction to Blockchain and Bitcoin*, will give us a step-by-step introduction to the essentials of Bitcoin and
blockchain. It will cover the basics of this unique technology, which is developing greatly. We will cover the fundamentals of cryptography and cryptocurrency, an introduction and history of Bitcoin and blockchain, its structure, the various types of blockchain, and more. This chapter will also provide the bigger picture of what makes Bitcoin and blockchain the next great innovation after the internet.

`Chapter 2`, *Fundamentals of Decentralization*, will enable us to understand the various situations in which we can use decentralization and blockchain for the benefit of society and individuals. Since this technology is completely new and undergoing changes, we hope to see a better world tomorrow that includes security and transparency while eliminating all the downsides of the technology. Towards the end of the fundamentals of decentralization, we will see how decentralization is going to impact the present and future world in a better way.

`Chapter 3`, *Advanced Blockchain Concepts*, will cover some of the advanced concepts used in blockchain and various consensus protocols used in various blockchain implementations. We will look at some of the key challenges in privacy on blockchains and how solutions such as ZKP can help safeguard privacy. Then we will discuss smart contracts, which is one of the core building blocks of blockchain: how they are written, what they are, and how they are executed.

`Chapter 4`, *Bitcoin and Blockchain Security*, will start with an introduction to the fundamentals of cryptography, and it is using cryptocurrency. We will look into the history of Bitcoin, the structure of a blockchain, and the various types of blockchain. We will get familiar with the decentralization that sits at the core of blockchain. We will get insight on how decentralization works, its pros and cons, what all can be decentralized, and how it is impacting the world today. We will also get a deeper understanding of the advanced concepts of blockchain, such as its structure, architecture, and the protocols used. Finally, this chapter will enable us to understand the features and safety provided by the various crypto wallets. We will look at how hardware wallets work, some types of physical coin, the chances of survival of the various cryptocurrencies, such as Bitcoin and Altcoin, and we will try to understand how to balance and diversify risks related to investing in crypto tokens.

To get the most out of this book

This book will give you an overview of in-depth knowledge of blockchain and Bitcoin. You need not have any prior knowledge before exploring this book. You will get well versed in how exactly the blockchain technology is implemented in today's world, and how it enables permanent, transparent, and secure data storage. This is a perfect entry point to decentralized digital databases. By the end of this book, you will know all the basic concepts and challenges of the blockchain technology, how this technology helps secure your cryptocurrency, the concepts around decentralized digital money, and also blockchain and Bitcoin security.

Conventions used

There are a number of text conventions used throughout this book.

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "This template creates a form whose superclass is `QWidget` rather than `QDialog`."

A block of code is set as follows:

```
import sys
from PyQt5.QtWidgets import QDialog, QApplication
from demoSignalSlot1 import *
class MyForm(QDialog):
    def __init__(self):
        super().__init__()
        self.ui = Ui_Dialog()
        self.ui.setupUi(self)
        self.show()
if __name__=="__main__":
    app = QApplication(sys.argv)
    w = MyForm()
    w.show()
    sys.exit(app.exec_())
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
[default]
exten => s,1,Dial(Zap/1|30)
exten => s,2,Voicemail(u100)
exten => s,102,Voicemail(b100)
exten => i,1,Voicemail(s0)
```

Any command-line input or output is written as follows:

```
C:\Pythonbook\PyQt5>pyuic5 demoLineEdit.ui –o demoLineEdit.py
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "The amount the slider handle moves can be specified via the **pageStep** property."

Warnings or important notes appear like this.

TIP

Tips and tricks appear like this.

Sections

In this book, you will find several headings that appear frequently (*Getting ready*, *How to do it...*, *How it works...*, *There's more...*, and *See also*).

To give clear instructions on how to complete a recipe, use these sections as follows:

Getting ready

This section tells you what to expect in the recipe and describes how to set up any software or anypreliminary settings required for the recipe.

How to do it…

This section contains the steps required to follow the recipe.

How it works…

This section usually consists of a detailed explanation of what happened in the previous section.

There's more…

This section consists of additional information about the recipe in order to make you moreknowledgeable about the recipe.

See also

This section provides helpful links to other useful information for the recipe.

Get in touch

Feedback from our readers is always welcome.

General feedback: Email feedback@packtpub.com and mention the book title in the subject of your message. If you have questions about any aspect of this book, please email us at questions@packtpub.com.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit www.packtpub.com/submit-errata, selecting your book, clicking on the Errata Submission Form link, and entering the details.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at copyright@packtpub.com with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit authors.packtpub.com.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit packtpub.com.

1
Introduction to Blockchain and Bitcoin

In this chapter, we will take a step-by-step approach to understanding the principles of "Bitcoin" and "blockchain", and their various features and characteristics. The buzzwords Bitcoin and blockchain relate to emerging technologies that have taken the world by storm. As we progress through the chapter, we will cover the fundamentals of these unique technologies in a detailed manner. The chapter will also take you through the essence of cryptography and how cryptocurrencies are using this innovation as a foundation. We will also look into the history of Bitcoin, the alternate cryptocurrencies available, and the various Bitcoin wallets, and we will get an understanding of the structuring of the Bitcoin block header. When it comes to blockchain, we will go through the different types of blockchain, blockchain structure, its various workings and features, the challenges faced, the various platforms available for blockchain, and more.

In this chapter, we will look into the following topics:

- Cryptography and cryptocurrency
- History and introduction to Bitcoin
- An introduction to blockchain
- Comparing private, public, and consortium blockchains

An introduction to cryptography and cryptocurrency

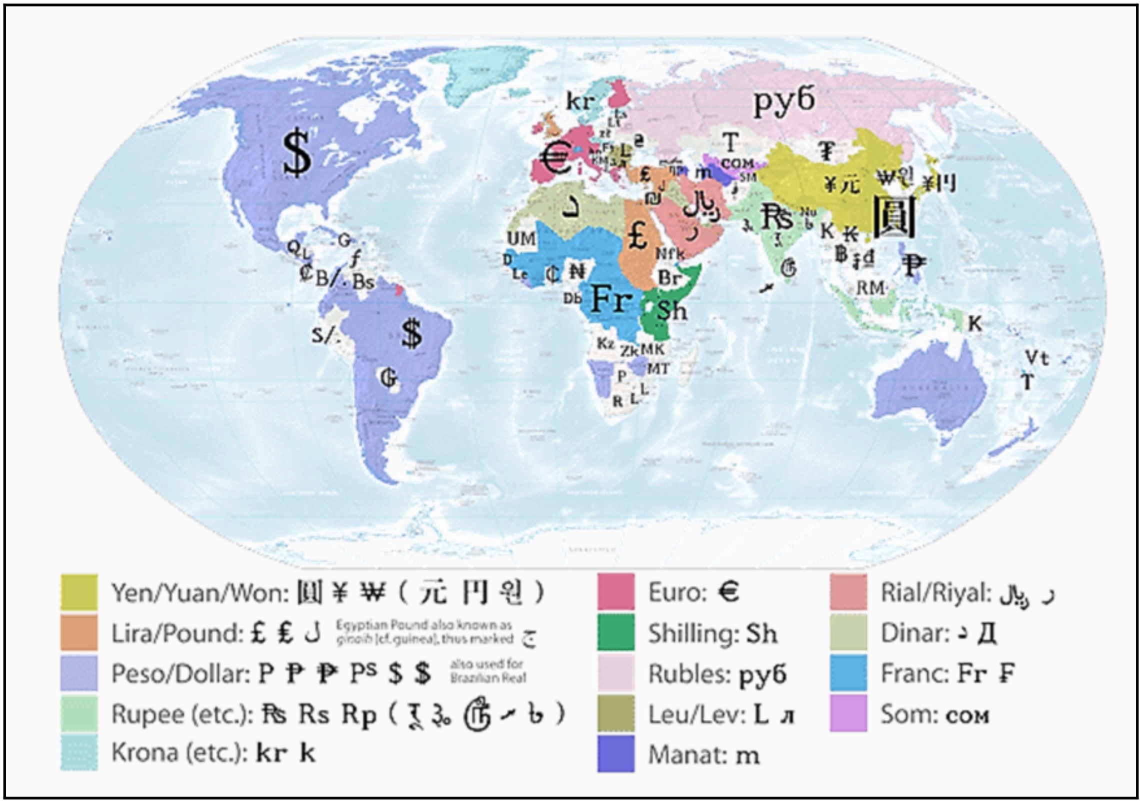
The blockchain technology is the backbone of cryptocurrency and it uses cryptography to keep the data secure. In this section of the chapter, we will discuss cryptography, cryptocurrency, and how cryptography is used in cryptocurrency implementation. We will also look into the workings of fiat currency cryptography, energy use in cryptocurrency, and also the security features of cryptography that are used. We will learn everything we need to know about decentralized digital money and its underlying architecture.

As we browse through the various parts of this section, we will learn about the history of Bitcoin, its alternative currencies, Bitcoin basics, and the technical operation of Bitcoin; then, we will browse through the technical foundation of the blockchain, the fundamentals of cryptography, and how it keeps data secure. From there, we will move on to understanding blockchain, its features, the underlying architecture on top of each Bitcoin, and how cryptocurrencies are implemented.

Workings and security of fiat currencies

Before we understand cryptocurrency, let's first look at some basic currencies used around the world. These currencies are also known as fiat currencies.

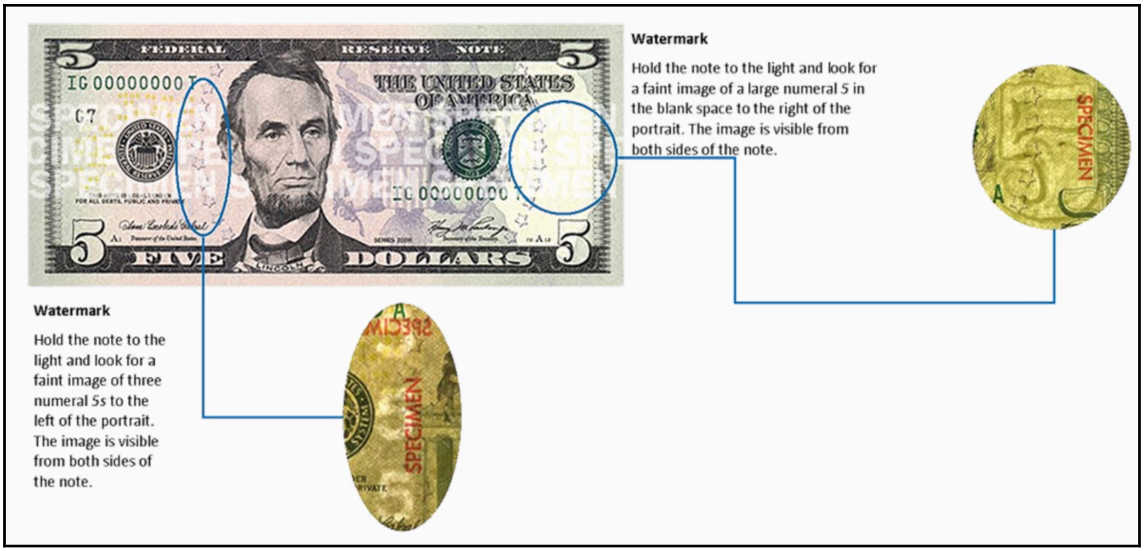
They are shown in the following diagram:


kr
руб
$
€
£
Fr
Sh
Rs
圓
₱
RM
Vt
T
UM
Nfk
Br
S/.
Bs
Yen/Yuan/Won: 圓 ¥ ₩ (元 円 원)
Lira/Pound: £ ₤ ل Egyptian Pound also known as ginaih [cf. guinea], thus marked ج
Peso/Dollar: P ₱ ₱ ₧ $ $ also used for Brazilian Real
Rupee (etc.): ₨ Rs Rp (꘡ ૱ ௹ ৳)
Krona (etc.): kr k
Euro: €
Shilling: Sh
Rubles: руб
Leu/Lev: L лв
Manat: m
Rial/Riyal: ﷼ ر
Dinar: د Д
Franc: Fr ₣
Som: сом

Some of the characteristics of fiat currencies are as follows:

- These are owned by the governments of countries
- They are centrally controlled through banks or legal entities
- They are inflationary, meaning the value of a currency decreases
- They include various security properties to prevent counterfeiting and cheating, but it is not impossible to counterfeit them

Since it is not impossible to counterfeit currencies, law enforcement comes into the picture to stop and prosecute those involved in counterfeiting fiat currencies. We will now look at various security features that are implemented in fiat currencies, as shown in the following diagram:


Watermark
Hold the note to the light and look for a faint image of a large numeral 5 in the blank space to the right of the portrait. The image is visible from both sides of the note.
Watermark
Hold the note to the light and look for a faint image of three numeral 5s to the left of the portrait. The image is visible from both sides of the note.
SPECIMEN
SPECIMEN

You will find two watermarks. You'll also see micro lettering and identification marks being implemented. Most of the time, fluorescent ink is used on notes for detecting notes that are fake.

Understanding cryptocurrency and its uses

Cryptocurrency is a very interesting and intriguing topic that has become a global phenomenon. It is different from all the currencies that are found all over the world. Right from the working of cryptocurrency, to who owns or controls it, its benefits and limitations, its use and much more, are all based on new ideas and processes. Let's now see a brief overview of the various features of cryptocurrency.

The main features of cryptocurrency are as follows:

- It is a **digital asset** used as a medium of exchange
- It secures transactions and controls supply by using **cryptography**
- It is a subset of **alternative currencies**
- In 2008, the first **decentralized cryptocurrency** was conceptualized
- Cryptocurrency is **digital money**, while the underlying technology that enables the moving of digital coins or assets between individuals is called **blockchain**

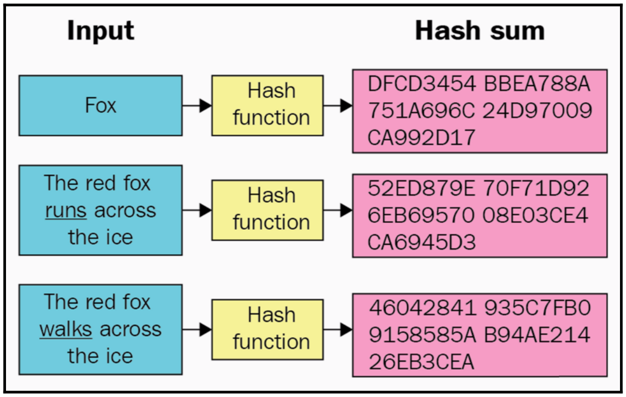
Hash function

The main cryptography techniques used in cryptocurrency are a hash function and a digital signature.

Let's look at each of these briefly. The hash function is a mathematical function with the following properties:

- Any input that we provide, be it a string, number, floating number, or anything, can be of any size
- It produces a fixed-size output such as a 128-bit hash outcome or even a 256-bit outcome
- It is collision-resistant
- It hides the data within it

Let's now look at an example of a hash function in the following diagram:


Input
Hash sum
Fox
Hash function
DFCD3454 BBEA788A 751A696C 24D97009 CA992D17
The red fox runs across the ice
Hash function
52ED879E 70F71D92 6EB69570 08E03CE4 CA6945D3
The red fox walks across the ice
Hash function
46042841 935C7FB0 9158585A B94AE214 26EB3CEA

Let's look at the hash function being used here. In the preceding diagram, we gave **Fox**, one string, as an input to the encryption module and we applied a hash function to it. It gives a specific fixed hash outcome, which is also known as a **digest hash sum**. Let's say we pass another statement that says **The red fox runs across the ice** and we apply a hash function to it. It gives us a specific hash sum, also known as a **digest**. Then, we add another statement, **The red fox walks across the ice**, and we see that it changes the hash function as the input has been changed. This is the key feature that the hash function brings.

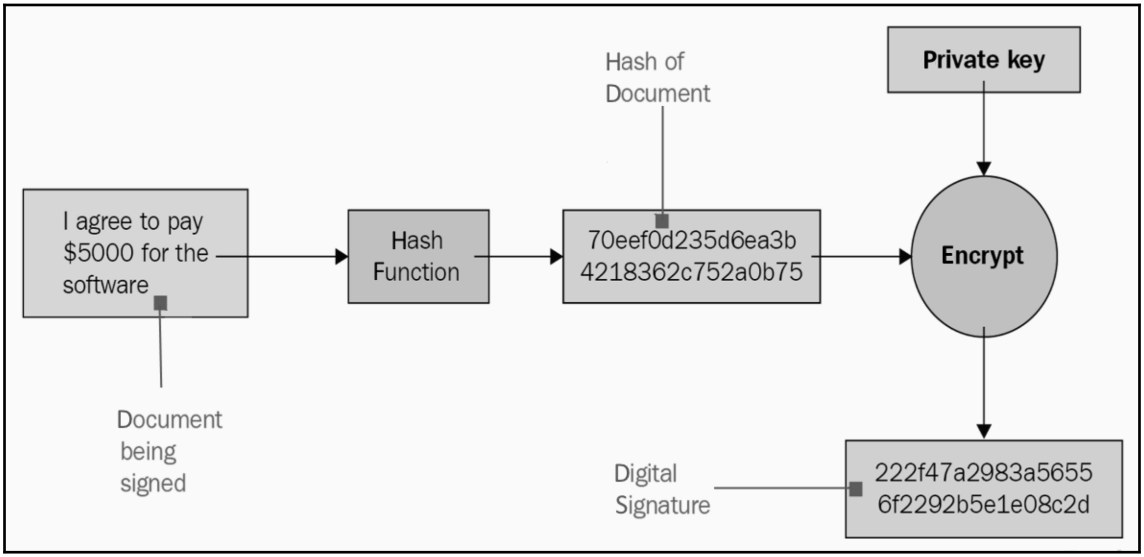
Digital signature

This is the second building block of cryptocurrency and is digitally analogous to the hand written signatures that we usually make.

The properties of the digital signature are as follows:

- You can create your own signatures, but they can be verified by another person too
- The signature is tied to a particular document or message so that it cannot be used again and again for different documents and messages

Let's now look at an example of a digital signature in the following diagram:


Hash of Document
Private key
I agree to pay $5000 for the software
Hash Function
70eef0d235d6ea3b 4218362c752a0b75
Encrypt
Document being signed
Digital Signature
222f47a2983a5655 6f2292b5e1e08c2d

Let's take an example and say that there is a string in the document which states that "**I agree to pay $5000 for the software**". Since this is the document that is being signed, we first apply a hash function to it. It gives us a hash or digest of the document, which is again fixed in size. Then, we apply our private key, or a specific key, to encrypt it and we get the outcome as a digital signature. This digital signature is signed specifically for this input, which states that "I agreed to pay $5,000 for the software".

Here, we saw how cryptography and cryptocurrency are digital assets that are widely used. We also saw how cryptocurrency uses cryptography and its techniques, such as hash functions and digital signatures.

An introduction to Bitcoin

Bitcoin is the first decentralized digital currency, and as such it is a revolutionary technology invention. It changed the way we compute things and the way we operate software and computers. Bitcoin and blockchain are considered to be the next big wave of change after the internet.

Now, let's look at the following properties of Bitcoin:

- It's an international network of payments.
- It uses cryptography to control its creation and management, rather than relying on central authorities such as governments, banks, union territories, or intermediaries.
- It's not printed but is produced by people using software that solves mathematical problems.
- It is controlled and limited in supply, which arrests the hyperinflation problem. For example, whenever African countries were short of currency notes, they had to print more notes, which resulted in hyperinflation and brought the value of the currency down.
- Since the arrival of Bitcoin, the way Bitcoin programs are written means there will always be a maximum of 21 million Bitcoins available across the globe. The moment 21 million Bitcoins have been mined, the program will not generate any more new Bitcoins. Hence, Bitcoins will be limited in supply and this will arrest the problem of hyperinflation.

History of Bitcoin

Bitcoin was conceptualized by Satoshi Nakamoto in 2008. We do not know whether it is a person or a group of people. This anonymous person or group of persons still remains a mystery. What we know is that Nakamoto has claimed to be a man living in Japan born on April 15th, 1975. However, there are a lot of theories and speculation about the identity of Nakamoto. Some people say that the identity of Nakamoto is based on a number of cryptography and computer science experts living in the US and the EU, not necessarily Japanese people. In November 2017, Nakamoto was believed to own up to roughly 1 million Bitcoins, the value of this 1 million comes to be 7.2 billion US dollars, which is a huge amount of money owned by someone who is not known to anybody in the world.

Alternative cryptocurrencies to Bitcoin

Altcoins is an alternate cryptocurrency to Bitcoin. Once Bitcoin became popular, people realized the value, robustness, and flexibility Bitcoin brought and also started liking the fact that Bitcoin appreciated in value. They simply took the source code of the Bitcoin protocol available from GitHub repositories, forked it, modified it as per their needs, and created alternative cryptocurrencies. With the increasing popularity of Bitcoin, the usage and rate of Bitcoin have skyrocketed. Leaving that aside, the next question that arises is "how do we store or possess this virtual currency securely in digital form?".

Bitcoin wallets

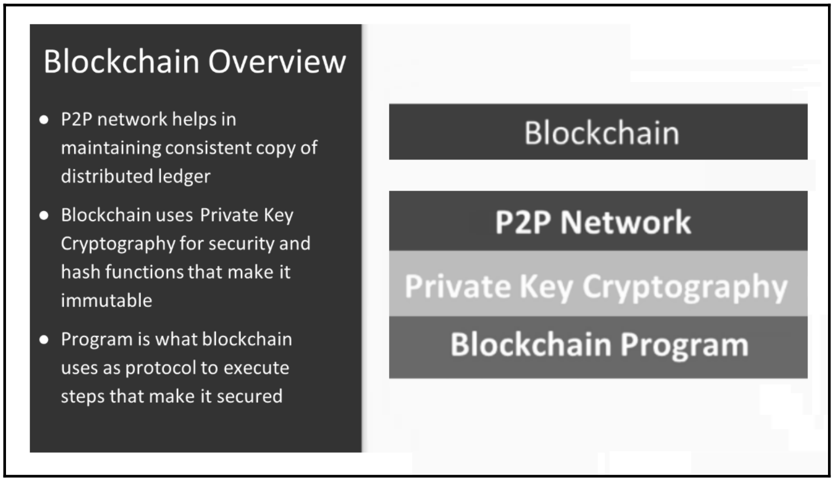
There are several types of wallet available, in which we can hold our Bitcoins safely. Each of these wallets has their own function and ways to operate.

The different kinds of the wallet are as follows:

- **Software wallet**: The software wallet is a Bitcoin application that sits on your computer's hard drive and allows you to completely control and secure your Bitcoins. Bitcoin Armory is an example of a software wallet and is supposed to be the most stable and secure wallet of all.
- **Web wallet**: The next type of wallet is a web wallet. Web wallets are more convenient than software wallets since they can be accessed to use your funds, Bitcoins, or assets from any device. So, you can access your web wallet on your Android or iOS device, your desktop and even on the internet.
- **Cold wallet**: The next type of wallet is called a cold wallet. Cold wallets are simply any kind of Bitcoin wallet that is not connected to the internet. These can be in paper form, or you can have wallets on USB drives as well.
- **Brain wallet**: The next type of wallet is the brain wallet. The brain wallet has its address generated by a computer program by hashing the passphrase with words that the user enters.
- **Hardware wallet**: The next type of wallet is the hardware wallet. The hardware wallet can only be accessed through physical contact with the wallet by the designated person, who owns the wallet. It stores the user's private keys in a secure hardware drive that is accessible only to the user and usually uses a fingerprint scanner or biometrics to access it.

An introduction to the blockchain

In this section, we will look at the architecture of blockchain, how it works, and what the salient features are that make it so disruptive. Blockchain was created by Satoshi Nakamoto as an infrastructure for Bitcoin and it is treated as the biggest thing since the internet. Blockchain, at a high level, consists of three major components, which are shown in the following diagram:



Blockchain Overview

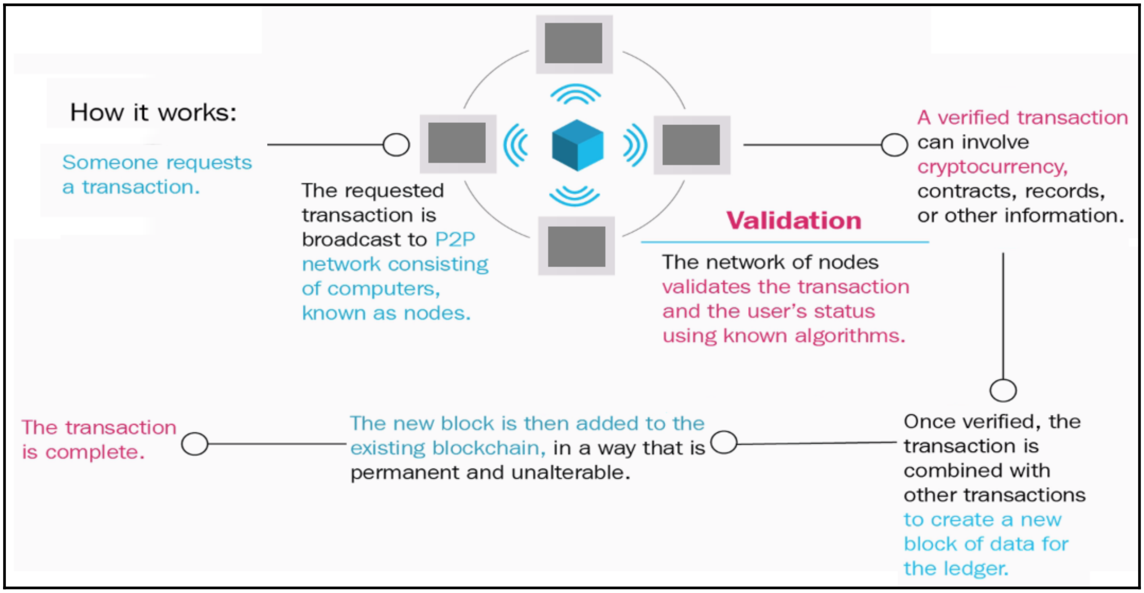
- P2P network helps in maintaining consistent copy of distributed ledger
- Blockchain uses Private Key Cryptography for security and hash functions that make it immutable
- Program is what blockchain uses as protocol to execute steps that make it secured

Let's now look into the following three major components of blockchain:

- **P2P Network**: A **peer-to-peer network** (**P2P**) helps maintain a consistent copy of the distributed ledger. All the transactions that are captured on the blockchain in the form of blocks are maintained across the network of nodes running the blocks and programs by the distributed ledger.
- **Private Key Cryptography**: This component is used by blockchain for the security and hash functions that make it immutable.
- **Blockchain Program**: This component is used by blockchain as a protocol to execute steps that make it secure.

Workings of blockchain

Now, let's look at how a blockchain implementation works and what all the things are that are involved in completing the flow of execution. Let's take the example of a Bitcoin, shown in the following workflow for blockchain:


How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

In the preceding diagram, we see how blockchain works and the steps mentioned are as follows:

1. Let's say someone requests a transaction in Bitcoin; for example, person A wants to send Bitcoin to person B. That person or entity requests a transaction that results in debiting person A's wallet and crediting person B's wallet with one Bitcoin.
2. Now, this requested transaction is broadcasted to the P2P network, consisting of computers known as nodes, which are spread across the globe.
3. Now, once the transaction is propagated, the transaction is picked up by the network of nodes, they validate the nodes that are running the blockchain programs, and they validate the transaction and the user status using known algorithms that are common across all nodes.
4. In our example, we talked about person A sending one Bitcoin to person B, which involves the cryptocurrency as well. The verification part also involves checking whether person A initiating the transaction for one Bitcoin really owns that Bitcoin or not.

One must avoid double booking and fake transactions altogether. Verification may also involve contracts, records, agreements, or documents that need verification.

5. Once verified, the transaction is then combined with other transactions to create a new block of data for a ledger. This freshly created block of a series of transactions then gets added to an existing blockchain in a way that is permanent (it's unalterable).
6. With this block added to the blockchain, the transaction is complete.
7. Once the block is added, it remains there for the rest of the blockchain's life.

Features of blockchain

We will now discuss the following features of blockchain:

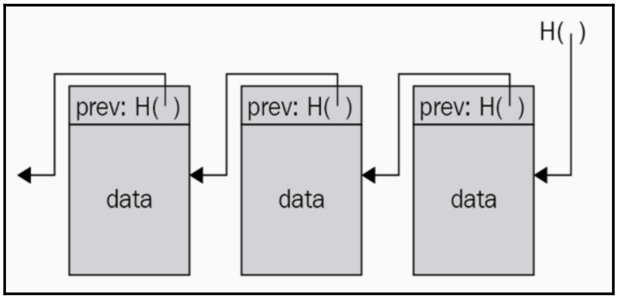
- **Secure**: It is really impossible for anyone to tamper with transactions or ledger records present in the blockchain, which makes it more secure, so it is seen as a reliable source of information.
- **Global reach**: Blockchain has been adopted worldwide and has the backing of many investors from banking and non-banking sectors, which makes it a globally accepted technology stack.
- **Automated operations**: Operations are fully automated through software. Private companies are not needed to handle operations, which is why there is no mediation required to carry out the transactions, and trust is assured, so people can carry out their own transactions.
- **Open source**: Blockchain is an open source technology. All the operations are carried out by the open source community.
- **Distributed**: Blockchain works in a distributed mode, in which records are stored in all nodes in the network. If one node goes down, it doesn't impact any other nodes or any other records, because they are globally distributed across all the nodes.
- **Flexible**: Blockchain is programmable, using basic programming concepts and programming semantics, which makes blockchain very flexible.

Structure of blockchain

In this section, we will learn about the following aspects of blockchain: its structure; its building blocks; and its core parts that make it disruptive, robust, strong, and tamperproof.

Let's have a look at the structure of the blockchain. The blockchain structure is very similar to that of **linked lists** or **binary trees**. Linked lists or binary trees are linked to each other using pointers, which point to the previous or next list elements on the nodes in the linked list. The structure of blockchain is not really different from that of binary trees, but the major difference is that blockchain is tamperproof and it is also very easy to find out if any tampering has taken place.

In the following diagram, we will look at a representation of how blockchain is constructed and how it is a linked list:

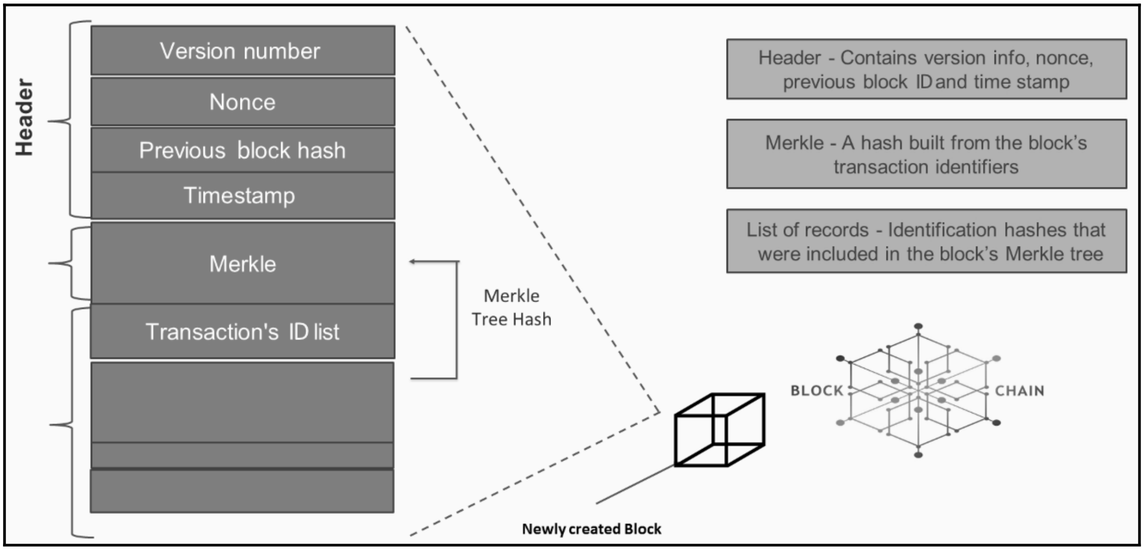


Let's now discuss the structure and elements of the blockchain.

The blockchain is a linked list that is built with hash pointers instead of pointers. This is the exact reason why blockchain, though it resembles a linked list, is different because, in the linked list we have been using the pointers to point to previous nodes for the elements in the lists, but in the case of the blockchain, the pointers are hash pointers and not just simple pointers.

So, typically, any block in the blockchain consists of three parts, or feet such as a **Header**, **Merkle**, and **Transaction's Id list**. This is a newly created block.

We can see the structure of blockchain in the following diagram:


Header
Version number
Nonce
Previous block hash
Timestamp
Merkle
Transaction's ID list
Merkle Tree Hash
Header - Contains version info, nonce, previous block ID and time stamp
Merkle - A hash built from the block's transaction identifiers
List of records - Identification hashes that were included in the block's Merkle tree
BLOCK
CHAIN
Newly created Block

We will now look into the following blocks and their elements:

- **Header**: This block contains the version information of the block, the nonce, the previous block ID, and the timestamp that is being hashed again at the time the block is created.
- **Merkle**: This block is a hash built from the block's transaction identifiers.
- **Transaction's Id list**: This block represents the transactions themselves. It's a list of records, identification hashes, that are included in the block's Merkle tree.

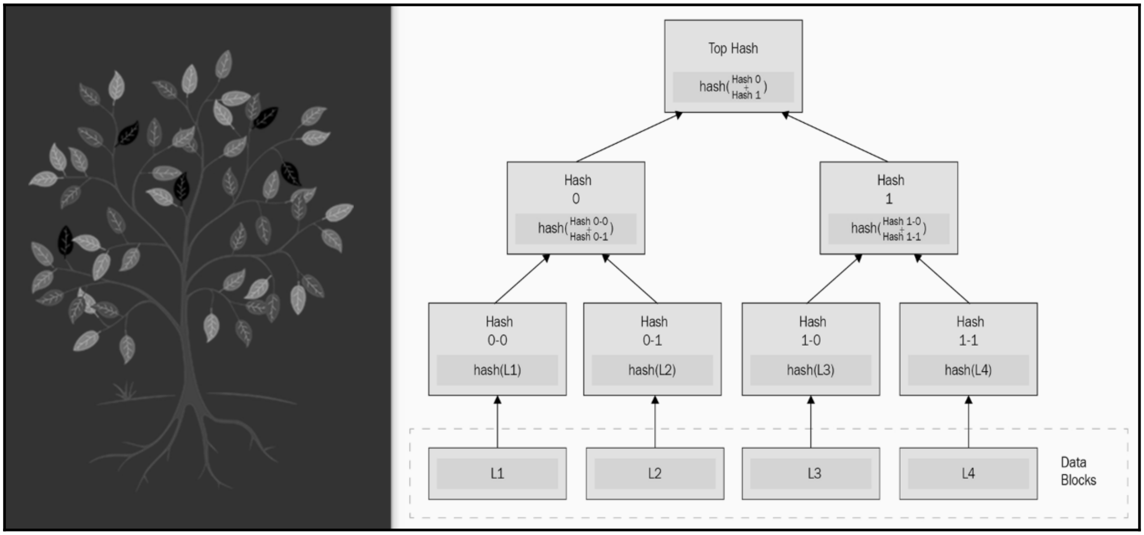
The block is then created with all of the preceding details. This newly created block gets added to the blockchain.

Now, let's look at what the Merkle tree is, as follows:

- In the blockchain structure, it's also known as a binary hash tree. It's a data structure used for summarizing and verifying the integrity of large sets of data.
- It not only summarizes the data that is being captured on a particular block, but it also verifies the integrity of the data, which makes sure that the data represented in the block is integrated and not tampered with. It contains cryptographic hashes, which are used to make sure integrity is maintained across the block.

- It's an upside-down tree where the root is at the top and the leaves are at the bottom.

Now, let's look at a representation of the Merkle tree in the following diagram:



Here is a brief overview of what the top hash, data blocks, and Merkle root stand for, as follows:

- In the preceding diagram, we can see **Top Hash,** which is the root of the Merkle tree, and there are leaf nodes or leaves that make up the entire tree.
- **Data Blocks** are transactions that have been captured and hashed. They are paired and hashed multiple times, and that's how you reach the top of the Merkle tree.
- A block of one or more new records is collected, and such records are then paired and hashed together multiple times until a single hash remains. This single hash is called the **Merkle root** of that Merkle tree.

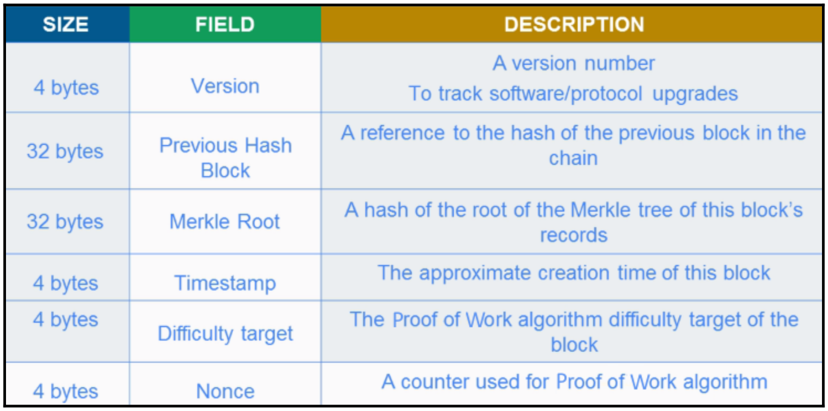
If any change or tampering occurs in any part of the transaction data, we can see this compromise in a bold and clear manner. Hence, the Merkle tree is important in the implementation of blockchain and is a major contributor to making sure that blockchain data has not been tampered with.

Structuring the Bitcoin block header

Now, we will look into the structure of the Bitcoin block header, in which the header consists of a block and each block holds the following three sets of block metadata:

- A reference to a previous block hash
- The difficulty, timestamp, and nonce parts of the header
- The Merkle root

Let's look at the various terms represented in the following diagram:



SIZE	FIELD	DESCRIPTION
4 bytes	Version	A version number To track software/protocol upgrades
32 bytes	Previous Hash Block	A reference to the hash of the previous block in the chain
32 bytes	Merkle Root	A hash of the root of the Merkle tree of this block's records
4 bytes	Timestamp	The approximate creation time of this block
4 bytes	Difficulty target	The Proof of Work algorithm difficulty target of the block
4 bytes	Nonce	A counter used for Proof of Work algorithm

The following is an elaboration of the terms mentioned in the preceding diagram:

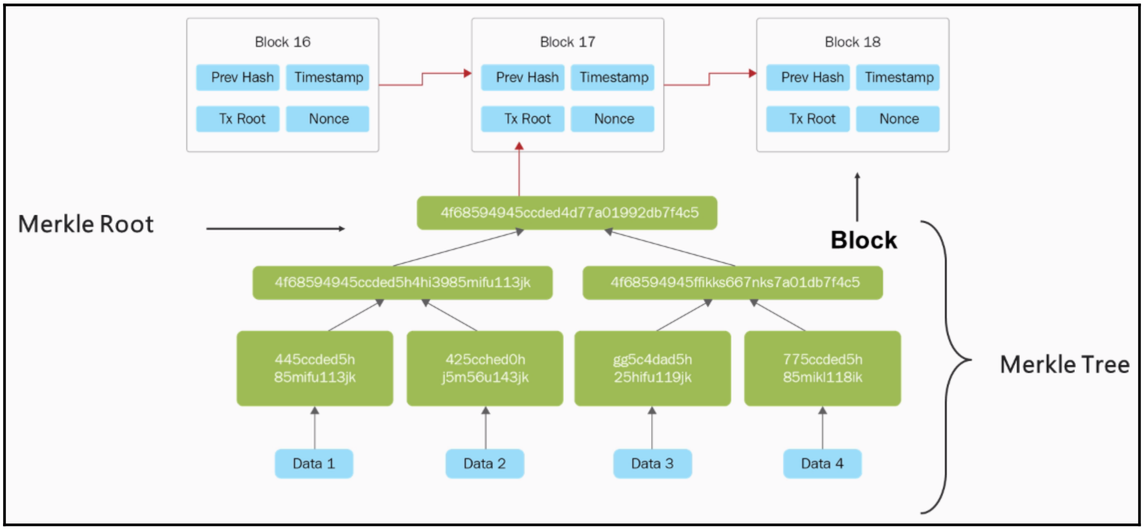
- **Version**: The first part of the header is the **4 bytes** of version. A version number tracks software protocol upgrades. It is really important to capture that data as part of the block itself because, if there are any changes made in subsequent versions of the program, it becomes necessary to capture which program or node is running each program to send the transactions and blocks across the internet.
- **Previous Hash Block**: The second part of the header is the **32 bytes** previous hash block or previous hash block code. It's a reference to the hash of the previous block in the chain. It's not just a link to the previous block, it's a hashed pointer to the previous block, which makes sure that the new block added maintains the sequence of the blocks or the chain.
- **Merkle Root**: The third part of the header is the **32 bytes** of the Merkle root. We just looked at the Merkle root, which is a hash root of the Merkle tree. It is a final hash code of all the transactions that were captured as part of the block.

- **Timestamp:** The fourth part of the header is the **4 bytes** of timestamp. It is the approximate time taken for the creation of this block. We use the term approximate because once the block is created, it takes a few milliseconds to get added to the actual blockchain as the transactions are verified by different nodes.
- **Difficulty target**: The fifth part of the header is the **4 bytes** that capture the difficulty target. It's the proof of work algorithm of the blocks. It is given for a particular node that is running the Bitcoin blockchain program.
- **Nonce**: The sixth part of the header is **4 bytes** of the nonce. It is the counter used for the **Proof of Work** (**PoW**) algorithm. Whichever node is first in calculating and solving the mathematical problem actually yields the result of the problem-solving solution and the result contains this nonce, which is used to capture the transaction and verifies that the PoW being carried by the node is correct.

Thus, we can see that this is the typical structure of a Bitcoin block header, which is roughly 80 bytes of information that is captured in each of the blocks.

Representing the blockchain structure

Now, we will look at the overall structure of the Bitcoin blockchain header in the following diagram:



In this example, **Block 16** represents the previous block's hash and consists of the timestamp of creation, the transaction root is also known as the Merkle root, and the nonce is the algorithm-cum-counter that has to be verified. All of the hidden information on the transactions is hashed again, and that hash is captured in **Block 17**. It consists of the previous block's hash, the timestamp, the Merkle root, and the nonce.

In the sections for **Data 1**, **Data 2**, **Data 3**, and **Data 4** in the preceding diagram, all the data is paired and hashed multiple times. Thus, the data keeps going in the upward direction until it gets to one final hash. These blocks keep moving and the entire Merkle tree is formed by the transactions that are captured in the blocks. This is what makes it so strong, robust, tamperproof, integrated, and immutable. This is the beauty of blockchain.

Challenges with blockchain

After looking at the building blocks, structure, and core parts of the blockchain, we are now going to learn about the various types of blockchain implementations available, and we will also look at their features and benefits. As we already know, the Bitcoin blockchain became popular for its immutability, security, robustness, and transparency. The industry was in need of the Bitcoin blockchain architecture, but there were challenges that came up.

The challenges faced by the industry are as follows:

- **How will it cater to an enterprise's specific needs**: We know that the Bitcoin blockchain is open source, which is open to all kinds of solutions. If the IT industry or various enterprises wanted to use this blockchain architecture, they would not be able to use it as their needs are different.
- **How can we use other currencies with blockchain**: Enterprises that were willing to use the blockchain architecture due to its immutability, security, and transparency wanted to track their own assets, which wasn't possible in Bitcoin blockchain as it was using Bitcoin and other Altcoins as currency.
- **How will it allow us to define specific roles and permissions on the blockchain**: Different enterprises have their own roles, privileges, and permissions that have to be captured and executed on the blockchain nodes. In the case of the Bitcoin blockchain, we know that each and every node plays the same role across the globe.

So, these challenges triggered the need for specific changes to blockchain for industries, enterprises, and IT companies, in order to use blockchain for their own purposes, which in turn gave birth to different blockchain versions or variants.

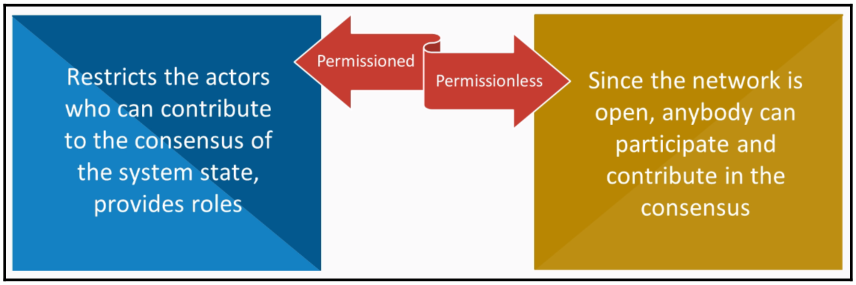
Types of blockchain

Let's have a look at the following types of blockchain:

- **Public**: Public blockchains have ledgers visible to everyone on the internet and anyone can verify and add a block of transactions to the blockchain. Some examples are Bitcoins, Ethereum, Dash, Factom, and the hundreds of Altcoins that are available in the market today.
- **Private**: The second type of blockchain is the private blockchain. All permissions are kept centralized to an organization. Private blockchains allow only specific people with specific roles in the organization to verify transaction blocks, but everyone on the internet is allowed to view them. This also depends on the organization's decision. Some examples are **MultiChain** and **Blockstack**.
- **Consortium**: The third and most popular type of blockchain is a consortium. It's controlled by a consortium of members. These members are from top companies who came forward to make changes to blockchain for specific purposes. So, only a predefined set of nodes have access to write data or blocks to the blockchain. Some examples are **Ripple**, **R3**, **Hyperledger 1.0**, and **Hyperledger 2.0**.

Permission and permissionless blockchain implementations

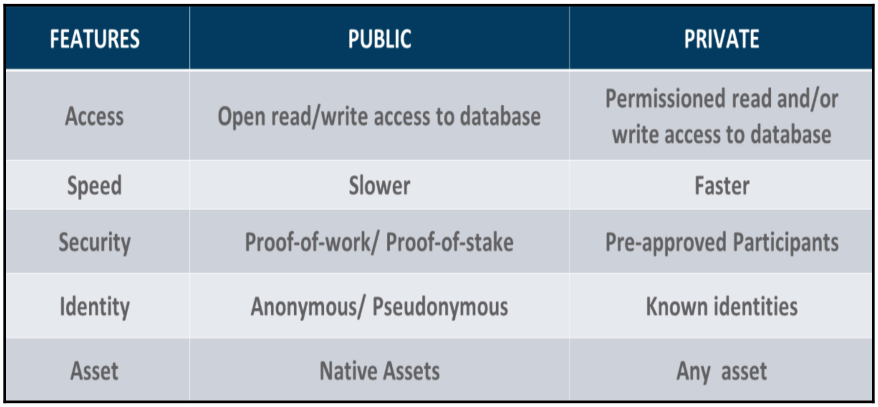
Now, let's look at the difference between a **permission** and a **permissionless** blockchain implementation, shown in the following diagram:


Restricts the actors who can contribute to the consensus of the system state, provides roles
Permissioned
Permissionless
Since the network is open, anybody can participate and contribute in the consensus

Let's explore the difference between a permission and a permissionless blockchain as follows:

- **Permissionless blockchain**: Since the network is open, it's called a permissionless blockchain. Anybody can participate and contribute to the consensus. Now, the consensus varies in all the nodes that are participating in blockchain mining. Even one individual can set up the mining and start running the blockchain implementation. It's a public network, that is available for everyone to play a specific role, or rather, a generic role.
- **Permission blockchain**: It restricts the actors who can contribute to the consensus of the system state and provides role-based access to the blockchain for actors who are participating in the implementation.

The following table depicts the difference between the public and private blockchains:



FEATURES	PUBLIC	PRIVATE
Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Proof-of-work/ Proof-of-stake	Pre-approved Participants
Identity	Anonymous/ Pseudonymous	Known identities
Asset	Native Assets	Any asset

So, let's take a look at the following features that are being provided by these implementations:

- **Access**: In terms of access, the public blockchain is open with read and write access to the database for any node that is running the blockchain implementation. On the other hand, the private blockchain needs permission to have read or write access to the database.
- **Speed**: In terms of speed, the public blockchain is slower. The reason for this is that it's public and the volume, size, and number of nodes that participate in the blockchain are higher, so it takes some time to capture the transactions. When it comes to private blockchains, they have specific roles which are played by limited nodes that help to make the implementation of the transaction faster.

- **Security**: The way the public blockchain works is on the premise of PoW or the **Proof of Stake** (**PoS**), while the security in the private blockchain is provided by preapproved participants that can only participate or contribute to the blockchain.
- **Identity**: In terms of the public blockchain, it provides anonymity or a pseudonym to the actors contributing to the blockchain. But, in the private blockchain, the identity is known by including each of the nodes that are participating.
- **Assets:** The public provides native assets, even in cryptocurrencies like Bitcoin, Ether, and all Altcoins. But, in the private blockchain, the purpose is to use any asset, thus providing a feature that tracks the assets on the blockchain.

Here is an example. Let's say two organizations agree to execute some work, and transfer or exchange assets or currency after the transition gets executed. So, the agreement that they make can be an asset on the private blockchain.

Platforms for blockchain

Let's take a look at the various platforms that have implementations of blockchain:

- **Hyperledger**: The first is Hyperledger, which is consortium-built. It's an open source collaborative effort created to advance cross-industry blockchain technologies. It's a very famous platform.
- **Ethereum**: The second is Ethereum or Enterprise Ethereum, which has two variants. The first is an open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology. Like Bitcoin, no one controls or owns Ethereum, and Enterprise Ethereum is a similar consortium to Hyperledger.

- **IBM Bluemix**: This is a **Platform as a Service** (**PaaS**) that's built on top of the Hyperledger project, and it offers additional security and infrastructure facilities for enterprises to use the Hyperledger blockchain implementation for their own purposes.
- **MultiChain**: This is a platform for the creation and deployment of private blockchains or permission blockchains, either within or between organizations.

- **Corda**: It's a distributed ledger platform with a pluggable consensus that gives flexibility for enterprises to plug in their own consensus or smart contracts for their own purposes.
- **Openchain**: This is a well suited for organizations wishing to issue and manage digital assets. It takes a different approach than the standard Bitcoin approach in implementing blockchain as it works on the partitioned consensus system in which every Openchain instance has only one authority to verify transactions, based on the assets that are being exchanged.

These are just a few examples of blockchain implementations; other than these, there are numerous implementations of platforms available today.

Summary

In this chapter, we began with the fundamentals of cryptography and cryptocurrency. We also got an understanding of its workings and techniques. Then we moved on to an introduction to Bitcoin, its history, and the various wallets and alternate currency available apart from Bitcoin. We then looked at what blockchain is, its structure, features, and the various types available. This chapter has given us a bigger picture of what makes Bitcoin and blockchain the next major innovation after the internet.

In the next chapter, we will focus on decentralization. You will become familiar with decentralization, which sits at the core of blockchain as an innovation, and you will get insights into how decentralization works, what can be decentralized, and what its impact on the world is. We will also go through the pros and cons of decentralization, giving you a holistic overview of it. Stay tuned!

2
Fundamentals of Decentralization

After having gone through the fundamentals of Bitcoin and blockchain in the previous chapter, let's now try to understand a little bit about decentralization. In this section, we are going to take a look at the following topics:

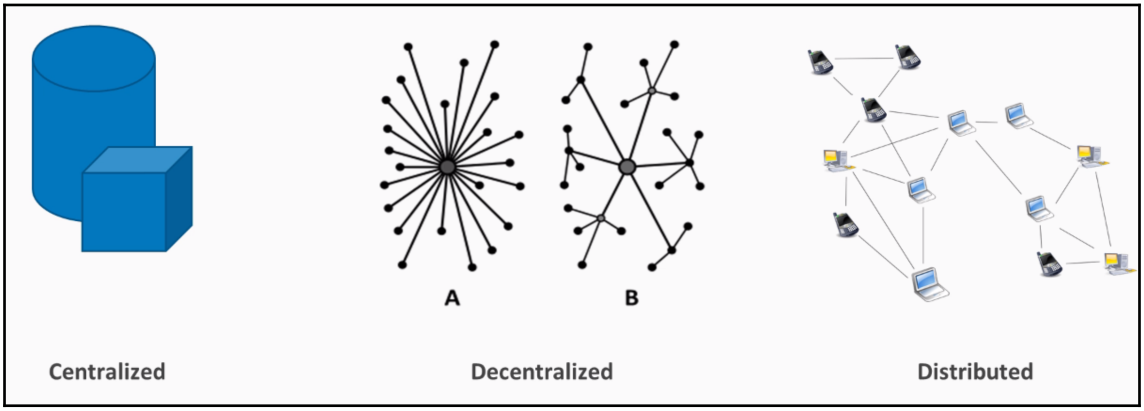
- How decentralization works
- What can be decentralized
- The impact of decentralization on the current and future world
- The pros and cons of decentralization

So, what is decentralization in the first place? Now that you have started to understand blockchain technology and its architecture, you should be hearing a lot about decentralization. It is one of the buzzwords used more frequently in the cryptocurrency space and is often considered as the sole purpose of blockchain technology. Decentralization sounds like it is the opposite of something that is centralized, but it is far more than that.

Decentralized, centralized, and distributed systems

Bitcoin based its foundation on its cryptographically secure ledger, unique assets model, and P2P technology. It led to a new architectural era that helped in building massively scalable and profitable applications, a new type of software referred to as **decentralized applications (Dapps)**. Now let's go through the three types of applications and their differences. Most of the applications that we use are based on a centralized or client-server model. A few discs are distributed, but now more and more are becoming decentralized.

The following diagram demonstrates the differences between these three types of software:



Let's now look into the following different types of applications mentioned in the preceding diagram:

- **Centralized systems:** Centralized software or systems are extensive. These are single instance systems running in a standalone system. The decisions for the system goal are created in the central mechanism and are then transferred to the executive components or people. They do everything in a single node. All executives rely on the central mechanism to take actions, for example, traditional corporations, wherein we have just one CEO or CXO who governs the entire corporation or central laws of a nation. Federal reserve authorities and financial institutions are other examples of centralized systems. Most of the services are found on the internet.
- **Decentralized systems:** Decentralized systems run on a P2P network of computers instead of one computer or single instance. It means that not one single entity has control over all the processing. Decentralized computing is the allocation of resources to each and every workstation on hardware and software. Basically, none of the nodes inform any other node on what is to be done. Decentralized systems bring decision locality, which means that the system's components operate on local information to accomplish goals, rather than the result of the central ordering influence. By nature, this implies that it is distributed among various parties. A key point about decentralization is that there is no central point of control. No one entity controls the others, which is why we said that no node is informing any other nodes of what to do, for example, BitTorrent, which was used for downloading large video files or movies. Blockchain, for that matter, is a classic example of a decentralized system.

- **Distributed systems:** Large internet application services are distributed, but most of them are centralized because the company running them can alter or stop the system all the way, which brings us to an important aspect of distributed systems. The distributed system consists of autonomous components connected using distribution middleware. These components communicate with each other in order to achieve the same goal. The components are located on the networked computers, and they communicate and coordinate their actions by passing messages. Distributed means not all the processing of the transaction is done in one simple, single, or same place. This does not mean that those distributed processors aren't under the control of a single entity. State-level governments are a classic example of distributed systems. Gas stations, for that matter, are again another example. When we think of a gas station, we know that there are Shell stations all over, yet not all gas stations are Shell, which brings us to another important aspect wherein decentralized systems are also distributed systems, but every distributed system does not necessarily have to be a decentralized system.

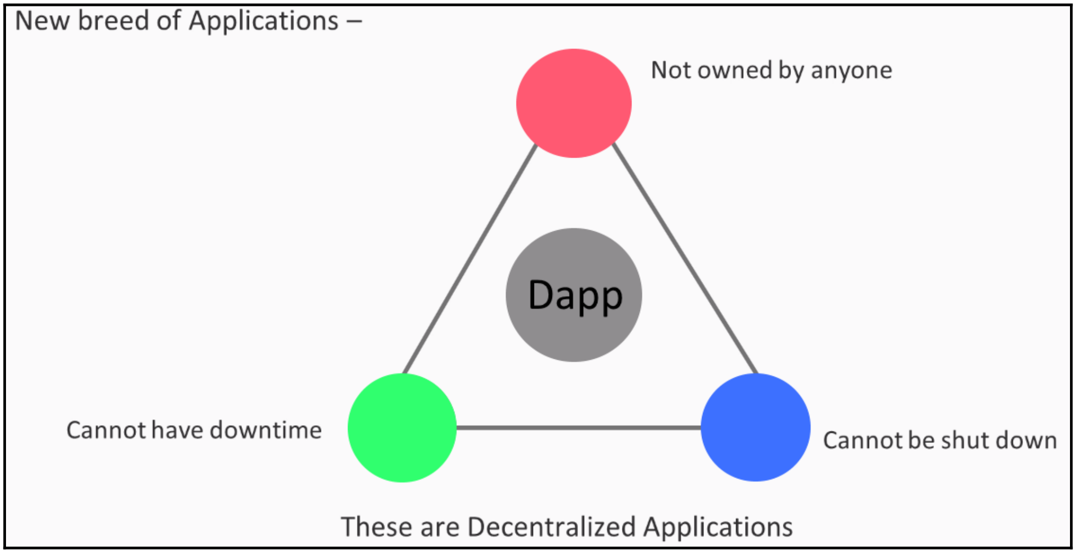
How decentralized systems work

Let's now move forward and look at how exactly decentralized systems work:

- In decentralized systems, storage of data is across the network, which eliminates the risks of a central storage of data or a central point of failure.
- To receive messages, ad hoc message-passing and distributed networking are used.
- It makes use of the public key cryptography. The public key is a cryptographic process whose main function is authentication. The key is available to all, and the usage of the key depends on mathematical processes that are applied to the information that is to be encrypted.
- Each and every node or minor in the network duplicates the blockchain, which is really important.
- Data equality is retained by massive data replication, which means no central official copy exists, but the copy which is available across the network of the decentralized nodes is the official copy. This means no other user is trusted, so there is no affinity to a particular user or set of users, but all the users are treated equally.
- Using software, the transactions are broadcast to the network.
- The messages are delivered in real time within the stipulated amount of time, which means there will be reattempts to deliver the messages.

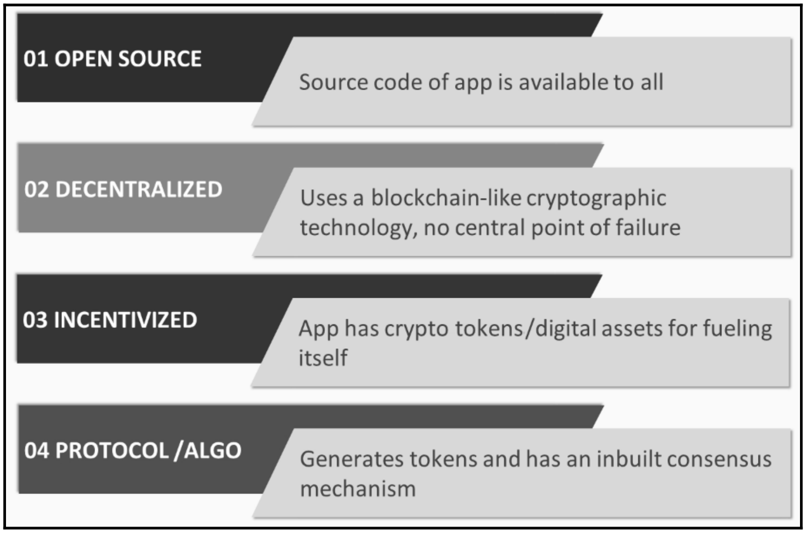
Decentralized applications

Let us take a look at the features of Dapps in the following diagram:


New breed of Applications –
Not owned by anyone
Dapp
Cannot have downtime
Cannot be shut down
These are Decentralized Applications

A new line of applications is being discussed across the world. These types of applications have no owner, they cannot be shut, and they do not have a downtime. This new grid of applications is named Dapps.

The characteristics of Dapps are shown in the following diagram:


01 OPEN SOURCE
Source code of app is available to all
02 DECENTRALIZED
Uses a blockchain-like cryptographic technology, no central point of failure
03 INCENTIVIZED
App has crypto tokens/digital assets for fueling itself
04 PROTOCOL /ALGO
Generates tokens and has an inbuilt consensus mechanism

Let's explore the characteristics of Dapps mentioned in the preceding diagram:

- **OPEN SOURCE**: When we look at the source code of the application, we need to know that it is accessible to everyone. Ideally, its governance should be autonomous, and all the changes should be taken care of by the consensus or a major chunk of its users. Its code base should also be available for scrutiny.
- **DECENTRALIZED**: The applications use a blockchain-like cryptographic technology in which there is no central point of failure. The documentation of the application's operations must be stored on a public and decentralized blockchain to avoid the pitfalls of centralization.
- **INCENTIVIZED**: In order to fuel itself, the app has crypto tokens or digital assets. The valid readers of the blockchain should be incentivized by benefiting from cryptography, which is motivation for the barrier editors to validate the transactions on the blockchain.
- **PROTOCOL/ALGO**: The decentralized applications create tokens and have a built-in consensus instrument. To verify value, the application consortium must agree on a cryptographic algorithm. For example, Bitcoin and Ethereum use PoW with plans for a hybrid PoW or PoS in future.

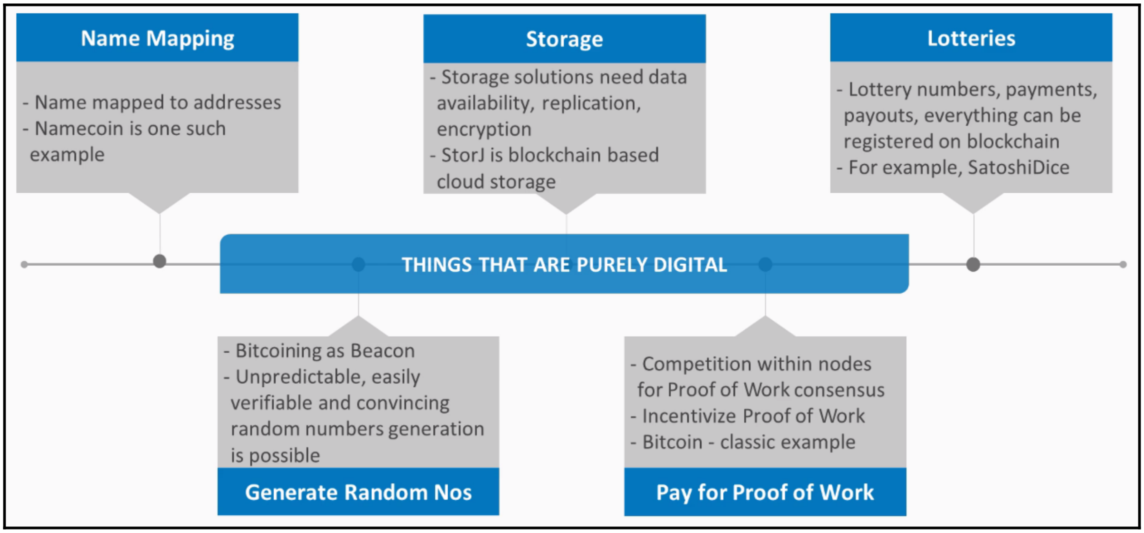
So, if we consider the preceding characteristics, the first Dapp was, in fact, Bitcoin itself. Bitcoin is an implemented blockchain solution that arose from problems revolving around decentralization and censorship. We can say that Bitcoin is an effective public ledger that allows smooth transactions without intermediaries and central authorities. So, the Ethereum white paper classifies Dapps into three types, based on the following two types of perspective:

- **Functional**: In the functional perspective, there are the following three types of Dapps:
    - **Type one**: This type of Dapp manages money or crypto tokens. A user may need to use crypto money or token such as Ether or Bitcoins as a way to settle a contract with another user by using the network's distributed computer nodes as a way to facilitate the distribution of the data.
    - **Type two**: This type of Dapp is where crypto tokens or money are involved, but it also requires something else besides it.
    - **Type three**: This type of Dapp is in the "other" category, which includes solutions to general problems; for example, voting, governance systems, and decentralized autonomous organizations are one particular ambitious breed of Dapps, which are also referred to as **Data Access Objects (DAOs)**. It forms a leaderless organization.
- **Technological**: In the technological perspective, there are the following three types of Dapps:
    - **Type one:** This type of application has its own blockchain; for example, Bitcoin or any Altcoins fall under this category.
    - **Type two**: This type of Dapp uses the blockchain of type one Dapps. This type of Dapp has procedures and tokens that are necessary for their function. The Omni protocol is the best example of this type of Dapp.
    - **Type three**: This type of Dapp uses the protocol of type two Dapps. For example, the **Secure Access For Everyone** (**SAFE**) network uses the Omni protocol for issuing safe coins that are then used to construct the distributed file storage.

These are the types of Dapps from the functional perspective as well as from the technological implementation standpoint.

Decentralizing various entities

After having talked about what decentralization is and how we achieve decentralization, let's now look at what can really be decentralized. It is very exciting to know that many things in the real world can be brought onto a decentralized blockchain platform:


Name Mapping
- Name mapped to addresses
- Namecoin is one such example
Storage
- Storage solutions need data availability, replication, encryption
- StorJ is blockchain based cloud storage
Lotteries
- Lottery numbers, payments, payouts, everything can be registered on blockchain
- For example, SatoshiDice
THINGS THAT ARE PURELY DIGITAL
- Bitcoining as Beacon
- Unpredictable, easily verifiable and convincing random numbers generation is possible
Generate Random Nos
- Competition within nodes for Proof of Work consensus
- Incentivize Proof of Work
- Bitcoin - classic example
Pay for Proof of Work

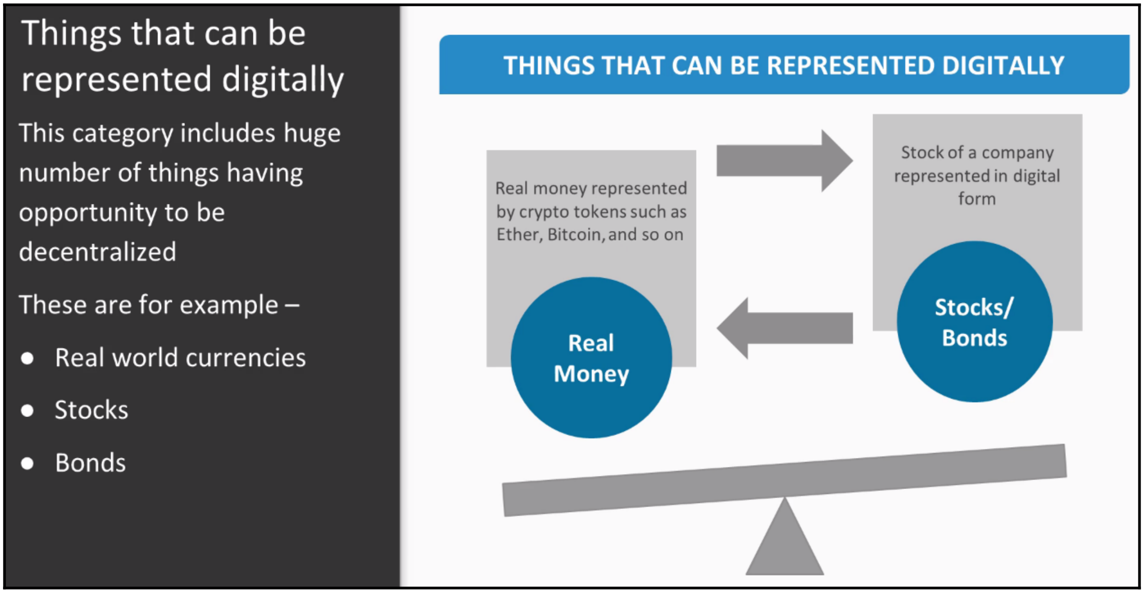
Now we will look into the things that can be decentralized in detail as shown in the preceding diagram:

- **Name Mapping**: Anything that is purely digital can be decentralized. The first example in this category is **Name Mapping**. **Namecoin** is a good example where human-readable names are mapped with addresses. Different participants can enter names as values, update these values, and blockchain can be used to maintain the current state of that value.

- **Storage**: This category is another classic example and a business case to use decentralization. The most important and critical requirement of any storage solution is data availability, avoidance of a single point of failure, data replication, and automatic backup. All these can be handled very well by the decentralized storage solution that uses a secured blockchain solution. **Storage** or **StorJ** is an open source cloud storage platform, which uses blockchain for encrypted and distributed object storage.
- **Lotteries**: By using the decentralized blockchain solution, payment and payout can be denominated in the currency of blockchain itself. This helps in making it easy to have the lottery use a random number generation. **SatoshiDice** is one such example of a lottery that uses the decentralized blockchain solution.
- **Generate Random Nos**: Next is random number generation. Bitcoin can be used as a beacon to provide unpredictable and publicly verifiable yet convincing random numbers, which means that the output is unknown at the time the beacon starts. Yet everyone can verify that the output is close to uniform after the beacon terminates. This is a far more reliable method that generates such random numbers.
- **Pay for Proof of Work**: The next and the last in this category for us to understand is paying for PoW. It complements the concept of storage, but it's mainly aimed at incentivizing the PoW. It aims at creating competition among the verifiable nodes to arrive at a consensus. Various nodes involved in validating the transactions that are a part of the blocks in the blockchain require showing that they have invested significant computing power in performing the verification. In a classic example of Bitcoin, miners compete to process a block of transactions and add it to the blockchain. They do this by joining enough random guesses on their computer to come up with an answer within the parameters established by the Bitcoin program.

Categories of assets

There are many things or assets that are inherently digital and can be represented in a digital manner. We can see these categories in the following diagram:



Things that can be represented digitally

This category includes huge number of things having opportunity to be decentralized

These are for example –

- Real world currencies
- Stocks
- Bonds

THINGS THAT CAN BE REPRESENTED DIGITALLY

Real money represented by crypto tokens such as Ether, Bitcoin, and so on

Real Money

Stock of a company represented in digital form

Stocks/ Bonds

This category includes a huge number of things that have an opportunity to be decentralized, which are as follows:

- Real-world currencies
- Bonds
- Stocks
- Debentures and other such assets

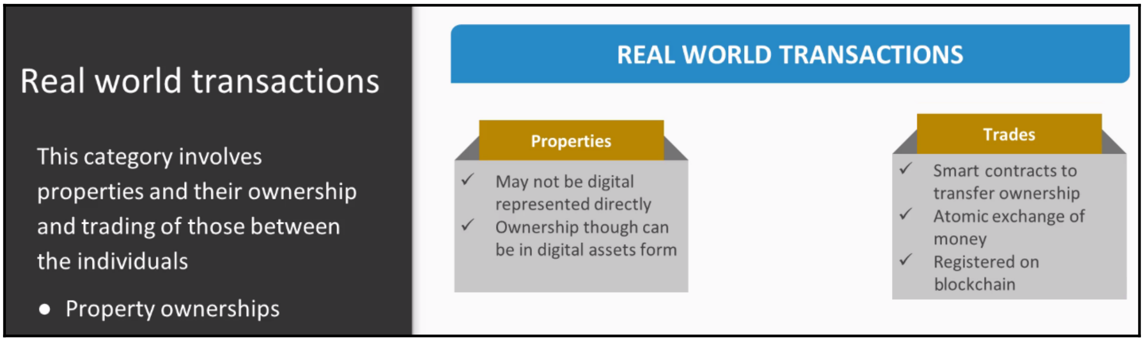
Let's look at these assets and how they can be decentralized by taking an example. Let's say one colored coin represents one particular currency and the other colored coins represent the stock of a particular company. Now, all these assets can be transferred between different participants. Let's say that one participant transfers assets such as bonds or stocks to the other participant, while the other participant pays currency against those assets being transferred to them. This trading of assets can very well be decentralized. You can have atomicity between trading of these assets and transfer the money together, just to make sure that the transfer of assets and the transfer of money takes place at the same time, making one complete transaction.

However, all this is easy to achieve with a solution to a fundamental challenge, that is, how do you ensure that 1 dollar in a colored coin is actually worth 1 dollar? This can be achieved when a bank or a consortium of banks agree that they will bank this colored coin of 1 dollar and that they will maintain the ratio. So, this entity will have to ensure that this one-to-one ratio is being maintained throughout. Similarly, the entity that repossesses the digital stocks must ensure that the digital stock is equivalent to the physical stock. They need to get an agreement to keep this ratio maintained.

Real-world transactions

In the previous section, we saw how easy it is to transfer stocks using a decentralized platform. However, the case is not the same as the real estate properties.

We can see the features of the real-world transactions in the following diagram:



Real world transactions

This category involves properties and their ownership and trading of those between the individuals

- Property ownerships

REAL WORLD TRANSACTIONS

Properties

- ✓ May not be digital represented directly
- ✓ Ownership though can be in digital assets form

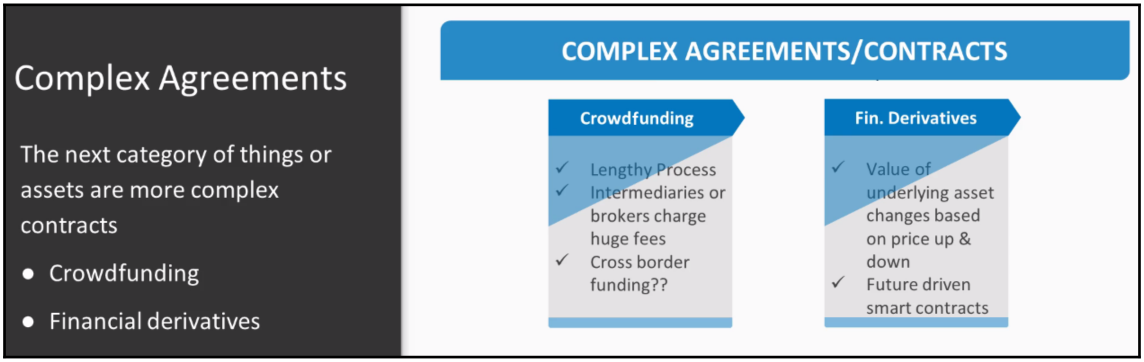
Trades

- ✓ Smart contracts to transfer ownership
- ✓ Atomic exchange of money
- ✓ Registered on blockchain

Properties may not be represented digitally. However, their ownership can very well be represented digitally by using tokens or assets. Then, by using smart contracts and atomic trade exchanges, ownership of these assets can be transferred between individuals. Such digitally executed trades are captured on decentralized platforms. There are many decentralized blockchain platforms available today, that help buyers to transfer property between individuals. The buyers can transfer property ownership in exchange for money and keep the ownership agreements secure on decentralized blockchain platforms. The examples of such a platform are **Atlant** and **Propy**. Properties are just an example that we looked at, but there are a number of such assets on which the ownership transfer and trading can be decentralized.

Complex agreements

The next category of things or assets is more complex, for example, crowdfunding and financial derivatives, as shown in the following diagram:



Complex Agreements

The next category of things or assets are more complex contracts

- Crowdfunding
- Financial derivatives

COMPLEX AGREEMENTS/CONTRACTS

Crowdfunding

✓ Lengthy Process
✓ Intermediaries or brokers charge huge fees
✓ Cross border funding??

Fin. Derivatives

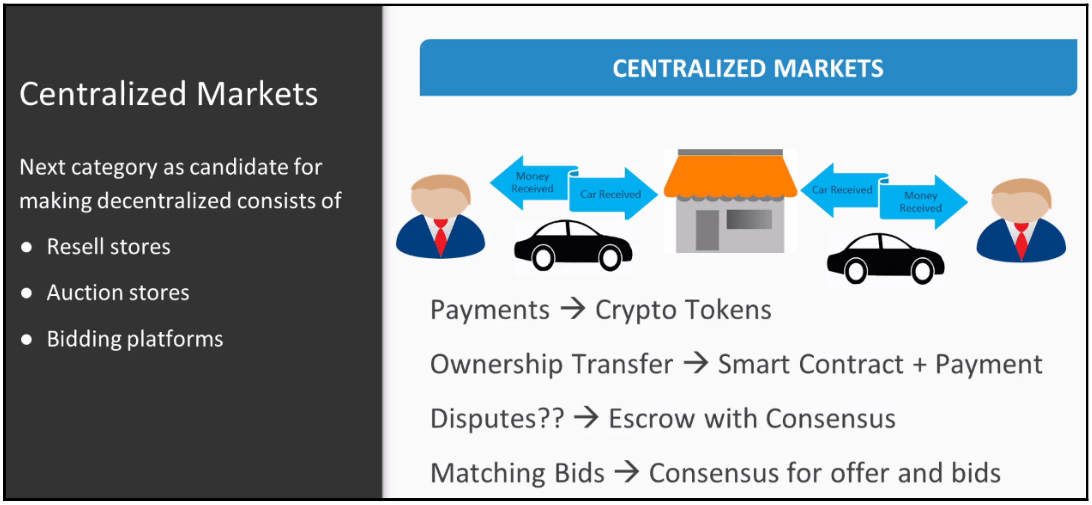
✓ Value of underlying asset changes based on price up & down
✓ Future driven smart contracts

So let's look into what crowdfunding, financial derivatives, and centralized markets involve:

- **Crowdfunding**: We are aware of the star-tup companies that raise funds from investors but have to go through a very lengthy process, which includes legal activities. The most difficult and cumbersome part is that such start-ups usually need to first approach an intermediary or a broker who then connects them to the real investors. Needless to mention, these brokers charge a hefty percentage of an amount as a brokerage fee, besides the time taken to complete the transactions. Decentralization can completely democratize the investing process by eliminating intermediaries and placing the power and the control where it belongs, which is entirely in the hands of the investors. Crowdfunding over the blockchain enables ordinary people to access investment opportunities that they will otherwise never see. The exciting feature of crowdfunding with cryptocurrencies is that it allows the investor to trade the investment immediately on the trading platform available. With the help of decentralized blockchain platforms, start-ups can create their own cryptocurrency, crypto coins, or crypto tokens, backed by their future revenue generation plan. These crypto coins are usually backed by real currency, with an appropriate ratio for each coin. They can then, by using the decentralized platform, offer these coins to the interested investors.

This process is usually referred to as **initial coin offering** (**ICO**). People or entities across the globe willing to participate in this ICO investment register on the platform, purchase the desired amount of crypto coins, and exchange those with real currency. This is relatively an easy, less cumbersome process and, most importantly, it eliminates intermediaries or brokers. There are many crowdfunding platforms available today that are built using decentralized blockchain technology. **Wave** and **OpenLedger** are two of the most well-known platforms.

- **Financial derivatives**: Let's briefly look at financial derivatives. Financial derivatives are another wide area which has the scope to be decentralized. Financial derivatives have an underlying asset and the value of the derivative depends on the price movement that is the upward and downward movement of the underlying asset. The key aspect of a derivative is that it can be considered as a conditional statement written into a smart contract that depends upon the price of the underlying asset, sometimes in the future and so forth. Various Altcoin-based systems can easily be used to build a decentralized derivatives platform.
- **Centralized markets**: The next category as a candidate for making the decentralized solution, consists of markets and options. We can see the characteristics of centralized markets in the following diagram:



Centralized Markets

Next category as candidate for making decentralized consists of

- Resell stores
- Auction stores
- Bidding platforms

CENTRALIZED MARKETS

Payments → Crypto Tokens

Ownership Transfer → Smart Contract + Payment

Disputes?? → Escrow with Consensus

Matching Bids → Consensus for offer and bids

Let's look into the various platforms used in the preceding diagram. We are aware of many online auction stores or resale stores. Let's take one example to understand this in detail. Let's take an example of a used car which is in the buying or selling store. So, typically, what we do is we sell the used car to the store in exchange for money. This completes one transaction. Then, the store executes another transaction where they sell this car to someone else in exchange for money. In this example, you really do not bother about any customer who purchases the car. Another example would be **eBay**. eBay is yet another auction platform. It matches the participants based on their needs and routes payments. **PayPal** is another platform, which is a payment processing platform. It does not do any matching of participants or auctions. It simply provides some payment options and limited variation for disputes arriving from payment.

Decentralization of markets

Now, let's look at how we can decentralize these markets. So, let's take an example of the used cars in the buying and selling the store. We can make this a decent class platform from where P2P transactions can be taken care of very swiftly. So, the premise on these markets can be governed through crypto tokens such as Ether or Bitcoin. The ownership transfer can be done using smart contracts and atomic digital transfers of assets. Dispute handling can be done by using **escrow** or **consensus** to some limited level, which in turn helps mediate the disputes as well. When it comes to matching the bits, we can use consensus and smart contracts to match and get approval from the selling entity. Miners can match the offers and bits together.

Centralized markets for decentralization

Let's now look at the next category for decentralization. Centralized markets, such as exchanges, are yet another classic case to be decentralized. Online exchanges bring lack of trust and hence have a middle man who establishes the trust. A decentralized exchange is an exchange market that does rely on a third-party service to hold the customers' funds. Instead, trades occur directly between users, that is, P2P, through an automated process. This system can be achieved by creating proxy tokens such as crypto assets that represent a certain cryptocurrency or asset that represent shares in a company or through a decentralized, multi-signature escrow system. Among all the solutions that are currently being developed, this system contrasts with the current centralized model, in which users deposit their funds and they exchange issues an IOU that can be freely traded on the platform. When a user asks to withdraw his funds, these are converted back into the cryptocurrency that they represent and are sent to their owners. **Ripple** is an example of an exchange platform that decentralizes the currency exchange and provides cross-border remittance by using the transitive trust.

There are the following differences between centralized exchanges and decentralized exchanges:

- **Centralized exchanges**: Centralized exchanges control the funds. You cannot remain anonymous in centralized exchanges. In centralized exchanges, there are hacks and server downtime.
- **Decentralized exchanges**: Decentralized exchanges allow users to control the funds. You can remain anonymous or pseudonymous in decentralized exchanges. In decentralized exchanges, there are no hacks and server downtime is next to impossible.

Thus we have learned that anything digital can be decentralized and anything that can be represented digitally, can also be decentralized.

The impact of decentralization

In the previous sections, we looked at how decentralization works and what can be decentralized. In this section, we will look at the following topics:

- Why are decentralization and blockchain being considered as some of the most important platforms or technologies in today's and the future world?
- What is the possible impact this technology can bring to today's world and the futuristic vision?

The blockchain technology has been hailed as a revolutionary technology that can dramatically impact the following key factors that play a key role in the day-to-day activities across the globe:

- Cost of trades or transactions
- Speed of execution
- Transparency of all transactions
- An involvement of intermediaries
- Security

Each of these factors has implications in almost every industry, be it banking, stock market, legal, agriculture, business, trading, security, medicines, manufacturing, supply chain, bioinformatics, music, and various other service sectors.

Sectors affected by decentralization

Let's further discuss the following sectors and how decentralization impacts them:

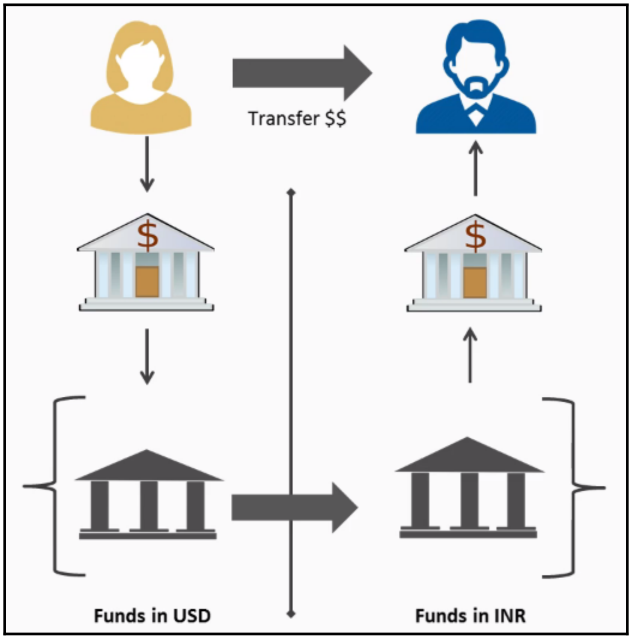
- **Stock markets:** Let's take an example of stock markets to see how decentralization can impact this sector. Today's stock markets have modern computing and the internet has also sped up the transactions. In the modern stock markets that we have today, stock transfer agents are decentralized registrars who drag and share the ownership for issuers and the stock market, while the modern transfer agents use today's latest technology. But the same old centralized register model persists even today. Let's now look into the following challenges that we see in today's modern stock markets:
    - The first challenge is that it is centralized and expensive.
    - Depositories and transfer agents are the middlemen and are hence a single point of failure.
    - Various processes involved, such as a registration, transfer, distribution, scrutinizing, and courier fees, yield higher charges. As the scope of the stock market gets wider and wider, the administration cost keeps on increasing.
    - Another challenge we see is limited transparency. There is a lot of information asymmetry, that leads to market advantages to those who have access to this information. There is always a concern to do with forged security and asymmetric counterparty risk.
    - Most importantly, the legal ownership remains with the transfer agents in the majority of jurisdictions and the investors do not have the title with them.

  Let's look at how decentralization impacts this current status. Centralized and decentralized hubs can be eliminated and the decentralized blockchain based implementation can be used, which will help to directly transfer the shared ownership between the investors, using P2P communication and consensus mechanism. Besides this, the decentralized ledger which gets updates within a minute could also save millions spent on collateral and settlement costs. Decentralization can cut inefficiencies in the share settlement function, trades being settled by P2P communication cuts the middleman out, resulting in a lesser cost of record-keeping. Due to P2P communication, the settlement can happen in real time instantaneously. Needless to say, above all of this, all these being on the shared ledger brings a lot of transparency.

- **Banking sector:** Let's now look at the impact that decentralization can bring in the banking sector. The typical key routine or procedures carried out in banks on daily basis are **know your customer** (**KYC**)and **payments and fund transfers**. We will look into the KYC processes as well as the payments and transfers. While using the compliance platform and KYC processes, we have umpteen challenges. We will get a detailed gist of these challenges in the points as follows:
    - The KYC process is a centralized process and it's done in isolation by each bank.
    - It's a repetitive task.
    - There are costs which are increasing day by day.
    - Bookkeeping of records is always done in isolation.
    - The banks do not involve each other in these documentation depositories.

  We will now discuss what impact decentralization brings in the section. By using the compliance platform and KYC process of decentralized blockchain technology, banks can reduce operation costs and increase efficiency. KYC can be performed once and can then be made available as a reference for other future transactions. Moreover, once these KYC details are made available on blockchain, they can be used by other banks, accredited institutions, or organizations without the need to re-initiate the KYC for the same customer again and again. This will save the cost spent on the repeated KYC process, the time spent on completing the KYC, and it enables faster and more accurate travel of records. Banks and financial institutions can attract customers since they will improve the ease of work and the speed of work, and the customers will need to be provided with the KYC documents only once.

- **Payments or fund transfer**: Let's take an example. A typical bank wire transfer transaction takes place across the border and invoice for an exchange. Let's say Jessie needs or wants to transfer 1,000 dollars from her US account to her friend John in India. We can see the transfer transaction for Jessie and John in the following diagram:



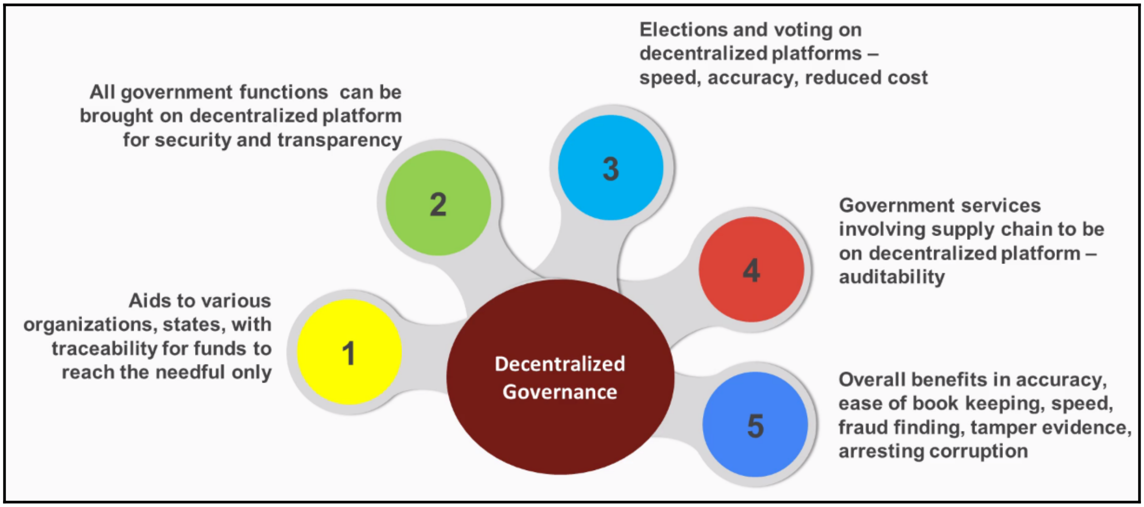
Let us look at the challenges faced in the following section:

- Multiple parties are involved in the process. The bank where Jessie holds her account is in the US and involves third-party foreign exchange that is present in the US and third-party foreign exchange that is present in India since John holds his account in India. The money moving across all these accounts take a considerable amount of time, usually anything between 5 and 7 days.
- The second challenge is the time duration for transfer. Even if we assume a same-day transfer from one account to other, we are talking about at least 4 to 5 days minimum.
- The third challenge is private bookkeeping. Each bank keeps its own bookkeeping record privately. This leads to increased time needed for validating proof of ownership of funds.
- The fourth one is the lack of clarity and choice on rate applied. And also customer is not guaranteed to get the desired exchange rate due to the time is taken by the entire process. Moreover, there is no clarity on why a particular rate was applied.
- The fifth and foremost challenge is higher charges and fees. It is needless to state the number of charges applied by all these intermediaries and banks.

So, let's look at how decentralization impacts the foreign exchange process in the sector:

- Now, if this entire foreign exchange process is brought onto the decentralized blockchain platform, the first benefit is in is the elimination of the intermediaries that claim to establish the trust for the transactions. This reduces the time taken at least by half. Now, how do we establish trust in this transaction?
- Well, let the P2P consensus bring transitive trust. Real or fiat currency can be represented in crypto tokens or assets digitally. These tokens can be then transferred through the blockchain program from Jessie to John, almost in seconds. The transaction can be executed in minutes, if not in seconds. It brings transparency in the actual rate applied, speeds up the transaction, reduces the charges or fees drastically, and establishes a secure and transparent book of records for future compliance purposes.
- Many banks across the world today have started collaborating with each other in the foreign exchange space to reduce the time and cost and increase transparency and security.

We will now look at how the decentralized blockchain platform transforms a government or government organizations. As an example, any government in today's world struggles due to challenges in accountability, lack of transparency, and efficiency. Decentralization can help in bringing fair, transparent, and accountable governance, enabling trust and confidence in the citizens. Let's take a look at how decentralization can help in achieving the desired goals as shown in the following diagram:


Elections and voting on decentralized platforms – speed, accuracy, reduced cost
All government functions can be brought on decentralized platform for security and transparency
3
2
Government services involving supply chain to be on decentralized platform – auditability
4
Aids to various organizations, states, with traceability for funds to reach the needful only
1
Decentralized Governance
5
Overall benefits in accuracy, ease of book keeping, speed, fraud finding, tamper evidence, arresting corruption

Let's explore the ways how decentralization can help:

- It helps in providing aid to program in various states and nations and it ensures that the funds reach the intended recipients only.
- All the government operations and systems, such as properties, taxes, public services, social benefits, health benefits, and utilities, if brought on a digital ledger, can bring security and transparency.
- Elections and voting can be brought onto the decentralized platform, which in turn will bring speed, transparency, and accuracy in the election process and will also reduce the cost and complexity involved. The result will be faster and correct.
- The fourth benefit is that the government services that involve supply chain management will be cheaper, accurate, and auditable.
- Lastly, the most important part is that once all the government operations are brought onto the decentralized platform, there will be more accurate in bookkeeping, increasing speed and easing the fraud finding, tempering, and arresting corruption to a larger extent.

The pros and cons of decentralization

After going through the journey of understanding decentralization in detail, we now have reached the end of this section. In this section, we will look at some of the most important pros and cons of decentralization. Over the past few decades, the technology advancements and innovations have helped mankind and this world make good progress and growth. However, at the same time, any such innovations in technology have also exposed the dark side of the internet and has shown us the misuse of the technology itself.

The internet, for example, has its benefits but also has its disadvantages as well. People misuse the internet for hacking online systems and various other scams. It is not primarily the pitfall of the technology, but the usage of it with wrong intentions. The coin always has two sides and we are talking about the crypto coin here. Similar to the internet, even decentralization and blockchain have their own pros and cons. So, let's look at some of those at a broad level.

Firstly, one of the most significant benefits of blockchain is that it is a distributed network rather than being a centralized one. Transactions can be verified by a widely spread P2P global network of nodes. This means if someone wants to manipulate the data present on the blockchain, they will need to get access to all the computers in the distributed network, at the same time.

The computing power needed to conduct such a hack can be compared to something equivalent of the hashing for money. In this example, you really do not bother about any customer who power of a nation or state and all the technology companies therein to overcome more than 51% computational power of the entire network, which is next to impossible. This eliminates the single point of failure.

But looking at the cons part of it, there are still possibilities of hacking and manipulation of data. There are several types of hacks that are possible if the decentralized blockchain platform is not devised to safeguard from them. Let us discuss the hacks:

- **Miner**: For example, a 51% attack is considered as an inherent setback of public blockchains. One who has reputed the maximum to the network's mining hash rate has the ability to manipulate the ledger as per desire. In simple words, if you are a miner and are mining more than 51% of the blocks on a blockchain, then you can potentially change the ledger contents in all the blocks that are being written hereafter.
- **Eclipse:** Another type of hacking called an Eclipse attack involves crippling of one of the nodes in such a way that it fails to interact with all other nodes. This way, the percentage of mining hash rate does not pose as a restricting attribute and the remaining nodes probably may take the highest side of mining, dictating the rest of the blocks.
- **Money making scams:** The decentralized public blockchain can be used as a medium to ask for money from the public, for example, the **Ransomware** virus attack.
- **Bank vulnerability:** Even banks are vulnerable to fraud and robbery. A recent example would be when a group of hackers took control of all online and ATM operations of a large bank in Brazil. They got access to passwords, credit cards, and all other personal information of the individuals. This attack provided them with money and additional private information which can be used for future attacks as well.

We will now discuss the pros of decentralization in a detailed manner:

- Decentralization primarily eliminates intermediaries such as banks due ti which such information of value would not have had a central point of access. Due to its tamper-evident structure and immutability, the decentralized blockchain technology can help detect corruption and fraud in the government organizations as well. For example, the Silk Road online case which was shut down by the Federal Bureau of Investigation a few years ago. It was a darknet marketplace and consisted of a nexus of unlawful elements, which even the federal agencies were not able to trace. It was the decentralized blockchain ledger that helped the federal to uncover the real culprits who were covering up the evidence. The people who were actually the federal agents were the culprits and were part of the investigation team itself. This was only uncovered because of the decentralized, immutable, no single owner ledger of the blockchain platform.
- On the flip side of it, while decentralization eliminates the need for an intermediary or a middleman, over decades the whole world has been operating and is being driven by intermediary agencies only. Such intermediary agencies have been making money year on year. Besides this, due to its underlying complexities, blockchain and decentralization are not that easy for people to understand. The cryptography, the blockchain, the decentralization, and all the jargon are tough for them to understand. So, there will be a lot of resistance to accepting decentralization, especially in government organizations and some of the key agencies in the society.
- On the decentralized blockchain, anything that is worth the value can be transferred between entities and saved safely and confidentially. This restricts our attempt to alter with the wrong intention because the person has to find specific data for a particular individuals transaction. The anonymity on a decentralized platform can act as a two-edged sword: while it maintains confidentiality, it also helps the scammers and unlawful people who use it for their own advantages, to carry out illegal trades and transactions while remaining anonymous.
- The security provided by the decentralized blockchain is achieved using cryptography and restricting the changes to the data written on the blockchain. This immutability keeps the data safeguarded lifelong. However, since transactions or data return on the platform is irreversible, any data that was mistakenly written and has to be corrected needs to be rewritten as a new record. One can only add corrected data as the new transaction. This, of course, needs to undergo additional computation, verification by the nodes, network sharing, and so on.

Summary

This chapter has enabled us to understand and look at the various possibilities in which we can use decentralization and blockchain for the benefits of society and individuals. Since this technology is completely new and undergoing changes, we hope to see a better world tomorrow that includes security and transparency while eliminating all the cons present. This brings us toward the end of the fundamentals of decentralization and how decentralization is going to impact our present and the future world in a better way.

In the next chapter, we will get to know some advanced concepts of blockchain and the various security features. We will also look at hardware wallets and how Bitcoin is physically stored and much more.

3 Advanced Blockchain Concepts

In this chapter, we will discuss the advanced concepts of blockchain and the various protocols, challenges, and solutions to it. In the earlier chapters, we looked at the consensus protocol or algorithm as one of the most critical components, or building blocks, of the blockchain. When we speak about blockchain, the first thing that comes to mind is security and the blockchain consensus algorithm. We will look into these challenges and the solutions. From there, we will progress into smart contracts and how they work with the protocols in the blockchain.

In this chapter, we will cover the following advanced concepts of the blockchain:

- Consensus protocols, which are the running engine of the blockchain
- Types of consensus algorithms
- Key challenges in the blockchain to maintain privacy
- Smart contracts
- Distributed applications

Introduction to consensus protocols

A consensus algorithm is a process implemented in distributed processes or systems to achieve agreement on some particular data. The blockchain consensus algorithm keeps the ledger transactions synchronized across the network to ensure that ledgers are only updated when the appropriate participating board approves transactions and, when ledgers are updated, they are updated with the same transactions in the same order. This process is called a **consensus**, and the protocol program that keeps this running is the consensus algorithm. That is why a consensus is considered to be the running engine or heart of blockchain.

So, consensus primarily establishes a strong technology infrastructure layer for the blockchain, which makes it the most critical part. It ensures that every next block that gets added to the blockchain is the one and only true version and that there are no other blocks that represent another version. It also safeguards the entire blockchain against powerful adversaries that may potentially derail it and cause it to fail to maintain its integrity. In short, for a blockchain network, achieving consensus ensures that all nodes in the network agree upon the consistent global state of the blockchain.

Properties of consensus mechanism

A consensus protocol has the following few key properties, which determine its applicability and efficacy:

- **Safety**: According to the rules of the protocol, if all nodes produce the same output and the outputs produced are valid, the consensus protocol is determined to be safe. This is also referred to as the consistency of the shared legislature.
- **Liveness**: The liveness of a consensus protocol is guaranteed if all the faulty nodes participating in the consensus eventually produce a value.
- **Tolerance**: A consensus protocol provides fault tolerance if it can recover from failure often or participate in a consensus.
- **Non-repudiation**: This provides the means to verify that the supposed sender really sent the message.
- **Decentralized consensus**: A single central authority cannot provide transaction finality. Hence, the consensus must be of a decentralized nature.
- **Quorum structure**: Nodes exchange messages in predefined ways, which may include several stages or tiers at the same time.
- **Authentication**: The consensus process provides the means to verify the participants' identity.
- **Integrity**: The process enforces the validation of the transaction integrity.

While all the preceding properties are crucial, a famous result by Fisher, Lynch, and Peterson, known as the **FLP Impossibility Result**, states that no deterministic consensus protocol can guarantee safety, liveness, and fault tolerance all together in an asynchronous system. Although fault tolerance is crucial for globally distributed networks to operate, depending on their system requirements and assumptions, distributed systems tend to choose between safety and liveness.

The Byzantine Generals' Problem

In a distributed system, faults are categorized into the following two types:

- **Fail-stop faults**: These are benign faults that cause nodes to stop participating in the consensus protocol due to hardware or software crashes. The nodes will stop responding when the fail-stop fault occurs.
- **Byzantine faults**: These are faults that cause nodes to behave erratically. Leslie Lampert also identified and characterized this category of fault as the **Byzantine Generals' Problem**.

The Byzantine Generals' Problem is conceptualized on the basis of a situation where a group of generals, each commanding a part of the Byzantine army, have surrounded an enemy fort. To successfully attack and take over the fort, all the generals have to agree on a common battle plan and generals can communicate through messengers (horse riders or runners) only. But, there is a possibility that these messengers might get captured by the enemy and the message might never reach the other generals. Moreover, the difficulty in reaching an agreement is that one or more generals might be traitors and might possibly be interested in sabotaging the whole battle plan. Being traitors, they might send false messages, distort messages, or not send any message at all. But all loyal generals will act accordingly to the plan. In short, a small number of traitors should not cause the loyal generals to adopt a bad or a wrong plan. With this example, we can see that the Byzantine Generals' Problem is a typical challenge for a distributed and decentralized system.

Solution to the Byzantine Generals' Problem

Distributed systems now have a traditional consensus approach that focuses on building fault tolerance in the face of unreliable systems, provisioning mainly for fail-stop faults. Some examples of the Byzantine General's Problem are **Paxos**, **Raft**, and **Viewstamped** replication. The traditional consensus approach is used for putting an order of transactions in the distributed databases, to order client-generated requests and other respective stage changes which take place in distributed applications by using replicated state machines. The number of nodes needed in such networks is `2 f + 1` to be able to tolerate `f` fail-stop failures. Tolerating Byzantine faults increases the complexity of the consensus protocol by adding several extra layers of messaging to the system. All these solutions carry overhead and add more complexity, making them practically impossible.

Practical Byzantine Fault Tolerance

The approach that allowed for Byzantine fault-tolerant applications with low overhead was **Practical Byzantine Fault Tolerance** (**PBFT**). PBFT was first proposed by Miguel Castro and Barbara Liskov in 1999. PBFT can process an enormous number of direct P2P messages with minimal latency. To be able to tolerate `f` faults in the system, PBFT needs `3f + 1` replicas. So, PBFT uses the concept of primary and secondary replicas, where the secondary replicas automatically check the sanity and liveness of decisions taken by the primary, and can collectively switch to a new primary if the primary is found to be compromised. Each node maintains an internal state. Upon receiving a message, the respective node uses the message, in conjunction with the internal state, to run a computation or operation. This directs the node as to what to do or think about the message it received. Once the node reaches an individual decision about the respective message, it propagates this decision with all other nodes participating in the system. A consensus decision is arrived at, based on decisions propagated by all the participating nodes. This mechanism of arriving at a consensus requires less effort and adds less overhead than the other methods.

Types of consensus algorithms

The following three consensus algorithms or protocols are used in the majority of blockchain platforms:

- PoW
- PoS
- PoET

We will also do a quick comparison of these three, in the later sections. Before we look at these different consensus algorithms, let's take a look at the reasons behind the variety of algorithms. The following are some of the reasons for that variety:

- **Business need**: Business demands drive which algorithm to use.
- **Use case**: The use case for using a public or private blockchain influences which algorithm will be used.
- **Token need**: Not every business case needs to use tokens or cryptocurrencies, and may just want to use the underlying blockchain with a consensus.
- **Security and privacy**: Security requirements may vary, and the same goes for privacy. Some may want a public blockchain, while others may prefer private ones.

- **Performance**: Public blockchains may need more time to arrive at a consensus, while private ones may do it faster.
- **Robustness**: Banking use cases may demand extremely high cryptography and consensus algorithms, as compared to others.

Proof of Work

The PoW algorithm, also used by Bitcoin, is the best known method of achieving a consensus on a blockchain. To achieve a consensus in PoW, unlike PBFT, the submission of individual conclusions is not required from all the nodes in the network. Instead, PoW uses a hash function to create conditions that allow a single/individual participant to announce their conclusions about the submitted information, which are then verified by all the other system participants. The hash function has a parameter that ensures false information will fail to compute in an acceptable way to prevent any false conclusions.

Participants in the Bitcoin system, who publicly verify information on behalf of the network, are rewarded with a newly created Bitcoin. This process of searching for valid hashes for the verification of information is called **mining**. This system of rewarding participation in the network allows broad participation, which results in building a more robust network and a safer blockchain. This broad participation ensures greater network stability with minimal requirements for each participant and allows participants to remain anonymous.

Challenges with PoW

Although PoW has its benefits, besides being the best known method, it also has its own inherent challenges. Nodes need to use real-world resources, such as computers and electricity. It takes a lot of power to run the computers, or clusters of computers, that calculate different potential solutions, which from an ecological standpoint isn't ideal and it is bad for the environment as well.

The nodes need a lot of computing hardware to reach a consensus and such hardware is really expensive. There is a possibility of miners moving their hardware to mine a different coin or an old coin if the reward is better there. In this case, miners and nodes are less loyal. PoW incentivizes the consensus process, which is a motivation for miners to mine blocks and earns rewards. However, with the maximum capacity of 21 million Bitcoins, with more and more points being released over a period of time, miners' rewards will come down as coins become harder to mine. This may lead to demotivation for miners to continue mining, which might challenge the overall consensus.

The fact that you need a serious amount of computing power, more than the average person could afford or would even be able to work with, means the mining community is getting smaller and more exclusive. This goes against the idea of decentralization and could potentially lead to a 51% attack.

Proof of Stake

PoS is the most common alternative to PoW for verifying and validating the transactions on the block. In this type of consensus algorithm, instead of investing in expensive computer equipment in a race to mine blocks, a validator invests in the coins in the system.

> Note the term validator, because no coin creation or mining takes place in PoS. Instead, all the coins exist from day one and validators, also called stakeholders, are paired strictly in transaction fees only.

In PoS, the selection of individuals for the approval of new messages to confirm the validity of new information submitted to the database is done in a more deterministic way. This selection is done by the network on the proportional stake of each individual in the network. In PoS, your chance of being picked to create the next new block depends on the fraction of coins in the system you own or have to set aside as a stake. For example, a validator with 500 coins will be five times as likely to be chosen as someone with 100 coins.

Switching to PoS could help to encourage more community participation as well as aid decentralization. Taking mining out of the hands of the few pools of GPU farms doing the bulk of the mining, which somewhat resembles an oligopoly, and then distributing it evenly across the network, should lead to a more real decentralized system. Naive PoS algorithms suffer from a problem of keeping nothing at stake. It doesn't punish actors for validating more than one history, meaning the network could easily disagree on the real history. A participant with nothing to lose or with no stake involved has no reason not to behave badly. These implementations do not provide incentives for nodes to vote on the correct block. Therefore, nodes can vote on multiple blocks, supporting multiple forks, to maximize their chances of winning a reward, as they do not expend anything in doing so. This nothing-at-stake problem needs to be tackled for the correct and efficient implementation of PoS.

Proof of Elapsed Time

PoET is a consensus algorithm similar to PoW which it consumes far less electricity, that Intel has developed for their own use. The algorithm uses a **trusted execution environment** (**TEE**), such as **Software Guard Extensions** (**SGX**), to ensure blocks get produced in a random lottery fashion without any work done, instead of having participants solve a cryptographic puzzle. This approach is based on a guaranteed rate time provided through the TEE. According to Intel, the PoET algorithm scales to thousands of nodes and will run efficiently on any Intel processor that supports SGX. A major drawback for PoET is the requirement to always put your trust in Intel, when moving away from putting trust in third-parties is the fundamental reason for the public blockchain. This algorithm can be looked at as another alternative approach.

Comparison between PoW, PoS, and PoET

We will now compare the three consensus algorithms that we have seen for a better understanding, and weigh them against certain parameters. The following table shows the state of respective consensus algorithms for each parameter:

Parameters	**PoW**	**PoS**	**PoET**
Blockchain type	Permissionless	Both	Both
Transaction finality	Probabilistic	Probabilistic	Probabilistic
Transaction rate	Low	High	Medium
Token needed	Yes	Yes	No
Cost of participation	Yes	Yes	No
Scalability of peer network	High	High	High
Trust model	Untrusted	Untrusted	Untrusted

Now, let's discuss the preceding table:

- **Blockchain type**: This indicates the type of blockchain platform, permission or permissionless, in which the consensus model can be used. This is mainly governed by the type of membership allowed by the consensus model. While PoW models are built exclusively for the permissionless platform with open-ended participation, they can technically be used with permission platforms but won't be ideal in that setting. PoS and PoET, by design, can work in both function types.
- **Transaction finality**: This indicates whether the transaction, once added to a block in the blockchain, is considered final. PoW- and PoET-based consensus models carry the risk of multiple blocks being mined at the same time due to their model of leader relationship in combination with network latency.

- **Transaction rate**: Platforms that can confirm transactions immediately and reach a consensus quickly have a higher transaction rate. PoW approaches are probabilistic and have to spend a significant amount of time-solving a cryptographic puzzle. Therefore, these models have high transactional latencies, hence a low transaction rate.
- **Token needed**: As the designs are based on the existence of a token, a cryptographic token is inherently required for PoW and PoS models, whereas PoET models do not require a token for a consensus to be achieved.
- **Cost of participation:** There are inherent costs associated for PoW and PoS to participate in a consensus. To develop the security deposit to declare interest and bond with the platform, PoW requires expending energy, which is a resource that is external to the consensus protocol, while PoS requires nodes to buy some initial cryptocurrency.
- **Scalability of peer network**: The scalability of the consensus model is its ability to reach consensus when the number of peer nodes is constantly increasing. All models summarized previously have high scalability.
- **Trust model**: This determines whether the nodes participating in the consensus have to be known or trusted. In PoW, PoS, and PoET, nodes can be untrusted as the mechanism to reach consensus is based on other means, such as computational work or security deposits. As long as more than 25 to 50% of the network is not adversarial, consensus decisions will not be effective.

There is one more parameter that is not listed here, which is **adversary tolerance**: that is the fraction of the network that can be compromised without the consensus being affected. Each consensus model has a certain threshold or true adversary tolerance.

Key privacy challenges of the blockchain

Let's take a look at some general challenges regarding privacy in blockchain and the solutions to overcome those challenges. Eric Hughes, cofounder of the Cyberpunk Movement, UC Berkeley, and a well-known mathematician, said in 1993 that privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary system. An anonymous system empowers individuals to reveal their identity when desired, and only when desired. But, is this the case with Bitcoin and public blockchain? There is a popular delusion that Bitcoin is anonymous and untraceable. It's an understandable mistake, given Bitcoin's popular use case, which was the infamous Silk Road we covered in earlier chapters.

The FBI was able to trace and expose people involved in this case with the help of immutability in the Bitcoin blockchain. However, we must not ignore that they were able to trace the flow of currency and single out the exact person they sought. The truth is that Bitcoin is indeed pseudonymous and traceable. Every transaction in Bitcoin maps the inputs to the outputs, allowing anyone to follow the money in a very trivial manner. Satoshi Nakamoto in his white paper defined Bitcoin as a history of its custody. In 2009, he stated the following:

> *"We define an electronic coin as a chain of digital signatures."*

Pseudonymous behavior of Bitcoin

Pseudonymity is when we arrive at a relationship with some entity without disclosing the individual identity of that entity. A pseudonym refers to a unique alternative identifier, such as the nickname of a person, credit card number, student number from college, and bank account number. Using a pseudonym, you can tag various messages and transactions from the same entity by making a group of these transactions. Pseudonyms are widely used in social networks and other virtual communication channels. For example, any customer care representative introduces himself or herself with a pseudonym, instead of revealing their original name; this is pseudonymity. Twitter handles and Facebook accounts, for example, are classic examples of pseudonyms.

We must remember that while using pseudonymity, one cannot be identified but can still be singled out, and that's what poses a challenge in privacy for blockchain. Let's take a look at the following challenges:

- **Public blockchain ledger**: Since the public blockchain ledger is available for anyone, some addresses can be grouped by their ownership, using behavioral patterns and publicly available information from outside blockchain sources.
- **Wallet address**: The wallet address reuse links your transactions together into a single profile.
- **IP address reuse**: IP address reuse also hints to the world that a single party, such as you or me, controls various addresses.
- **Combining inputs from multiple transactions**: This reveals the set of addresses you control.
- **Using lite clients**: If you're using lite clients, not really strictly written clients, these are effectively revealing to a third-party your full set of addresses and whatnot.

Bitcoin addresses clustering as another famous technology stack, which poses a challenge for deanonymizing Bitcoin address users. It does so while addressing all addresses generated by a single user, via analysis of information derived from the blockchain. It can then be observed that the P2P network represents other information sources that aid in the deanonymization of Bitcoin users. Combining these two together can easily assist Bitcoin address clustering and help in identifying individuals. In some cases, it can also help in correlating all transactions of the file user. At the same time, there are many companies in the world today that are building businesses around blockchain. As the network increases, these companies gain a lot of importance because incentives to track the flow of such capital becomes stronger.

Solutions to privacy challenges

Let's look at some of the solutions that can help deal with the privacy challenges posed by public blockchain.

CoinJoin

CoinJoin is an anonymization method for Bitcoin transactions proposed by Gregory Maxwell. It is a method of Bitcoin transaction compression, which aims to improve privacy by discarding unnecessary information. A CoinJoin transaction is one where multiple people agree to form a single transaction where some of the outputs have the same value. All parties come together over some anonymous channel and each of them provides a destination address, which belongs to them. One of the party creates a transaction, which sends one coin to each destination address. All parties log out and then separately log in to the channel, and each contributes one coin to the account from which the funds will be paid out. If `X` number of coins is paid into the account, they are distributed to the destination addresses; otherwise, they are refunded. Some popular examples of CoinJoin implementations are SharedCoins, Dark Wallets, CoinShuffle, and Dash.

Ring signatures

Ring signatures are a technically complicated technology but are extremely promising and help to achieve token anonymization and to identify applications. Essentially, a ring signature is something that proves that the signer has a private key corresponding to one of a specific set of public keys, but does not reveal which one it is. It is composed of the actual signer, who is then combined with the nonsigner to form a ring. The actual signer and nonsigner in this ring are both considered to be equal and valid. The actual signer is a one-time use key thing that corresponds with an output being sent from the sender's wallet. The nonsigners are outputs from past transactions that are drawn from the blockchain. These past transaction outputs function as a decoy in the ring signature transaction by forming part of the input of a transaction. All the inputs appear equally as likely to be the output being spent in a transaction from outside the ring.

For example, if Dan wishes to send one Monero to Melissa with a ring size value of five, one of the five inputs will be pulled from Dan's wallet, which will then be added to the ring signature transaction. The other four inputs are past transaction outputs that are pulled from the blockchain. These four inputs are decoys and, when fused with the input from Dan's wallet, form a group of five possible signers, making a ring of those five. A third party would not be able to determine which input was actually signed by Dan's one-time use key. However, with the use of a key image, the network is able to verify that the asset or coin being transferred to Melissa has not been spent before. Monero is the best example that uses the ring signature mechanism.

Zero-knowledge proof

Another technology that has very powerful properties to solve privacy challenges is **zero-knowledge proof** (**ZKP**). ZKP allows a user to construct a mathematical proof so that, when a program is executed on some hidden input known only to that user, it has a particular publicly known output, but without revealing any other information beyond this. **Zero-Knowledge Succinct Non-Interactive Argument of Knowledge** (**Zk-SNARKS**) is an even stronger technology in the ZKP protocol. It is proof that something is true without revealing anything about what specifically makes it true. Zcash is the first ever cryptocurrency that maintains total anonymity. It uses a Zk-SNARKS cryptography implementation. It provides complete anonymity by hiding all knowledge about the transactions. It provides users with a private access control of their specific financial information. It also uses a concept called a **view key**. Users can provide this view key to individuals to get details of the transaction.

Smart contracts and decentralized applications

We discussed Bitcoin and blockchain in earlier chapters, and how this entire technology is the next big innovation after the internet. Besides all the unique features of the blockchain, such as immutability, cryptography, and security, smart contracts make blockchain an even more innovative technology. Besides the P2P network and private key cryptography, blockchain program is something that governs the execution of money flow in a programmatic manner. These programs are a kind of smart contract that remains at the core of blockchain. If you look at a typical standard contract agreement between two parties, it basically dictates the terms of a relationship, where these terms or relationships are then usually enforced by legal entities. On the other hand, smart contracts enforce their relationships with smart code written using cryptographic techniques. In simple words, smart contracts are programs that execute themselves exactly in the way written by their creators or programmers.

This concept was first conceptualized in 1993 by Nick Szabo, a famous computer scientist and cryptographer. He made the analogy of a digital vending machine and explained how users could input anything, such as data or a value, and receive a specific item, similar to a real-world snack or soft drink that we could get from a vending machine. In the case of blockchain, the user would create a smart contract by writing a program and pushing the data to that contract so that it could execute the desired command.

Understanding smart contracts

Smart contracts are at the core of blockchain technology. These are programs written in Turing-complete programming languages and are capable of self-verifying and self-executing agreements that can function autonomously or without any external intervention. In layman's terms, if we consider Bitcoin as digital money, a smart contract is highly programmable digital money. A smart contract is a piece of code that is stored in the blockchain, is triggered by the blockchain transactions, and which then reads or writes data from/to that blockchain's database.

The network of nodes will only validate transactions if certain conditions are met, but Bitcoin is limited to dealing only with the currency use case. But, what about many nonfinancial use cases or even financial use cases where money is not a center point but is involved at the triggering point? Ethereum, one more variant of blockchain that was forked from Bitcoin and modified further, replaced Bitcoin's restricted language with a Turing-complete, more robust language that allows for the writing of extensive smart contracts.

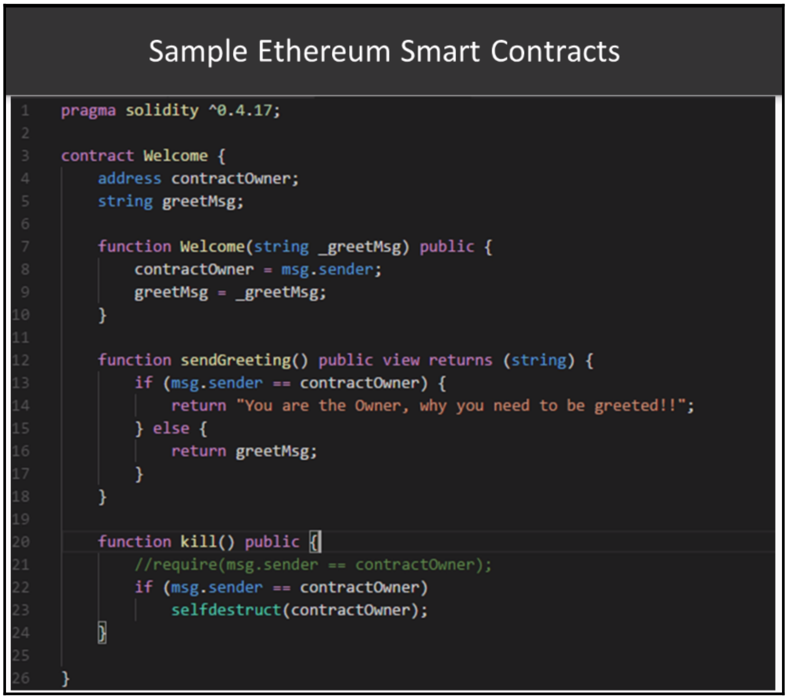
Workings of smart contracts

Now, let's look briefly at the following factors and conditions that trigger the working of a smart contract:

- **Agreement**: An option contract between two or more parties is written, coded, and deployed on the blockchain platform. The individual parties involved can remain anonymous, but the contract is written in the public ledger and remains unchanged.
- **The triggering or execution point**: Any triggering event, be it within the blockchain or outside of the blockchain, gets the contract into execution according to the coded terms. A triggering event, for example, could be an expiration date or a renewal date of a contract, a particular price being hit on an exchange, or some cut-off rate being reached on our system.
- **Outcome**: The execution of a smart contract can produce an outcome that will change the state of a transaction, or the state of the blockchain for that matter, for example, a cash ledger. It may also impact on other systems as well.
- **Transparency**: This is another important aspect of contracts. These contracts are immutably available on the blockchain. Regulators can use these on blockchain to understand the activity of the market while maintaining the privacy of the individual parties involved.

Now, let's look at an example of writing a contract. The following are the steps to follow to start:

1. Create a new file and name it `sample.sol`.
2. Next, open the file to begin writing the code, as shown in the following screenshot:



Sample Ethereum Smart Contracts

```
pragma solidity ^0.4.17;

contract Welcome {
    address contractOwner;
    string greetMsg;

    function Welcome(string _greetMsg) public {
        contractOwner = msg.sender;
        greetMsg = _greetMsg;
    }

    function sendGreeting() public view returns (string) {
        if (msg.sender == contractOwner) {
            return "You are the Owner, why you need to be greeted!!";
        } else {
            return greetMsg;
        }
    }

    function kill() public {
        //require(msg.sender == contractOwner);
        if (msg.sender == contractOwner)
            selfdestruct(contractOwner);
    }

}
```

B11516_3_03

Let's see the steps covered in the preceding code:

1. First, let's declare the version of Solidity we'll use, which is `pragma solidity^0.4.17`. This allows the Ethereum platform to compile the contract in a specific version.
2. Then, let's declare a contract and name it `Welcome`.

3. Next, let's declare two instance table variables in this contract. One is the `contractOwner` address. This will capture the address or the account of the owner of this contract, who is going to deploy the contract on the Solidity platform.
4. Next, we declare a `greetMsg` string, which we capture from the contract's owner.
5. Now, we declare a `Welcome` function. Whenever the contract gets deployed on the Ethereum platform, this instance or function gets called publicly.
6. Next, we pass the `_greetMsg` string in this function. We will also make this a public contract.
7. Next, we assign the `contractOwner` variable its value: `contractOwner = msg.sender`. So, whoever has called this function will actually be the message owner, who has a right to create this contract.
8. Likewise, we also assign the value of `greetMsg` as `greetMsg = _greetMsg`. So, what we have done here is we have created a constructor function called `Welcome`, which gets called when the contract gets deployed on the Ethereum platform.
9. Then, we declare one more function called `sendGreeting()`, which will return a string-type variable, `greetMsg`.
10. To see one more function, let's convert `public returns(string)` to a void view function by adding the `public view returns(string)` view.
11. We can slightly tweak this function to become a condition: `if message.sender == contractOwner`. This will return `Hello Mr. Owner why you need to be greeted!` to the owner, or else it will return `greetMsg`.
12. Again, we will declare one more public function called `killContract()`.
13. Then, we give a condition, `if message.sender == contract Owner`, and assign a task, `selfdestruct(this)`. So, unless the owner of the contract calls this kill contract function, it will disturb the contract from the Ethereum platform.

TIP

This is very important so you can decide the conditions in which you want to resolve the contract from the platform. So, there you can have a time-bound contract being created there.

So, that was an example of how you write detailed smart contracts.

Decentralized applications

Since its inception, the application of the blockchain has already increased a lot of expectations from every industry and it also promises to be more prevalent in most innovative technologies. It has a lot to offer in terms of immutability, security, cryptography, distributed ledgers, and so on. We should not ignore the fact that blockchain can solve specific issues with immutability, transparency, anonymity, and security. However, it has its own challenges as well, for example, the speed of a consensus required, the time required to arrive at a consensus, and the replication time across the public ledger.

Challenges and solutions

We have already covered decentralized applications in the previous chapter. Dapps are not owned by anyone, cannot be shut down, and cannot have downtime. So, whenever we want to build a Dapp, we need to keep some considerations in mind, such as that a Dapp has to be a completely open source and operate autonomously, with no entity in charge of the majority of its currency. It has to have protocol changes that are designed to make some overall improvements, approved by all users. It cryptographically stores all of its operations data in a public blockchain, and most importantly, it has to incentivize. You truly need to have a consensus among miners to arrive at a consensus. There has to be some motivation for miners at the same time. If the objective is just to use bring about decentralization, then there are many other ways to achieve it, such as BitTorrent.

So, while blockchain is still evolving and there are many new things being derived, making it more and more mature, we as an entire community need to avoid abusing this technology by not using it everywhere. Rather, there has to be a thorough analysis of a technological, architectural, and design basis as to when and why to use blockchain as a solution to solve a problem. We must not think that it is a one-stop solution that fits all problems.

Summary

In this chapter, we learned about some of the advanced concepts used in blockchain and covered various consensus protocols used in various blockchain implementations. We also looked at some of the key challenges to privacy on blockchain and how solutions such as ZKP can help safeguard privacy. Then, we progressed to discussing smart contracts, one of the core building blocks of blockchain; how they are written; what they are; and how they are executed. We also looked at Dapps, when to use them, and when not to use them. In the next chapter, we will look at some of the general practices used to safeguard Bitcoin and cryptocurrencies in general.

4

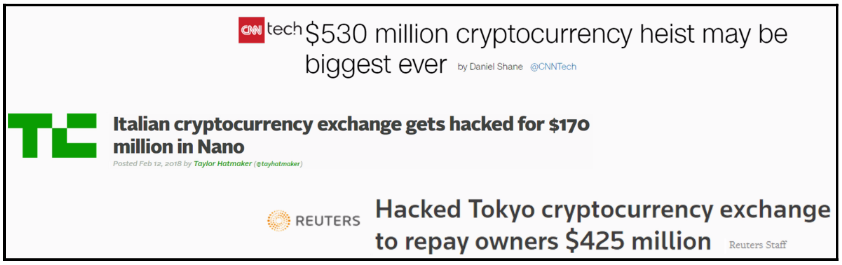
Bitcoin and Blockchain Security

In the preceding chapter, we learned about the fundamentals of Bitcoin and looked at blockchain and some of its advanced concepts. We got a brief overview of various systems, such as centralized systems, decentralized systems, and distributed systems. We also looked at some of the positive features and limitations of decentralized systems, and how they impact various aspects. In this chapter, we will go through some of the following general concepts:

- User security and best practices for Bitcoin
- Hardware wallets
- Physical Bitcoin storage
- Balancing and diversifying investment risks
- Survival of cryptocurrency

Securing Bitcoin and blockchain

Investing in Bitcoin or any other Altcoins is a lucrative option that promises high returns in a short time, subject to risks. That is probably why we see a huge demand for these cryptocurrencies, which also shows us why there are ongoing attacks against exchanges and currency theft. An example of this was when the news was filled with headlines stating that top cryptocurrency exchanges were hacked and currency worth several hundred million dollars was stolen. You can see these headlines in the following screenshot:



$530 million cryptocurrency heist may be biggest ever by Daniel Shane @CNNTech

Italian cryptocurrency exchange gets hacked for $170 million in Nano

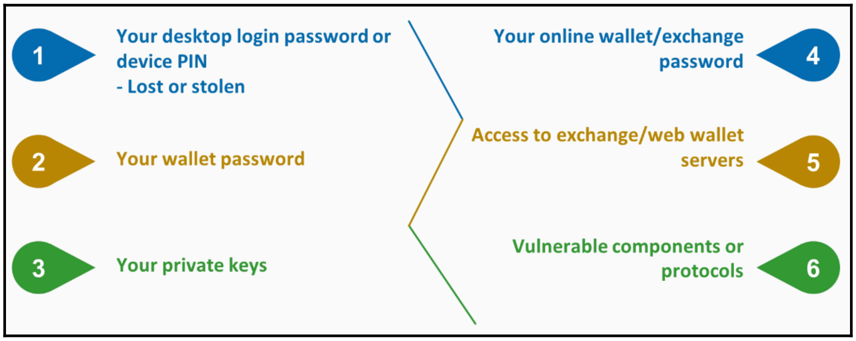
Posted Feb 12, 2018 by Taylor Hatmaker (@tayhatmaker)

Hacked Tokyo cryptocurrency exchange to repay owners $425 million Reuters Staff

The questions that arise are as follows:

- How do we keep currency safe from all such attacks?
- Is there any safe place?
- Are there any do's and don'ts to be followed that can safeguard our currency?

So, most Bitcoin thefts are due to poor wallet or security management. In the following diagram, we can see the things that interest Bitcoin or cryptocurrency thieves:

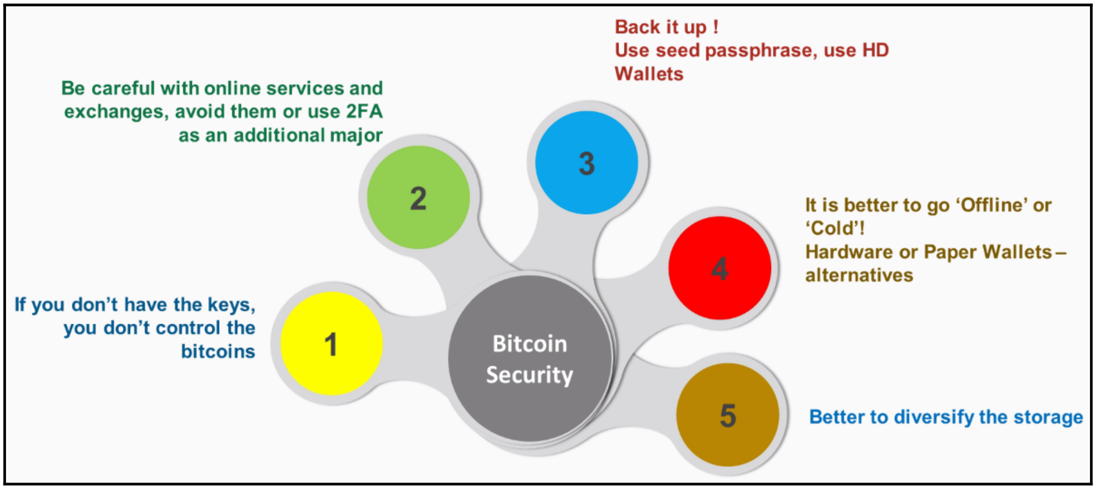

1
Your desktop login password or device PIN - Lost or stolen
2
Your wallet password
3
Your private keys
Your online wallet/exchange password
4
Access to exchange/web wallet servers
5
Vulnerable components or protocols
6

The following items mentioned in the preceding diagram catch the interest of Bitcoin thieves:

- **Your desktop login password or device PIN**: It is as good as someone getting access to your home in your absence and stealing almost everything. Mobile devices are especially vulnerable, mainly because they have a higher chance of getting lost or stolen and, with hacking, they may provide access to the wallets on them.
- **Your wallet password**: Your wallet password is a gateway to your holdings.
- **Your private keys**: Thieves, of course, want your private keys.
- **Your online wallet/exchange password**: This is as good as knowing the password to your online bank account.
- **Access to exchange/web wallet servers**: This includes access to your web wallet servers and exchange.
- **Vulnerable components or protocols**: The vulnerable components or protocols used by online services.

Security practices for your wallet

Let's look at the various best practices to be followed to safeguard your assets if you want to be a revered cryptocurrencies investor or a person that wants to trade in cryptocurrency. Let's look at them very quickly in the following diagram:


Back it up !
Use seed passphrase, use HD Wallets
Be careful with online services and exchanges, avoid them or use 2FA as an additional major
3
2
It is better to go 'Offline' or 'Cold'!
Hardware or Paper Wallets – alternatives
4
If you don't have the keys, you don't control the bitcoins
1
Bitcoin Security
5
Better to diversify the storage

Let's explore all the practices mentioned in the preceding diagram:

- **Secure your private keys**: Any typical Bitcoin transaction needs your private key to unlock its Bitcoin outputs or its value. Bitcoins are stored in wallets. These wallets are collections of public and corresponding private keys, where the public keys are represented by the Bitcoin address. If your Bitcoins are not at a Bitcoin address that you directly control, they are not under your control at all. It is said that if you do not have the keys, you do not have control of the Bitcoins. Basically, you only own the Bitcoins when you own the corresponding private keys. If a third-party obtains one or more of the private keys that are saved in your wallet, they can use any coins previously received by that public-private key pair or combination. Such a transaction doesn't have to be made using your wallet. It can be brought into any device, from anywhere. This is a design feature of Bitcoin that allows, among other things, the ability to import and export addresses between wallets. This is as good as your credit card PIN. You certainly do not want to let an unknown person know your PIN.

- **Beware of online services**: There are thousands of online exchanges today catering to the online trading of cryptocurrencies. When we aren't aware of these exchanges' origins, trusting them is out of the question. To date, 12-bit connections have been hacked and have had Bitcoins stolen from them. This type of invasion seeks a connection to the essence of the servers of the service where the account credentials and wallets are reserved. A simple way to avoid security breaches that are caused by third-parties is to not store cryptocurrencies on an exchange. If your particular trading or investment strategy requires you to preserve the balance of cryptocurrencies on your exchange, you must check the access funds or the exchange accounts daily. However, exchanges such as Coinbase do provide a web wallet service that uses the recommended policies and procedures to safeguard your tokens.

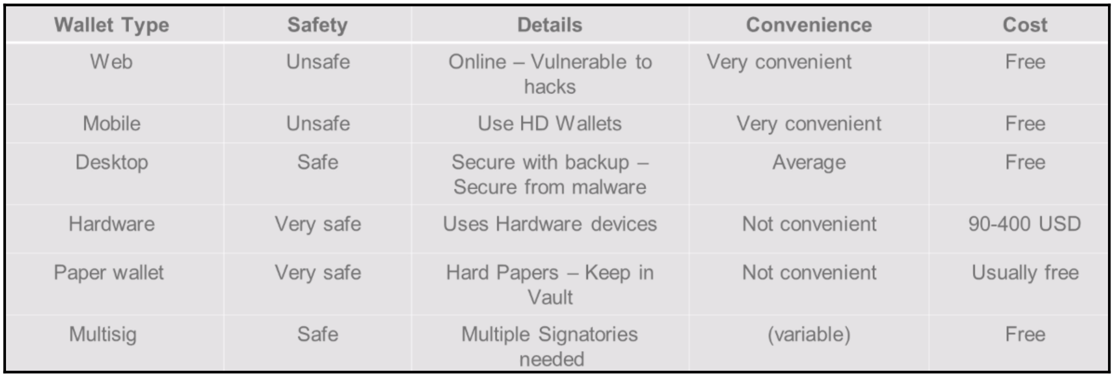
The Bitcoin world has seen a huge number of new users coming into the ecosystem. This always engages all kinds of hackers who try to attack the rookies. The most common Bitcoin scam is a **Bitcoin Doubler**. Operators of such con schemes state that they will give you back 5%, 100%, or even 200% on your deposits in a short space of time. Well, Bitcoin is fairly uncontrolled and nobody will come to your rescue when your savings are lost. This is an important part and an added security part for cryptocurrency investors. It is to do with two-factor authentication. It is necessary that investors use wallets and exchanges that force **two-factor authentication** (**2FA**). This needs a user to confirm their identity with more than a simple password. Users need to use fingerprints, knowledge of personal data, or validation from a secondary device to utilize 2FA, and this feature should be enabled by all users. While this may delay the login time, it may save you from an expensive hacking crisis. Remember that 2FA cannot secure access to your online account, but it can act as a tollgate while carrying out any purchases or sales involving coins.

- **Back it up**: Due to the breakdown of your computer or mobile phone, access to your coins is not possible. Coins that cannot be accessed are treated as lost forever. Backups are a must when handling important data, especially when the data is something to do with your money or cryptocurrencies. This is something that should be naturally followed. A good backup strategy is your safety net against the loss of your Bitcoin wallet due to hardware drive failures or natural disasters. If your hardware drive dies or if your computer is lost or stolen and you don't have a backup of the Bitcoins, they are gone. You can check with your wallet service provider or software about which files to back up. A good strategy is a **3-2-1 strategy**. Number **3** is three backups on two different media devices, such as an external hard drive or a USB flash drive; number **2** is to store them on your paper wallet; and finally, number **3** is to store them at a remote location or your friend's house. This 3-2-1 strategy has often helped people to prevent their cryptocurrencies from being stolen. If a wallet offers protection for your password, ensure that you use it. This feature conceals a wallet file, that is, the `file.dat` file, or something that is the same as the `file.dat` file, which stores private keys and any metadata that may harm your privacy if leaked. Even if an attacker tries to hack into your computer and gets access to the file, it will be of no use as it is encrypted and cannot be used without the password. A word of caution: use a strong password that is difficult to assume or crack. The **Hierarchical Deterministic** (**HD**) wallet uses the HD or VIP protocol, in which a backup has to be performed once, which consists of 12 or 24 human readable words that you can write down and keep in a secure place. Daily backups are not needed and whenever you want to restore your wallet, it will ask for these words in the exact same sequence.

- **Better to go offline or cold**: If you will not use your cryptocurrency for a long time, say a few months or a year or two, you need to keep your currency safe and prevent easy access. You can use offline wallets, as these are the most secure storage, where private keys are both developed and reserved offline. This greatly reduces the danger of coins being stolen by hackers or malignant software. Find the cold storage solution that is suitable for you. If you plan on holding a small amount of Bitcoins for any length of time, say three months or more, the best thing to do is to move them offline and off your computer. A paper wallet is a piece of paper with a private key engraved on it, and it is usually in the form of a QR code. Some paper wallets can be printed, so you can record your balance without importing the private key to a different wallet. You can securely develop a paper wallet and keep it safe in your personal vault. Payment for products and services that are offered by the site are not needed. Next is the hardware wallet—they are tiny devices or smart cards that can be connected to your computer, phone, or USB. This type of wallet is generally the most securely guarded because the private keys are stored offline and they never leave the device at all. Funds can be sent by users from their hardware wallets to exchange and trade them. At the same time, it ensures security for the bulk of their investments. **Trezor**, for example, is a hardware wallet that provides a high level of security without sacrificing convenience. Another benefit is that Trezor can sign a transaction while connected to an online device. That means spending Bitcoins is safe even when using a compromised computer.
- **Diversify your storage**: Diversification is always a way to mitigate risk. Based on your trading pattern and the amount of coins you trade daily, weekly, and monthly, you can store your cryptocurrencies in different wallets. You can use a number of wallets such as on desktops, mobiles, or even an offline wallet. In general, your largest stock can be stored in a hardware wallet, which is more secure. You can alternatively store it in a paper wallet and secure this paper in your personal vault. Some coins can be stored in your desktop or HD wallet, while a small amount of coins can be stored online for regular trading purposes. This makes life easier.

Types of wallets

Let's now compare some of the wallets in the following diagram and see what features they provide us with:



Wallet Type	Safety	Details	Convenience	Cost
Web	Unsafe	Online – Vulnerable to hacks	Very convenient	Free
Mobile	Unsafe	Use HD Wallets	Very convenient	Free
Desktop	Safe	Secure with backup – Secure from malware	Average	Free
Hardware	Very safe	Uses Hardware devices	Not convenient	90-400 USD
Paper wallet	Very safe	Hard Papers – Keep in Vault	Not convenient	Usually free
Multisig	Safe	Multiple Signatories needed	(variable)	Free

We will now look at these wallets and compare the safety and convenience that they provide:

- **Web wallets**: They are relatively unsafe. Since they are online, they're vulnerable to attacks by hackers. These are very convenient and easy to use because they are online, highly available, and free to use most of the time.
- **Mobile wallets**: They are equally unsafe. You can use HD wallets to utilize some security features, using seed words and keeping them safe. These are also very convenient because they are available at your fingertips and are inexpensive.
- **Desktop wallets**: They are a little safer than your mobile wallets because desktops are not publicly accessed that easily. You can secure desktop wallets with backups, which will keep them away from malicious software, or malware, or even Trojans. So, using secure backups is always the key to safeguarding your desktop wallets. These wallets are average in terms of convenience because you have to go to your desktop and access your wallets. Most of these wallets are freely available.
- **Hardware wallets**: They are considered very safe and are nothing but the hardware devices that you possess. They are not usually convenient, because they cannot provide you with easy trading or connectivity to online services. We can also see that there are a variety of hardware wallets available, costing between 90 to 400 US dollars.

- **Paper wallets:** These are very safe until you lose the paper because that leads to the loss of your Bitcoins or your cryptocurrency. Therefore, a hard paper is used, and we should keep them safe in personal vaults or in different locations that are not easily accessible by anybody else. Again, these are not convenient, because they are hard manual paper wallets. They are usually available free of charge, while some websites provide them for a small fee.
- **Multisig wallets:** Next are multisig or multisignature wallets. These are considered safe, as more than one entity, authority, or person needs to sign the transactions for them to be carried out. The usage of the wallet can vary between being easy to use or adhering to a relatively moderate level of complexity, since it depends on more than one person signing a transaction to complete it. Multisig wallets are freely available.

Hardware wallets

Hardware wallets are a type of crypto wallet that reserves the private keys of users in a secured hardware device. They are supposed to be the most heavily protected and safe sorts of wallet. Now, we will look at some of the benefits that they have to offer:

- The first benefit is that the private keys of the user are stored in an area that is safe and has a built-in microcontroller on the device. Therefore, these keys cannot be transferred off the device in plain text format, which is tightly secured and coupled with the microcontroller.
- They are immune to computer viruses that steal from software wallets. This key feature safeguards keys from the outside world because this hardware is not that easy to hack or crack.
- One more benefit is that the keys can then be used securely, which makes it convenient for the user's point of view. This is a relatively easy means of operation, as opposed to a paper wallet, which must be imported to a software wallet when you want to use it.
- Most of the time, the software is open source, allowing the user to approve the entire process of the device. This makes it auditable and transparent.

A hardware wallet can only be accessed through physical contact with the wallet, and each user's private key is stored securely in the wallet.

Workings of a hardware wallet

In order to explain the workings of a hardware wallet, let's look at an example.

We will take as an example the **Ledger Nano S** wallet, which is a well-known hardware wallet. You can see the diagram or the picture of the wallet that comes with a USB extension and can be connected to laptops or computers. When the ledger device turns on for the very first time, it uses an algorithm to figure out how to use a set of 24 regular words to get a seed. They are usually words with letters, for example, four to five letters, which form one word. Basically, there are words, which will be randomly picked up, and it produces a seed. Keys for wallets are generated from the seed.

It also specifies a way to annex these 24 words with an additional passphrase, which counts as word number 25. If no passphrase is selected, an empty one is used. So, it is necessary to always have the 24 words plus one passphrase, which could be empty. Also, remember that a passphrase is different from the passwords that we use in various applications as well. A valid seed is produced when any passphrase is combined with 24 words. It is advisable that the user writes these 24 words down on a piece of paper, usually the one that comes in the box with the ledger, and keeps that paper safe and away from the ledger itself. For example, let's say you have jotted down the four or five digit PIN of your credit or debit card, and you keep the paper along with the debit card or credit card; it is highly possible that someone can get access to your card and the paper, and then get full access to your account. To ensure that this breach doesn't take place, it is advisable to keep the paper on which you have written your PIN away from the card itself.

Now, this developed seed number is used to produce a root key, which is a mix of letters and numbers that cannot be predicted. Every blockchain of cryptocurrency has its own method of producing the root key from the seed. This key is then used to develop a number of private keys that then become cryptocurrency wallets for the cryptocurrency blockchain, which the user is keen on. In addition to that, the ledger device then requires the use of a PIN, which can be a combination of four to eight digits. This is an additional measure taken to safeguard the device. However, if the PIN is wrongly logged in three times in a row on your sequence, the ledger device automatically destroys all the data, making it useless to anyone who has access to it.

If the ledger gets destroyed, stolen, or lost, the question arises about how the user can get access to the keys, the wallet, and the currency in it? The original owner of the device can then use the words on the piece of paper to restore its contents, either on a backup ledger, another ledger, or any software wallet, thus regaining all funds and addresses. This is possible because all we need to do is develop the root key, the 24 words, and the passwords, if provided when creating the words in the seed.

Types of physical Bitcoins

Now, let's look at physical Bitcoins as a concept. Physical Bitcoins have been around for years, but they are not part of the mainstream trading platforms. There are very few companies that are involved in this untried and relatively raw industry. Some try to appeal to consumers through quality and the use of precious metals, such as gold and silver. Some offer good designs at relatively low prices, while some offer neither of these. The market for physical coins is very limited, and this is a place for collectors. Rather than being truly practical, physical Bitcoins are usually marketed as conversation pieces, such as limited series collectibles. At times, these are also referred to as "gifts for geeks". Some of the well-known physical Bitcoins are Casascius, Titan Bitcoin, Alitin Mint, and Cryptomint Coins. There are other physical Bitcoins that are available that can be looked upon as collectibles.

The survival of cryptocurrencies

In this section, we will go through some tips on balancing complete investment portfolios and diversifying the underlying risk. We will also look at the survival of cryptocurrencies.

"Do not put all your eggs in one basket," is a very famous saying that is very true when it comes to money and investment. This is critical when it comes to the cryptocurrency market. There is no specific rule on how one should diversify one's investment; it always depends on the risk appetite of the individual. It is advisable that individuals who are intellectual, conduct research and make their own decisions before investing in cryptocurrencies.

Let's look at the following factors that arise on investing in cryptocurrencies:

- **Volatility**: The crypto market is extremely volatile compared to the stock market. Investing in crypto assets has given very high returns to people over the last few years, making some millionaires. It has also made some losses in the greed of short-term gains at the same time.
- **Divide your terms and conquer**: There is one more concept of dividing your terms and conquering the entire portfolio, which means one must divide the overall portfolio into the following three terms:
  - **Long-term**: Coins that are worth holding for the long term say several months or a few years, are actually something that should be considered in the longer term for investment. Such coins are time-tested and have survived through all the rough waters. Some examples are Bitcoin, Ethereum, and Litecoin. Remember that such long-term coins should be kept safe in cold wallets or vaults.

- **Mid-term**: Coins that are the subject of speculation as to whether they will grow or not are called mid-term coins. You can consider such coins as worth investing in for a few weeks, or more as a mid-term investment. These could include Bitcoin Cash, Zcash, Zcoin, and ICOs, for example, and many other Altcoins. One can also think of making an early investment in some of the ICO crowdfunding. An ICO is similar to an **initial public offering** (**IPO**), the term used in equity markets, shares, and trading. There's a word of caution here. One must do thorough research on any particular ICO before investing in it. Visit company websites for the product, understand what offers they have and read the white papers they have probably published. At times, it is worth doing research on the founding members themselves, such as how much credibility and experience they bring to the industry. Also, check whether they have ICO ratings provided to them by individual third-parties. Most importantly, one must know when to exit from ICOs. What is advisable is that one must buy the ICO when it is published in the market and hyped and sell those when they list in publish exchanges, making a margin difference gain. One more thing to remember would be that not putting more than 5% of the overall portfolio into ICOs is a very good practice to follow.
- **Short-term**: Arbitraging and quick profits are made while investing in short-term investments. This is the most exciting way to use coins. Those with low risk appetites can use the short-term arbitrage method, but then it is better to avoid ICO investment. Constant follow-ups are needed to get clarity on where the market is heading, how the ICOs are doing, which coin is popping up, and more.

The next step would be to understand the risk. It is directly proportional to how much loss one can bear. The more loss one can bear, the higher the risk appetite. Thus, if your risk tolerance is low, your typical overall crypto portfolio investment may include the following:

- **Low risk appetite**: 50% arbitrage, 40% Bitcoins, 8% Altcoins, 2% ICOs
- **High risk appetite**: 50% ICOs, 30% Altcoins, 18% Bitcoins, 2% to 5% in arbitrage

You are the judge of your own investments and risk appetite.

It pays to follow knowledge sources, such as `https://coinmarket cap.com`. This is a good website to use to stay updated as to what is going on in the crypto world and find out more about your investments. It is said that an idea's or a technology's life expectancy is proportional to its age. This concept is called the **Lindy effect**. Let's take an example of a best selling book published in 2017, and let's compare it to the Bible, which has been around for over 300 years now. If you are asked about which book is more likely to still be in print in the next 100 years, the answer would obviously be the Bible, as it has a higher probability of survival. It has nothing to do with the contents of the book, it is just simple math. An idea that has survived for such a long period of time is and will likely continue in the same trend. A new book's contents might be relevant in today's world, but who is to really know if the hype will decline or reduce? The true test of any idea or technology is its survival over time. If the same is applied to Bitcoin, we can say that the longer Bitcoin survives, the stronger the idea of decentralized cryptocurrency becomes. If you look at ATM machines, they have been time-tested over a period of several decades, and now they are a mainstream asset. The same applies to the cryptocurrency world.

After its beginning in 2009, few people gave the Bitcoin blockchain a chance of survival. People were worried about possible attacks against the Bitcoin blockchain. However, it has been 8 years, and not a single hacker has been able to hack the blockchain itself. Although exchanges and wallets were hacked and exploited, which are the peripheral technology stacks or building blocks, the core of Bitcoin has never been hacked. The Bitcoin protocol has not just survived all such attacks, but it has reinforced itself after every attack and is ready and stronger, for the next such attack.

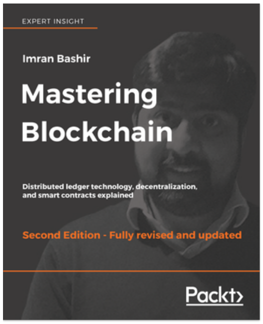
The success of Bitcoin and how it attracted investors from across the globe created opportunities for all Altcoin creators. For how long these artists can survive, is again hidden in the time to come. We should not give these Altcoins any benefit of the doubt, but we should give them time to prove themselves over a period of time.

Summary

This chapter enabled us to understand the features and safety provided by the various crypto wallets. We also looked at how hardware wallets work, some types of physical Bitcoins, the chances of survival of cryptocurrencies such as Bitcoin and Altcoins, and we finally tried to understand how to balance and diversify risks related to investing in crypto tokens.

Other books you may enjoy

If you enjoyed this book, you may be interested in these other books by Packt:


EXPERT INSIGHT
Imran Bashir
Mastering Blockchain
Distributed ledger technology, decentralization, and smart contracts explained
Second Edition - Fully revised and updated
Packt›

Mastering Blockchain - Second Edition
Imran Bashir

ISBN: 978-1-78883-904-4

- Master the theoretical and technical foundations of the blockchain technology
- Understand the concept of decentralization, its impact, and its relationship with blockchain technology
- Master how cryptography is used to secure data - with practical examples
- Grasp the inner workings of blockchain and the mechanisms behind bitcoin and alternative cryptocurrencies
- Understand the theoretical foundations of smart contracts
- Learn how Ethereum blockchain works and how to develop decentralized applications using Solidity and relevant development frameworks
- Identify and examine applications of the blockchain technology - beyond currencies
- Investigate alternative blockchain solutions including Hyperledger, Corda, and many more
- Explore research topics and the future scope of blockchain technology

Building Blockchain Projects
Narayan Prusty

ISBN: 978-1-78712-214-7

- Walk through the basics of the Blockchain technology
- Implement Blockchain's technology and its features, and see what can be achieved using them
- Build DApps using Solidity and Web3.js
- Understand the geth command and cryptography
- Create Ethereum wallets
- Explore consortium blockchain

Leave a review - let other readers know what you think

Please share your thoughts on this book with others by leaving a review on the site that you bought it from. If you purchased the book from Amazon, please leave us an honest review on this book's Amazon page. This is vital so that other potential readers can see and use your unbiased opinion to make purchasing decisions, we can understand what our customers think about our products, and our authors can see your feedback on the title that they have worked with Packt to create. It will only take a few minutes of your time, but is valuable to other potential customers, our authors, and Packt. Thank you!

Index