
BLOCKCHAIN
A TO Z
EXPLAINED
BECOME A BLOCKCHAIN PRO WITH 400+ TERMS
RAJESH DHUDDU
SRINIVAS MAHANKALI
bpb

Blockchain
A to Z
Explained

Become a Blockchain Pro
with 400+ terms

Rajesh Dhuddu

Srinivas Mahankali

www.bpbonline.com

FIRST EDITION 2022

ISBN: 978-93-91030-82-7

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

Divine Dedication

At the lotus feet of Sri Sathya Sai Baba who taught the world

'Hands that help are holier than lips that pray'

'Help Ever – Hurt Never'

'Love All – Serve All'

We dedicate this book to all individuals who have contributed to the advent of Blockchain and its adoption eventually. This book indeed is a tribute to all those with an undying zeal to learn Blockchain, appreciate its relevance and work relentlessly to promote practical applications of Blockchain especially in the midst various nay sayers and non-believers.

About the Authors

Rajesh Dhuddu

Rajesh is an alumnus of Columbia Business School & Sri Sathya Sai Institute of Higher Learning with a Gold Medal in MBA Finance. Driven by his life motto "Help Ever, Hurt Never", Rajesh has mentored several Entrepreneurs, Corporate Executives and MBA Students.

Rajesh has been recognized as one of the Global Blockchain Thought Leaders by Forbes, Lattice80, Thinkers360 and also by several industry bodies like World Economic Forum (WEF), Confederation of Indian Industry (CII), National Association of Software and Services Companies (NASSCOM) & Governments like State Government of Telangana. He spearheaded implementation of several Blockchain Platforms & Solutions globally for Multi National and Trans National Companies including Worlds' Largest Multi Cloud Blockchain implementation to block spam calls and text in partnership with 3 leading Telecommunication companies in India and Telecom Regulatory Authority of India.

He leads Blockchain & Cybersecurity practice for USD 5.2 billion IT giant, Tech Mahindra. He also guides a team of 1000+ highly accomplished Cybersecurity professionals empowering Global customers in USA, EMEA, APJ & India to strengthen their enterprise-wide Cybersecurity posture and build a highly resilient

security organization. He works closely with Global CISOs, advising them to leverage best practices both in technology and operations covering Cloud Security, Network Security, Advance Threat Management, Zero Trust, Offensive Security, Cyber-risk Quantification & SASE.

Linkedin ID: *https://www.linkedin.com/in/rajeshdhuddu/*

Twitter ID: *https://twitter.com/rajeshdhuddu*

Srinivas Mahankali

LinkedIn ID: *https://www.linkedin.com/in/srinivasindia/*

An alumnus from IIT Madras and IIM Bangalore, Srinivas has over 30 years industry experience of which 12 years is in leading IT Solutions in Indian Private & BSE listed organisations. He has taken an active role in promoting Blockchain across Government of India as the one of the first employees to lead Blockchain at NISG an organization promoted by NASSCOM and Government of India.

As the Program Director of the first University certified Post Graduate course in Blockchain in India Srinivas mentored over 500 students across the globe. He has authored over 10 books on Blockchain and emerging technologies including the World's first book to be translated into a Chinese language from English, by Artificial Intelligence bots, Blockchain-The Untold Story. He has also authored books, Blockchain for Non-IT Professionals, Blockchain & Smart cities.

Acknowledgements

We would like to thank our parents, family members, colleagues & acquaintances who extended their colossal support and motivated us to create this great resource.

We thank all our contributors and reviewers who have invested countless hours in collating various terms and reviewing our explanations.

We extend our gratitude to BPB team comprising Manish Jain, Varun Jain, Nrip Jain and others for supporting us completely to publish this book.

We have taken utmost care to list all these names below. Incase, we have missed anyone's name, we apologize for such omission which is either inadvertent or on the account of our thankless memory.

Family Members

Dr Padmanabhaiah, D Parvatavardhani, DSK Satya

Industry Colleagues

Dr Padmanabhaiah, D Parvatavardhani, DSK Satya, CP Gurnani, Rajesh Chandiramani, Vivek Agarwal, Srinivas Pingali, Jayesh Ranjan

IAS, Santosh Mishra IAS, Ramadevi Lanka, Pankaj Diwan, Prasanna Lohar, Julian Gordon,

Contributors and Reviewers

Prof. Lisa Short, Amey Rajput, Dharmen Dhulla, Aman Malhotra, Tina Singh, Anthony Day, Murthy Chitlur, Rajan Kotadi, Debjani Mohanty, Abhinav Garg, Todd McDonald, Ted Hong Kim, Purushottam Kaushik, Brian Beldhorf, Abhinav Garg, Abhishek Bhattacharya, Deepak Agarwal, Sanat Bhat, Varun Singhi.

Community Contributors

As part of this book's pre-launch announcement on LinkedIn, we ran an initiative asking LinkedIn network members to guess a Blockchain term that has not been covered and explained by us. We promised that the network members who will come up with interesting Blockchain terms will be duly acknowledged and the corresponding terms will be featured in this book. Mentioned below are the terms and their contributors. These terms have been explained in their respective sections. Thanks Brendan, Chiranjib, Harsha, Khalifa, Mark and Sunil for your contributions.

contributions.
contributions.
contributions.
contributions.

contributions.
contributions.
contributions.

Preface

Blockchain is catching the attention of masses all over the world, thanks to the spotlight on Bitcoin – the first successful commercial implementation of Blockchain. Adoption of Blockchain both for Public use and Enterprise use is growing by leaps and bounds.

While there are many resources that are available in the form of books, online courses and certification programs that equip one to understand Blockchain and use cases, there are very limited resources to explain key terms and lexicon used in Blockchain. Hence, we made the bold effort to scan the history of Blockchain, trace evolution of Blockchain, mine for terms that are used both frequently and rarely and explain them clearly.

Our efforts have resulted in collating over 400 terms, yes you have read it correctly; and explaining them in simple and lucid manner.

We expect this book to be a comprehensive compendium of Blockchain terms and evolve into a valuable resource for everyone, be it – Students, Academicians, Researchers, Blockchain Practitioners, Crypto enthusiasts, who are interested in learning and mastering Blockchain.

To the best of our knowledge, other re-sources that are available either online or offline, cover and explain at best 30 to 50 terms.

In essence, our book provides 10x value compared to those resources.

This book also acknowledges and explains key contributors to Blockchain, top-20 cryptocurrencies and leading Blockchain protocols. No wonder, we feel that readers of this book will graduate from Blockchain Dummies to Blockchain Pros by assimilating all the terms listed in this book, from A to Z!!

We promise that this book will continue to be a valuable resource over the years through inclusion of new jargons and terms as they appear on the horizon and covering them in subsequent editions.

Happy reading and sharing!!!

Foreword

C.P. Gurnani

MD & CEO, Tech Mahindra

Blockchain, undoubtedly, is the technology that has caught every CEO's attention globally. No other emerging technology has stirred such a massive and disruptive interest than what Blockchain has been able to garner in recent years. Be it on account of Bitcoin, the first commercial application of Blockchain technology, or its innate immense potential to transform numerous business processes and services that touch our daily lives.

In the Cryptocurrency world, Blockchain has not only spawned the Bitcoin network but also nurtured myriad other cryptocurrencies like Ethereum, Ripple, Litecoin, and several others that are changing the world, as we speak. Blockchain has also triggered the advent of fundamentally new applications and business models such as Non Fungible Tokens (NFTs) which ushered in a new trend of Crypto or Digital collectibles.

In the world of Enterprise applications, Blockchain has demonstrated its potential to transform:

Supply Chains by making them anti-fragile,

Payments and International Money Remittances through Stablecoins and Central Bank Digital Currencies

Trade Finance by empowering networks to perform automated & immutable invoice discounting

Digital Identities by securing them via Self Sovereign Identities and;

Media & Entertainment industry by configuring self-executing Contracts & Rights Management.

In Government to Citizens services, Blockchain has demonstrated significant potential to promote much required transparency in Benefits Administration, Title Management and even in Elections & Voting management.

Foreseeing these transformative trends, we officially launched the Blockchain Practice at Tech Mahindra in May 2018 under the able leadership of Rajesh. He is our 'Go to Guy' for all things pertaining to Blockchain in our company.

I personally think Rajesh has a unique quality of creating value in chaotic and uncertain circumstances. In the early days of Blockchain the technology adoption was unclear because regulators globally were either supporting or banning cryptocurrency every other month and Blockchain was related only to Cryptocurrencies. Albeit, Rajesh and his team were able to bring in a vision to find practical and meaningful applications for our various clients across

the Globe. In 2019, the TRAI UCC regulation was a defining moment for Tech Mahindra's Blockchain Unit. In a world full of skeptics and critics of this technology, Rajesh was able to lead not only his team but also technical and business representatives in the Indian Telecommunications ecosystem to establish the World's Largest & Multi Cloud Blockchain network to insulate end customers from Commercial calls and texts.

I am proud to say our blockchain competency is recognized globally for the investment, thought leadership and intellectual property created through research and execution of large scale projects. My most cherished recognition is 2021 Forbes Top 50 Blockchain Companies for Tech Mahindra. Some other recognitions include 6th Annual NASSCOM Technology Award and Hyperledger Certified Service Provider badge.

For Rajesh, giving back to the society is as important as revenue generation. I am always excited to invest in his ideas for Blockchain skills development and enhancement. As a matter of fact, at TechM, in his first 180 days tenure in the company, Rajesh had run over 8 Hyperledger Fabric and Corda classroom trainings across locations in India with over 350 technical participants. He also led the foundation and execution of Blockchain District with State Government of Telangana for Blockchain policy and start up ecosystem development.

I am so happy to see him continuing his journey to contribute to enhancement of Blockchain Knowledge through this book which I believe is a unique collection of over 400 terms and Blockchain lexicon and also first of its kind globally.

This book is not just culmination of the efforts of Rajesh Dhuddu and Co-Author Srinivas Mahankali but also has active inputs and contributions from our blockchain team members - Amey Rajput, Dharmen Dhulla and Aman Malhotra.

My bet on Rajesh as a Blockchain leader has yielded good results and I am sure his and the team's work in this book will be a knowledge enriching read for all those who are keen to advance their learning and master Blockchain.

Praise & Review for Blockchain A to Z Explained

An essential glossary for those wanting to learn about Blockchain, or for those already in the industry looking to expand their knowledge. Rajesh and team have covered everything from Air Drops to ZKPs. You'll soon be serenading colleagues and friends with tales of Bear Whales and Block Rewards; Doges and DIDs; Hashing and HODLing... you get the point. If anyone out there knows 100% of these terms before reading this, send them straight to me!

Anthony Day, Blockchain Partner, IBM

Blockchain body of knowledge is growing very fast. Every day there are new developments, technical advancements and ofcourse emergence of new words. To keep pace with all these, it is quintessential that one understands the technical terms easily. Infact, I have been looking for one book that I can refer to, pretty much like good old days' dictionary that explains everything lucidly. I am delighted that my search for such a valuable resource has ended with this book.

Tina Singh, Chief Digital Officer, Mahindra Finance

Blockchain is an important driver of Digital Transformation. To understand its role fully, its pertinent to understand its concepts, latest developments and terminology. This book will help all Blockchain learners – whether students or professionals to

overcome the lack of understanding of Blockchain jargon and in turns fosters good learning and mastery of the subject.

Dr Srinivas Pingali – Professor of Practice, IIM Udaipur

Blockchain is at the vanguard of the Fourth Industrial Revolution. However, to understand the "why", it is first imperative to understand the "what". Understanding "what'' is heavily contingent on understanding various Blockchain glossary & jargon. This book does exactly that, explaining everything in a comprehensive and engaging manner. Separating the signal from the noise, Rajesh & Srinivas gives readers a comprehensive reference tool to not only appreciate the building 'blocks' of this disruptive technology, but also its significance and impact.

Purushottam Kaushik – Center for the Fourth Industrial Revolution India, The World Economic Forum

Blockchain is the most disruptive technology during the last ten years. Yet a lot of concepts pertaining to blockchain technology are still too difficult to understand. There are many terms in use that might be foreign / alien to software developers and IT professionals. This book provides simple explanations for all blockchain terms. This book makes it possible to fully understand the intricate details about blockchain technologies. I am confident that this book will enable a much broader adoption of blockchain technology among enterprises. A must read for anyone interested in learning more about various use cases of blockchain technology.

Ted Kim, Sr Vice President, Samsung SDS

With bitcoin as its first commercial application in 2008, blockchain has continued to make the headlines across industries and geographies. This has introduced new blockchain jargon and complex terminology which has only grown over the years. This masterpiece will have you well covered. From learning about 'Bakong' to 'Bear Whale' to 'Atomic Swaps' and lots more, you cannot but marvel at the mere exhaustiveness of the terms and topics explained in a simple to learn language. I have no doubt that this thesaurus will make readers the smartest blockchain geeks going around, in the shortest possible time.

Indeed, this book will be your quintessential go-to source for all that's 'Blockchain'!

Rajesh Chandiramani, Sr VP – Digital Business, Tech Mahindra

Advance Comments on A2Z Glossary

Professor Lisa Short

DUniv., Grad. Cert Sc., Bch T&D, Dip. T&A Sys., Adv. Dip. OHS, BA (Economics, Geog., Fin. Mgt.) Dip. Ed.

Founder, P&L Digital Edge Ltd [UK] and Mind Shifting

The speed of digital change is so great that we now have 'revolutions' that take less time than a generation. Blockchain is a foundational technology of the Fourth Industrial Revolution that has jettisoned us into Society 5.0 and onto a vertiginous transformation curve that for some sectors is forty times faster than it was a year ago. It is heralded along with Artificial Intelligence and the Internet of Everything as shifting simple networks based on how we connect and transfer information to smart networks that have the capacity to transfer value. It isn't just about speed and efficiency; it is about changing behaviour, redefining, and redesigning the way we conduct business and are enabled to live our lives.

Blockchain is about valorising trust. Created in the aftermath of the 2008 global financial and trust crisis, it has become the building block of a brave new world where we have replaced our fundamental sense of governance and assurance with a technology that to be honest many don't understand. But blockchain technology is an enabler and becomes an engine of inclusion that

supports our economic and social systems including climate change and inequity. It can provide an identity to the greater than 2 billion people who cannot participate in the financial system. In doing so it converts fragmented communities, to educated, financially included 'thinkers and doers' who can transform nations and support their future.

If people don't understand blockchain they can't participate in its ability to empower and enable us, and perhaps more importantly, us empower it. It is incumbent upon influencers, industry leaders, educators, and credible experts, like me and the authors of this book who've got the knowledge that converges experience, pragmatism, and developmental know-how to share our wisdom in such a way so that adoption becomes ubiquitous.

Wisdom is not devoid of curiosity, effort, lifelong learning, and the joy of seeing the benefits of technology develop. I was not born a digital native. I can remember buying that first computer for my children in the 1990's, turning it on and seeing that green flashing 'dash' of a DOS based computing system and thinking this is grand, now what do I do? To be honest, I had absolutely no idea. Everyone I knew was in the same boat, so we muddled through together. The point is, we did, and we continued to learn, through trial and error and even floundered our way through dial up internet, floppy drives, disc drives, USB's, and CD's. Apples became computers not a piece of fruit, phones turned from bricks to essential pocket-sized accessories and laptops became something that empowered life away from a desk.

Not so many years ago I remember reaching out to a colleague to ask them *on earth was* It was the era of the Initial Coin Offerings [ICO's] and there was lots of technical banter on social media and developer networks. There was a vast and seemingly never-ending lexicon of new terms, words and processes that made me feel like I was in a Kafkaesque nightmare experiencing my worst ever episode of imposter syndrome as I was back in that place of having absolutely no idea. Ruminations about the potential of blockchain were overshadowed by the hype of failed ICO's and the cryptocurrency explosion. It certainly wasn't the gracious introduction such an amazing technology deserved and created a great deal of confusion, misinformation, and misunderstanding.

Had I had a resource that was a simple explainer of any name, term, acronym [and there are hundreds of them] and processes it would have made my journey much easier. This book does just that. It is not just a listed reference text, it represents an ontology of the author's priceless years of experience and learning and collaboration in the industry so that a clear contextual understanding of blockchain can be obtained in one place. If someone can understand the language, they will know the questions to ask to be included.

Rajesh Dhuddu is recognised as making blockchain relevant for the common person. Srinivas Mahankali is focused on enabling easy adoption of blockchain across the world. Together their experience, thought leadership and technical prowess are the reason our paths initially crossed. But it is the impact of their project delivery on society and the multidisciplinary approach they take which led me to know that this A to Z of blockchain is a lexicon that would be as pragmatic as they are and a resource

that every business, decision maker, student, parent, leader, educator, and journalist should include as a 'must have'. I am resolute that until the hype and misinformation is corrected, and terminology understood that the vertical rise in enlightenment cannot occur. Education and access to credible resources are the front door key to blockchain adoption.

Less than 3% of senior academics, government decision makers and board members have science and technology expertise and there is only a fraction of those with a knowledge of blockchain. To quote the French Minister of Economy Bruno Le Maire *I know is that most people talking about blockchain, know nothing about* Never truer word was uttered. This book offers them, and all small to medium enterprises who constitute 99% of the global economy a coalescence of a simple explanations of everything from a POET to a whale to eliminate the arcane language in the industry that can confuse even the best of us.

The A to Z of Blockchain is an important reference text because blockchain terminology can be unduly complicated and highly complex. That becomes a barrier to navigating the exciting frontier of a foundational technology where we can embed innovative ideas and solutions to create a human-centered smart society. Blockchain isn't just a technology, it is a philosophy, and everyone needs to know about the type of systemic changes it can affect and the industries it can disrupt, if you want the systems of the future to work for you.

Professor Lisa Short is recognised as one of the top 150 thought leaders in the world and top 50 leaders and influencers in the

world to follow for her work in blockchain, crypto assets and EdTech and is at the driving force of digital technology ecosystems.

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at business@bpbonline.com for more details.

At you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

BPB IS SEARCHING FOR AUTHORS LIKE YOU

If you're interested in becoming an author for BPB, please visit www.bpbonline.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.

The code bundle for the book is also hosted on GitHub at In case there's an update to the code, it will be updated on the existing GitHub repository.

We also have other code bundles from our rich catalog of books and videos available at Check them out!

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 business@bpbonline.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

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 BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit

Table of Contents

Binance

BIP (Bitcoin Improvement Proposal)
Bit
BITA (Blockchain in Transport Alliance)
Bitcoin
Bitcoin Core
Bitcoin Cash (BCH)
Bitcoin Faucet
Bitcoin Gold (BTG)
Bitcoin.org
Block
Block Cipher
Block Explorer
Block Header
Block Height
Block Propagation
Block Reward
Block timestamp
Blockchain
Blocktime
Bootnode
Bounty
BTC
BTC Escrow
BTD (Buy the Dip)
Bug Bounty
Burrow
Bitcoin Pizza Day

3. C

CA (Central Authority)

4. D

5. E

EXMO
Explorer

6. F

Fast_sync
Faucet
Fault_Tolerance_&_types
Federated_Identity
Fiat_Currency
Filecoin
Flow
FOMO
Fork
Frontier
FUD
Fungible

7. G

Game_Theory
Gas
Gas_Limit
Gas_Price
Gas_Price_Oracle
Genesis_Block
Geth
Ghost_(Greedy_Heaviest_Observed_Subtree)
Github

Go_Lang
Goerli
Gossip

8. H

9. I

15. O

16. P

18. R

R3
Rabbit MQ
React JS
RxJS
REKT
Relayer
Reputation
Rest API
Rinkeby
Ripple
RPC (Remote Procedure Call)
Ropsten
RSI (Relative Strength Index)
Rugging / Rugpull

19. S

Satoshi
Satoshi Nakamoto
Sawtooth
Schnorr
Scrypt
SDK (Software Development Kit)
SegWit (Segregated Witness)
Self-Destruct
Self-Executing
Serenity

Serpent
SGX (Software Guard Extension)

20. T

Prologue

Professor Lisa Short

DUniv., Grad. Cert Sc., Bch T&D, Dip. T&A Sys., Adv. Dip. OHS, BA (Economics, Geog., Fin. Mgt.) Dip. Ed.

Founder, P&L Digital Edge Ltd [UK] and Mind Shifting

The speed of digital change is so great that we now have 'revolutions' that take less time than a generation. Blockchain is a foundational technology of the Fourth Industrial Revolution that has jettisoned us into Society 5.0 and onto a vertiginous transformation curve that for some sectors is forty times faster than it was a year ago. It is heralded along with Artificial Intelligence and the Internet of Everything as shifting simple networks based on how we connect and transfer information to smart networks that have the capacity to transfer value. It isn't just about speed and efficiency; it is about changing behaviour, redefining, and redesigning the way we conduct business and are enabled to live our lives.

Blockchain is about valorising trust. Created in the aftermath of the 2008 global financial and trust crisis, it has become the building block of a brave new world where we have replaced our fundamental sense of governance and assurance with a technology, that to be honest, many don't understand. Blockchain technology

is an enabler and becomes an engine of inclusion that supports our economic and social systems including climate change and inequity. It can provide an identity to greater than 2 billion people who cannot participate in financial systems. In doing so it converts fragmented communities, to educated, financially included 'thinkers and doers' who can transform nations and support their future.

If people don't understand blockchain they can't participate in its ability to empower and enable us. Thus, it is incumbent upon influencers, industry leaders, educators, and credible experts, like me and the authors of this book who've got the knowledge that converges experience, pragmatism, and developmental know-how to share our wisdom in such a way that adoption becomes ubiquitous.

Wisdom is not devoid of curiosity, effort, lifelong learning, and the joy of seeing the benefits of technology develop. I was not born a digital native. I can remember buying that first computer for my children in the 1990's, turning it on and seeing that green flashing 'dash' of a DOS based computing system and thinking this is grand, now what do I do? To be honest, I had absolutely no idea. Everyone I knew was in the same boat, so we muddled through together. The point is, we did, and we continued to learn, through trial and error and even floundered our way through dial up internet, floppy drives, disc drives, USBs, and CDs. Apples became computers not a piece of fruit, phones turned from bricks to essential pocket-sized accessories and laptops became something that empowered life away from a desk.

Not so many years ago I remember reaching out to a colleague to ask them “What on earth was blockchain?”. It was the era of the Initial Coin Offerings (ICOs) and there was lots of technical banter on social media and developer networks. There was a vast and seemingly never-ending lexicon of new terms, words and processes that made me feel like I was in a Kafkaesque nightmare experiencing my worst ever episode of imposter syndrome as I was back in that place of having absolutely no idea. Ruminations about the potential of Blockchain were overshadowed by the hype of failed ICOs and the cryptocurrency explosion. It certainly wasn’t the gracious introduction of such an amazing technology and created a great deal of confusion, misinformation, and misunderstanding.

I had a resource that was a simple explainer of any name, term, acronym (and there are hundreds of them) and processes it would have made my journey much easier. This book does just that. It is not just a listed reference text, it represents an ontology of the author’s priceless years of experience and learning and collaboration in the industry so that a clear contextual understanding of blockchain can be obtained in one place. If someone can understand the language, they will know the questions to ask to be included.

Rajesh Dhuddu is recognised globally as making blockchain relevant for the common person. Srinivas Mahankali is focused on enabling easy adoption of blockchain across the world. Together their experience, thought leadership and technical prowess are the reason our paths initially crossed. But it is the impact of their project delivery on society and the multidisciplinary approach they

take which led me to know that this A to Z of blockchain is a lexicon that would be as pragmatic as they are and a resource that every business, decision maker, student, parent, leader, educator, and journalist should include as a 'must have'. I am resolute that until the hype and misinformation is corrected, and terminology understood that the vertical rise in enlightenment cannot occur. Education and access to credible resources are the front door key to blockchain adoption.

Less than 3% of senior academics, government decision makers and board members have science and technology expertise and there is only a fraction of those with knowledge of blockchain. To quote the French Minister of Economy Bruno Le Maire "all I know is that most people talking about blockchain, know nothing about blockchain!". Never truer word was uttered. This book offers them, and all small to medium enterprises who constitute 99% of the global economy a coalescence of a simple explanations of everything from a POET to a whale to eliminate the arcane language in the industry that can confuse even the best of us.

This book is an important reference text because blockchain terminology can be unduly complicated and highly complex; that becomes a barrier to navigating the exciting frontier of a foundational technology where we can embed innovative ideas and solutions to create a human-centered smart society. Blockchain isn't just a technology, it is a philosophy, and everyone needs to know about the type of systemic changes it can affect and the industries it can disrupt, if you want the systems of the future to work for you.

Professor Lisa Short is recognised as one of the top 150 thought leaders in the world and top 50 leaders and influencers in the world to follow for her work in Blockchain, Crypto assets and EdTech and is the driving force of digital technology ecosystems.

CHAPTER 1

A

Adam Back

He is a well known Cypherpunk, Cryptographer and widely recognized for his invention Hashcash a protocol that is used to identify email spam and control it. He proposed Hashcash in 1997 which was used by Satoshi Nakamoto, Bitcoin's inventor, to develop Proof of Work (PoW) consensus protocol. PoW is used in Bitcoin network as part of mining algorithm. He is also known as one of the first two people contacted by Satoshi Nakamoto for developing Bitcoin protocol. Adam Back is currently the CEO of Blockstream, a company that he co-founded in 2014. Blockstream is focused on building crypto financial infrastructure based on Bitcoin.

Address

In Blockchain world, an address would typically be a hashed version of the “public key”, which will be referred to by an individual or a platform, in order to transfer any cryptocurrency to a wallet. It is a combination of unique numbers and letters and works similar to an email address. Its like a bank account for cryptocurrency asset. In a public blockchain, address can also be used to perform analytics on a wallet as it is sufficient to trace assets in the wallet. In Bitcoin world, different address formats are used. Eg: P2PKH (addresses start with number 1) - 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2.

AES (Advanced Encryption Standard)

Also known by its original name Rijndael, Advanced Encryption Standard was developed by two Belgian cryptographers Vincent Rijmen and Joan Daemen. It is based on a design principle known as substitution - permutation network, made popular in 2001. Development started in 1997 when the need for alternate to Digital Encryption Standard (DES) was felt as DES was beginning to become vulnerable to brute force attacks. It is used in Software and Hardware globally to protect sensitive data in areas of government computer security, cybersecurity and electronic data protection. 3 different versions are available AES 128, AES 192 and AES 256. 128, 192 and 256 represent the key length that is used to encrypt and decrypt information. AES 128 uses 128 bit key length.

Air Drop

Air Drop is a popular marketing campaign or technique used in Initial Coin Offerings (ICOs) whereby a certain allotment of the native cryptocurrency (tokens) is set aside for free distribution and given to contributors and the community in general. This is mostly done to increase awareness, create early value for tokens as recipients will begin to trade their airdropped tokens. It also promotes participation in ICOs, Blockchain network or enhance activities on the platform. Cryptocurrency start-ups have traditionally airdropped tokens to the wallet holders on Bitcoin and Ethereum networks. Uniswap (UNI) airdrop is believed to be one of the most lucrative airdrops in recent times.

Air Gapping

When an individual or an entity is highly concerned about the security of any sensitive data or valuable asset held digitally like tokens and cryptocurrencies, they typically ensure physical separation of their devices from unsecure networks. This helps prevent likely cyberattacks that originate from unsecured networks or unauthorized access.

Alan Turing

Regarded as the Father of Modern Computer Science, Alan Mathison Turing's work led to the origin of Turing completeness. In the Blockchain world, Turing completeness means that the protocol is able to use its code base to perform any task as long as it has correct instructions, enough time and processing power. In essence, it allows writing programming loops. Turing completeness became prominent when Ethereum claimed it is Turing complete while Bitcoin is not. In reality, Bitcoin is Turing complete. Turing completeness helps to protect the data to avoid possible information thefts, enhances security of the system from hackers and offers safe transaction system.

Alt Coins / Alt Tokens/ Alternate Coins

They represent all cryptocurrencies other than Bitcoin. There are various attributes that differentiate alternate coins from Bitcoin such as Consensus mechanism, Smart Contracts, Low price volatility or no volatility at all. There are more than 10,000 alternate coins trading in over 350 exchanges globally

Anti-Fragile

An anti-fragile asset performs better when there is risk and uncertainty, and gains strength from adverse events. This concept was created by the famous author Nasim Nicholas Taleb. He said that “some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stresses and love adventure, risk and uncertainty”. A classic example is Bitcoin (BTC), it has become stronger with every price hit it has suffered over the years.

API (Application Programming Interface)

An Application Programming Interface allows any system to fetch from or push data to a third-party system. Prevalence of APIs has opened multiple possibilities across segments. In Banking, Open API Banking has resulted in creation of many innovative products & services by Fintechs and Banks leading to improved customer engagement, enhanced transaction security and increased convenience.

Ashdraked

Ashdraking is a complete loss of a crypto investor's capital as a result of shorting Bitcoin where the aim is to sell Bitcoin at a higher price and buy it back at lower price. The term is named after "Lord Ashdrake", a pseudonymous Romanian Bitcoin trader who used to short Bitcoin - betting that its value would decline. Initially he made large profits as Bitcoin declined in 2014 - 2015. Then he shorted Bitcoin at $300 expecting prices to drop. On the contrary, Bitcoin prices went upto $600 in a few weeks and he lost lots of money.

ASIC (Application Specific Integrated Circuit)

An Application Specific Integrated Circuit is particularly built for a specific computational use rather than being general-purpose. These have become very popular and are used in mining cryptocurrencies as mining on personal computers is difficult. They are more efficient than General Processing Units (GPUs). Once a cryptocurrency specific ASIC is released, mining without ASIC is usually unprofitable.

Asymmetric Keys

Asymmetric keys is the use of two distinct or separate public and private keys (keys are different and not same as is the case with Symmetric keys). Public key is used for encryption and this can be decrypted only by a private key. Public and Private keys are mathematically connected with each other and their relationship differs from one algorithm to another. These keys in cryptocurrencies ensure that transaction sources are legitimate and hackers cannot steal the funds. In Bitcoin, the wallet address is a hashed version of the corresponding public key. It proves the ownership of address to receive funds / tokens / coins.

ATH (All Time High)

All Time High for a cryptocurrency or any stock price is the maximum price that the asset has reached as on current date. For Eg, Bitcoin reached an ATH of USD 19,783 in 2017 and then an ATH of USD 61,712 in March, 2021.

ATL (All Time Low)

All Time Low is the lowest price of a cryptocurrency or any stock till date. This is used as a measure to understand the performance of an asset and the relative changes in the price.

Atomic Swaps

An atomic swap is when two cryptocurrencies can be traded amongst each other i.e. converted from one into another without the intervention of a third-party platform or exchange. They are made wallet to wallet in a fully person to person manner. They are called atomic as it results in either successful completion of swap and each trader receives the other's funds or nothing happens with both traders keeping their respective funds. Tier Nolan who accomplished this in 2013 is widely considered as inventor of atomic swaps. The first atomic swap was established between Bitcoin and Litecoin.

ABCI (Application Blockchain Interface)

The purpose of ABCI (Application Blockchain Interface) is to provide a clean interface between any finite, deterministic state transition machine on one computer and the mechanics of a blockchain-based replication engine across multiple computers also known as consensus engine.

AKS (Azure Kubernetes Service)

AKS is an open-source fully managed container orchestration service available on the Microsoft Azure public cloud that can be used to deploy, scale and manage Docker containers and container-based applications in a cluster environment. It helps in setting up and managing containerized applications in seconds and was released on 8th March 2019.

CHAPTER 2

B

B money

B-money was one of the earliest cryptocurrencies, which was never launched officially. B-money endeavored to provide many of the same services and features (anonymous, distributed cash system) that cryptocurrencies of today provide. It was invented by Wei Dai. He is a member of Cypherpunks and co proposed VMAC message authentication algorithm. The smallest unit of Ether is named as Wei in his honor. 1 Wei is one quintillionth of an Ether.

BAAS (Blockchain As A Service)

BAAS is the third-party creation and management of cloud based networks for companies in the business of building blockchain applications. These third-party services are a relatively new development in the growing field of blockchain technology.

IBM, AWS, Azure, Oracle, SAP, Alibaba, Stezy, Zeeve, Settlemint, Chainstack are some of the leading Blockchain as a Service Providers across the world.

Bakong

Bakong is the first Central Bank Digital Currency (CBDC) launched by The National Bank of Cambodia. This was co-developed by Japanese fintech firm SORAMITSU and launched on Oct 28, 2020. Bakong supports transactions in riel and dollars and it has its own mobile app for transactions.

Bear Trap

A bear trap starts with a group of traders selling a large number of cryptos. This makes other traders sell since they suspect a price correction. This causes the price to fall further. That's when the bear trap is released when the earlier sellers buy back the crypto at a lower price. Bear traps can happen over hours or days.

Bear Whale

A person in Crypto market who places a huge quantity to sell at a discount to market price, which pushes market prices to lower levels. This event has occurred in Bitcoin in the year 2014 where an individual known as Bearwhale lost faith in Bitcoin and transferred 30,000 coins to Bitstamp and placed a sell limit order at USD 300 per coin while market price was USD 350.

Besu

Hyperledger Besu is an Ethereum client designed to be enterprise-friendly for both public and private permissioned Blockchain use cases. It can also be operated on test networks such as Rinkeby, Ropsten, and Görli. Hyperledger Besu includes several consensus algorithms including Proof of Work (PoW) and Proof of Authority (IBFT, IBFT 2.0, Etherhash, and Clique). Its comprehensive permissioning schemes are designed specifically for use in a consortium environment.

BFT (Byzantine Fault Tolerance)

BFT is the property of a system that is able to resist the class of failures derived from the Byzantine Generals' Problem. This means that a BFT system is able to continue operating even if some of the nodes in Blockchain network fail or act maliciously. It is used as one of the consensus mechanisms in Blockchain networks to protect Blockchains from manipulation by rogue nodes or unknown actors. Practical Byzantine Fault Tolerance was introduced by Miguel Castro and Barbara Liskov at MIT Laboratory and used by Blockchain protocols – Hyperledger, Stellar and Ripple.

Binance

Binance is a cryptocurrency exchange that provides a platform for trading various cryptocurrencies. As of January 2018, Binance was the largest cryptocurrency exchange in the world in terms of trading volume. Binance was founded by Changpeng Zhao, a developer who had previously created high frequency trading software. Binance has also launched two cryptos developed internally – Binance Coin (BNB) with a market cap of over USD 50 billion and Binance Smart Chain (BSC). BNB can be used to pay exchange fees on Binance for various transactions.

BIP (Bitcoin Improvement Proposal)

It is a standard for proposing changes to Bitcoin protocol. They include consensus related critical changes like soft fork and hard fork protocol upgrades, bitcoin software implementations such as modifications pertaining to backing up seed formats and peer to peer layer. The first BIP – BIP 0001 was proposed by Amir Taaki in the year 2011. BIP 141 also known as Segragated Witness or SegWit has resulted in increasing Block size to address size limitation problem that reduced Bitcoin transaction speeds.

Bit

Bit is a common unit used to designate a sub-unit of a bitcoin - 1,000,000 bits is equal to 1 bitcoin (BTC). This unit is usually more convenient for pricing tips, goods and services. It is also known as Micro bitcoin. However, smallest unit of Bitcoin is Satoshi and 100 Satoshis make 1 Bit.

BITA (Blockchain in Transport Alliance)

The Blockchain in Transport Alliance (BiTA) is a standards and advocacy organization to help educate, advocate, and establish standards for blockchain applications in the Transportation industry. It was founded in August 2017. BITA has nearly 500 members from 3PLs / 4PLs, Air Freight, Logistics, Maritime and other service providers associated with the transportation industry in over 25 countries, that collectively generate over $1 trillion in revenue annually.

Bitcoin

Its world's first Decentralized Peer to Peer Electronic Cash System introduced by leveraging Blockchain, Distributed Ledger Technology. It was first presented to the world through a White Paper titled "A Peer to Peer Electronic Cash System" by Satoshi Nakamoto in the year 2008. It solved the problem of double counting that was prevalent with currencies issued through computers which is not the case with Fiat money (currency issued by Central Banks) where Central Bank as intermediary prevents double counting through serial numbers on currency notes. Bitcoin was invented to protect small and medium sized merchants from fraud and chargebacks pertaining to e-commerce transactions and promote peer to peer micro-transactions with low processing fees. It's a truly decentralized network where no single party owns or controls Bitcoin and every one can contribute. It's the first commercial implementation of Blockchain.

Bitcoin Core

It is the software that powers Bitcoin and developed in C++ by Gavin Andresen. He took up the role of lead developer after Satoshi Nakamoto stopped corresponding in 2010. Included in the software is a secure digital wallet that can be used to store and transact Bitcoins. Bitcoin Core helps to keep Bitcoin decentralized and identifies the chain that contains valid transactions.

Bitcoin Cash (BCH)

Bitcoin cash is a fork of Bitcoin. It is a spin-off or altcoin and was created on August 1, 2017 to accommodate larger block sizes so that more transactions can be allowed into a single block. It was spun off as the some of the Bitcoin developers didn't agree on increasing the original Bitcoin network capacity. As a result, the Bitcoin network became slow and expensive. BCH network now supports up to 32 MB blocks. Fork was created at Bitcoin block 478558. Like Bitcoin, BCH supply is capped at 21 million units. BCH offers faster transactions, a network without congestion and low transaction fees.

Bitcoin Faucet

A site run by Gavin Andresen to make Bitcoin popular. The visitors to the website had to complete a captcha to earn 5 Bitcoins. This was done with an intention to ensure that Bitcoin reached a wide audience who could make use of it. 19,700 Bitcoins were distributed free of cost through this faucet till the time it was closed in the year 2012. There were other free Bitcoin faucets such as FreeBitcoin.in, Cointiply and Faucethub.

Bitcoin Gold (BTG)

BTG is a hard fork of Bitcoin created on October 24, 2017 at block height 491407. BTG is a cryptocurrency with Bitcoin fundamentals, mined on common Graphic Processing Units (GPUs) instead of specialty ASICs. ASICs tend to monopolize mining to a few big players, but GPU mining means anyone can mine again restoring decentralization and independence.

Bitcoin.org

Bitcoin.org is a community funded project. It was originally registered by Satoshi Nakamoto and Martti Malmi. From 2011 to 2013 this was used to release new versions of Bitcoin software now called Bitcoin core. Today it is an independent open-source project with worldwide contributors. It helps people to understand accurate descriptions of Bitcoin properties, potential uses and limitations. It also maintains transparency with regards to events that impact Bitcoin network and improve its worldwide accessibility.

Block

Blocks are files where blockchain transactions are recorded permanently. Block is like a page of a ledger or record book. Each time a block is completed, it gives way to the next block in the blockchain. Blocks can also be created based on predefined time intervals like one block is created every 10 minutes in Bitcoin. A block is thus a permanent store of records which, once written, cannot be altered or removed. Current block height in Bitcoin is 676570. Blocks can be of different sizes varying from 1 MB to 8 MB.

Block Cipher

A block cipher encrypts data in specific sized blocks unlike stream ciphers where encryption is bit by bit. Most popular block ciphers are Digital Encryption Standard (DES), 3DES and Advanced Encryption Standard (AES). AES encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits.

Block Explorer

Block explorer is a blockchain search engine that allows anyone to search details about any blockchain transaction. A block explorer is an online tool to view all the transactions that have taken place on the blockchain, the current network hash rate, transaction growth as well as the activity on the blockchain addresses and other useful information. Bitcoin Explorer and Etherscan are good examples of Block Explorers for Bitcoin and Ethereum respectively.

Block Header

A block header is used to identify a particular block on an entire blockchain and is hashed repeatedly to create proof of work for mining rewards. A blockchain consists of a series of various blocks that are used to store information related to transactions that occur on a blockchain network. Constituents of Block Header are: Timestamp (4 bytes), Version Number (4 bytes), Merkle Root (32 bytes), Difficulty Target (4 bytes), Nonce (4 bytes), Previous Block Hash (32 bytes).

Block Height

Block height represents the number of blocks that were confirmed in the entire history of a particular blockchain network - from the genesis block (or block zero) until the most recent one. Unlike the genesis block, all other blocks contain a reference (hash) to the block that preceded it, and the block height is the number of each block in that sequence. The block height of the genesis block is #0, and the block height of the first block mined is #1. At the time of writing this description, Block Height of Ethereum is 12,657,904.

Block Propagation

The process of sharing Block with the network after it is mined is called Block Propagation. It involves an information sharing process where one miner sends the Block to peers who share it with few more until Block reaches the entire network. The average time taken for the new block to reach majority of nodes in the network is referred to as Block Propagation Time.

Block Reward

Block reward is a cryptocurrency reward to a miner when he/she successfully validates the latest block. The block reward is made of two components: the block subsidy and the transaction fees. The block subsidy consists of newly generated coins and represents the biggest part of a block reward. The other part is made up of all fees paid by the transactions that are included in the block. In Bitcoin, the Block reward currently is 6.25 BTC for every valid block mined. However, this changes and gets half of the reward amount, every 4 years or every 210,000 blocks are mined

Block timestamp

Every block contains a timestamp based on Unix time. The timestamp helps in tracking variations in block hashes and makes Blockchain manipulation difficult for bad actors. Each timestamp also includes the previous timestamp in its hash thereby forming a chain and reinforcing the earlier ones.

Blockchain

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. By facilitating secured track, trace and trade of virtually anything of value in a trusted manner between parties, hitherto unknown to each other inside a network, Blockchain Technology vastly reduces risk and also cuts costs for all involved.

It is a system of recording information in a manner that makes hacking or cheating the information difficult. It is essentially a record of transactions contained in a ledger maintained in Blocks that are replicated or distributed across the entire network. Thus changes are committed on the ledger only after consent for such changes is obtained by every participant in the network. The records in a Blockchain are therefore, tamper evident. Blockchain is also known as Distributed Ledger Technology (DLT). Public, Private and Hybrid (Consortium) are different types of Blockchains. Bitcoin, Ethereum and Litecoin are Public Blockchains, Hyperledger and Corda are Private Blockchains and Enterprise Etherium Alliance and TradeLens are Hybrid Blockchains

Blocktime

It is the time taken to create the next block in Blockchain. It is 10 minutes in the case of Bitcoin. Blocktime varies from one Blockchain protocol to another. In Ethereum, average Blocktime is 13.30 seconds and has been rising over the years.

Bootnode

Bootnode is used for Blockchain installation, running configurations, and managing updates. It is also used as a regular node to scale other nodes or discover them. It helps in discovering peers.

Bounty

A marketing strategy used in case of Initial Coin Offerings (ICOs) where incentives are offered to participants for various activities associated with ICOs especially in promoting them. After ICO completion, Bounty program can be used to obtain feedback on project code from external developers or as a reward to promote ICO or project in media channels.

BTC

The short code used to refer Bitcoin.

BTC Escrow

An intermediary between the participants in Bitcoin or crypto transactions. When a person decides to buy some goods or services by paying in Bitcoins, he / she sends those Bitcoins to an escrow service and it is kept in the system till the goods or services are provided by the seller. Once the transaction is completed, Bitcoins stored in escrow system are automatically sent to the seller.

BTD (Buy the Dip)

Slang used by cryptocurrency traders to indicate buying a particular cryptocurrency when its price dips or is on decline.

Bug Bounty

It's an initiative through which individuals who identify and report bugs in a program, code and application are rewarded. It helps in finding vulnerabilities before they become security issues. Intel, Facebook, Cisco, Apple, Dropbox and others have been running such programs successfully. Payments range from a few hundred dollars to thousands of dollars. Binance, one of the world's leading Cryptocurrency exchanges offers USD 200 to USD 10,000 per vulnerability identified and maximum reward is USD 100,000.

Burrow

Hyperledger Burrow is a permissioned Ethereum smart contract Blockchain node focused on simplicity, speed, and developer ergonomics. It supports both Ethereum Virtual Machine (EVM) and Web Assembly (WASM) based smart contracts and uses Byzantine Fault Tolerance (BFT) consensus via the Tendermint algorithm. Features include Proof of Stake support, On Chain Governance, Javascript client library and many others.

Bitcoin Pizza Day

May 22 is known as Bitcoin Pizza Day when in 2010 developer Laszlo Hanyecz from Florida, US bought two pizzas from Papa Johns with bitcoins and offered 10,000 BTC, equivalent to about USD 30 at the time. Value of this transaction is worth USD 580 million today considering the current price of Bitcoins.

CHAPTER 3

C

CA (Central Authority)

A Central Authority in any system in an organisation, an agency or a set of persons, designated to play a key facilitating role in the implementation and operation of the system. Central Authority takes the responsibility of undertaking activities that are designed to protect the members and users of the system. Government and Regulatory agencies, IT administrators, and Central Banks are some of the examples of a 'Central Authority' acting as a fulcrum around which large operations are undertaken.

CA in Blockchain (Certification Authority)

In Blockchain systems, the Central Authority's server guarantees the uniqueness of the addresses of participating entities by issuing them certificates recognized in the respective systems. It employs Certificate Authority to achieve this purpose. In cryptography, a Certificate Authority or Certification Authority is an entity that issues digital certificates. These certificates certify the ownership of a public key by the named subject mentioned in the certificate. In addition to user enrollment, CA also manages transactions invoked on Blockchain and Transport Layer Security (TLS) connections between various users in Blockchain.

CAP Theorem

Consistency (Uniform & identical view of data for all clients), Availability (Continuous performance and uptime in presence of node failures) and Partition tolerance (Accurate performance and integrity of data despite node partitioning) are some of the key features of distributed systems. As per CAP theorem, any distributed system/database can offer only 2 of the above 3 mentioned properties choosing to offer C&A, A&P or P&C at any point in time. For example, Permissionless Blockchains such as Bitcoin, Ethereum chose to offer Availability and Partition tolerance while sacrificing immediate Consistency, thus offering 'eventual consistency' of data stored.

Cardano

Cardano is a cryptocurrency network and open-source project that aims to run a public blockchain platform for smart contracts. Cardano's internal cryptocurrency is called Ada. The development of the project is overseen and supervised by the Cardano Foundation based in Zug, Switzerland. It was launched in 2017 by Charles Hoskinson, a co-founder of Ethereum and BitShares.

Calibra

Calibra is the blockchain division of Facebook. It will allow Facebook to enable digital payment to its users. Calibra team is building a digital wallet for Facebook's apps, which will eventually hold the Diem (formerly Libra) digital currency, but Facebook won't control the coin. Its not clear whether Facebook is actively pursuing this project.

Caliper

Hyperledger Caliper is a Blockchain tool hosted by Linux Foundation. It lets you compute performance of specific Blockchain implementations by leveraging a set of predefined use cases. Caliper can also generate reports on different performance factors, including resource utilization, transaction latency, and transactions per second (TPS).

Casper

The Casper Network is the first live proof-of-stake blockchain built based on the Casper CBC specification. Casper is designed to accelerate enterprise and developer adoption of blockchain technology today and evolve to meet user needs in the future. It fosters core Web3 principles that allow anyone to participate on Blockchain through various apps without monetizing their personal data.

CBDC (Central Bank Digital Currency)

CBDC is a new type of currency that central banks of many countries are experimenting with. This can be a digital form of current fiat currency in Blockchain. This is different from cryptocurrency because it is controlled by the central government. It will be a stable coin whose value will be linked to national currency of the issuing Country / issuing Central Bank. It can be either Wholesale CBDC that is exchanged and traded only between Central Banks and Private Banks or Retail CBDC that is meant for ordinary consumers and citizens; people who will use it for their daily purchases or activities. CBDCs are being promoted with the intent to accomplish Financial Inclusion, Combat Crime, Prevent Illicit activities andReduce the cost of distributing money in economy. China, Cambodia, Sweden, The Bahamas and Switzerland are actively piloting and testing CBDCs.

CDN (Content Delivery Network)

A CDN (Content Delivery Network) is a highly-distributed platform of servers that helps minimize delays in loading web page content by reducing the physical distance between the server and the user. This helps users around the world view the same high-quality content without slow webpages or app pages loading times. Cloudflare, Fastly, Microsoft Azure CDN and Google Cloud CDN are some of the leading CDN providers.

CeFi (Centralized Finance)

CeFi in Blockchain refers to the participation of intermediaries to facilitate crypto-asset exchange transactions between the respective holders. They act on behalf of the owners of the cryptocurrencies or the tokens by facilitating a number of different types of transactions. However, this induces a risk of malpractices by these intermediaries or hacks of holders systems leading to loss, thus acting like a Single Point of Failure. An alternative to this is the DeFi or Decentralized Finance that is facilitated by Decentralized exchanges, that eliminate the need of intermediaries, hence corresponding risks associated with them are also eliminated. However, Decentralized exchanges cannot offer a number of benefits offered by the Centralized exchanges like fiat conversion and Cross chain exchanges.

Cello

Cello is a Blockchain module toolkit from The Linux Foundation. It is essentially an on-demand “as-a-service” deployment model developed for the Blockchain ecosystem. Cello provides a multi-tenant chain service that can work on top of multiple infrastructures, including container platforms and virtual machines. In essence, it reduces the effort required for creating, managing and using Blockchains.

CEX (Centralized Exchange)

Centralized exchanges are third-party trading platforms that function like traditional brokerage or stock markets, acting on behalf of their users for trading crypto-currencies and assets. CEXs maintain customers' or end users' crypto funds, balances and possess custody of their private keys. Some centralized exchanges have shut down owing to death of their promoters or promoters fleeing resulting in loss of users' crypto assets. Kraken, Gemini and Robinhood are some well-known Centralized Exchanges.

Chain Code

Chaincode is a piece of code that is written in one of the supported languages such as Go or Java and runs on top of the Blockchain. It contains business logic pertaining to applications interaction with the ledger and runs in a secured Docker container isolated from peers that endorse transactions. For eg: It is installed and instantiated through a Software Development Kit (SDK) or Command Line Interface (CLI) onto a network of Hyperledger Fabric peer nodes, enabling interaction with that network's shared ledger.

Chain Link

Chainlink is a decentralized network of nodes that provide data and information from off-blockchain sources to on-blockchain smart contracts via oracles. The Chainlink aggregating contract collates all data from chosen oracles and validates and/or reconciles it, for accurate representation. Crop insurance on Blockchain is a proven use case of using Chain Link for decentralized oracle nodes that source weather data from multiple sources to self-execute claims through smart contracts.

Channels

In Hyperledger Fabric, there can be multiple ledgers and each ledger is referred to as a Channel. They help to promote Data Privacy by enabling private communications between various network members. They can be dynamically created and reconfigured. Parties transacting in a Channel should be authenticated to that particular Channel to ensure that external parties don't gain access to the communication. For eg: In a Supply Chain Blockchain, there will be a channel between the Customer and Supplier A and a separate Channel between Customer and Supplier B. This ensures that suppliers A and B transact privately and separately with the same Customer and don't have access to each other's channel.

Checksum

A checksum is generally designed to detect accidental errors in small blocks of data. It allows the user to check if piece of data or information is the same as expected. For eg: In Bitcoin, addresses include checksum so they can be checked to see if they have been typed correctly. This allows users to avoid sending Bitcoin to poorly formed addresses. They are created by hashing data through SHA 256 algorithm twice, the first 4 bytes of the result is taken as Checksum. 1 byte will be equal to two characters.

CIA Triad

CIA triad stands for Confidentiality, Information Security and Availability, the three fundamental tenets that stand as the goal of any system designed to perform in a secure manner. Blockchain implementation is deemed to enhance the resilience of the underlying systems and implementation based on CIA triad tenets. This triad has been formed over the years and doesn't belong to a single creator.

Cipher

Cipher is an encryption algorithm which is applied to a plain text to convert it into ciphertext which is the unreadable output of an encryption algorithm.. They are also used to decrypt cipher text into plain text. Keys are used to accomplish this conversion. There are 7 different types of ciphers – Caesar, Monoalphabetic, Homophonic Substitution, Polygram Substitution, Polyalphabetic Substitution, Playfair & Hill.

Cipher Text

Cipher text is the encrypted output of a plain text, which is the result of Cipher algorithmic operation. Cipher text can reveal the actual plain text that it represents when it is passed through the corresponding decryption algorithm.

Clique

Clique is a cross-client proof-of-authority (PoA) consensus protocol. It shadows the design of Ethereum mainnet, so it can be added to any client with minimal effort. In a PoA, the minted blocks are deemed to be signed by Trusted signers and thus, is a much simpler and energy efficient alternative to the Proof of Work consensus mechanism. Hyperledger Besu uses Clique consensus protocol.

Coinbase

A Coinbase transaction is the first transaction in a block, created and used by miners. It is used to collect the block reward for their work. Any other transaction fees collected by the miner is also sent in this transaction.

Coinbase Exchange

Founded in 2012, it is a fully regulated and licensed cryptocurrency exchange. It initially allowed only Bitcoin for trading and started adding other cryptos that confirmed to its decentralized criteria. It supports over 50 million users in 100 countries catering to USD 200+ Bn worth of assets.

Coin Desk

CoinDesk is a news site specializing in bitcoin and digital currencies launched in May 2013. The site was founded by Shakil Khan who is also an investor in Bitpay a Bitcoin payment processor and was subsequently acquired by Digital Currency Group.

Cold Wallet

The cold wallet is an offline wallet carried on a hardware device or printed on a paper that stores the user's address and private key and works in conjunction with compatible software in the computer. Since Cold Wallets are not connected to the internet, they are deemed much more secure than 'Hot wallets' that function on internet connected devices or portals. Ledger Nano, Trezor and KeepKey are the most popular Cold wallets.

Collusion

Collusion is an often-deceitful agreement or secret cooperation between two or more parties to work together and distort the market forces by limiting free and fair competition. Colluding as opposed to collaboration can cause unhealthy and fraudulent practices in the marketplace, thus disturbing the market equilibrium. In Cryptography, Collusion problem determines whether set of users through collusion can extract information that is designed to be hidden from them after a protocol is executed.

Compiler

In computing, a compiler is a computer program that translates source code from a high-level programming language, also known as source language, to a lower level language to create an executable program that is understood by the target computing machine. In Ethereum, Solidity acts as a Compiler. In Hyperledger, Fabric Compiler can publish code to a Fabric Store, making it available for download and use.

Confidential Computing

Confidential computing is an advanced cybersecurity paradigm that is used to encrypt and protect the data in use, while being processed, thus creating a highly secure computing environment. It enables encrypted data to be processed in memory and lowers the risk of exposure to rest of the system. It is achieved through a hardware enabled process that creates a trusted execution environment, isolating the protected data or applications from the operating system. Intel has rolled out a service called Software Guard Extensions (Intel SGX) that helps to keep sensitive data isolated from other privileged portions especially in multi-tenant cloud environments. Linux Foundation is promoting Confidential Computing Consortiums. R3 has launched a Confidential Computing platform called Conclave.

Conclave

A standalone platform launched by R3 leveraging Intel Software Guard Extensions (Intel SGX) to address business scenarios where data needs to be shared in a consortium of firms where one person or firm should not be able to see others information It helps in establishing trusted services that can detect fraud and reduce cost where owners of data can control how it is shared and processed.

Confirmation

Confirmation in Blockchain implies that a transaction has been processed by the network by clearing the consensus process that has been programmed in the system and thus is eligible to be added to the ledger being carried by the corresponding nodes, which are a party to the transaction. Once confirmed, the transactions are considered almost irreversible and tamper evident. Using Blockcypher or Blockchain.com explorers one can see numbers of confirmations that the transaction has obtained by pasting the transaction ID into the search field of respective explorers. In Bitcoin by design, a transaction will receive atleast 1 confirmation after an average of 10 minutes.

Consensus Mechanisms

The mechanism by which members come to an agreement about the authenticity of a transaction is referred to as the 'Consensus Mechanism.' Consensus formation ensures the involvement of multiple validators in a systematic and predetermined manner, ensuring decentralization and objectivity of decision making. It ensures implementation of the key features of the Blockchain platform like increased trust, immutability of the transactions, and maintenance of integrity of the platform. It is the soul of the Blockchain platform and will help help members in reaching right decisions at all times. Sanctity of Blockchain applications depends on the strength and reliability of consensus mechanism used by it. Bitcoin and the earlier version of the public Ethereum client follows 'Proof-of-Work (POW)' Consensus mechanisms where miners or validators compete with each other and burn valuable resources like computing power and enormous amounts of electricity to guess the right Nonce (number used only once) and create a targeted hash to win the race to create a block. Ethereum platform will soon shift to a 'Proof of Stake' (POS) based consensus, which involves negligible energy consumption. Some new-generation public platforms use variations of 'POW' and 'POS'-based consensus algorithms like PoET (Proof of Elapsed Time) and DPOS (Delegated Proof of Stake) to minimize resource utilization and wastage. Enterprise Blockchains like Hyperledger and others use energy-efficient algorithms like 'Proof of Authority' (POA), Practical Byzantine Fault-Tolerant' (PBFT), 'Node to Node'

(N2N) and their variations to arrive at a deterministic consensus. Consensus mechanisms aim is to ensure that all participants have identical copies of distributed database files.

ConsenSys

ConsenSys is Ethereum focused software company founded by Joseph Lubin in 2014. It offers next-generation applications and a modern financial infrastructure to access the decentralized web. Their product suite composed of Infura, Quorum, Truffle, Codefi, MetaMask, and Diligence, serves millions of users, supports billions of blockchain-based queries for the Ethereum ecosystem participants across the world and handles billions of dollars in digital assets.

Consortium

A consortium is an association of two or more individuals, companies, organizations or governments with the objective of participating in a common activity or pooling their resources for achieving a common goal. A Blockchain consortium is formed by a group of players in the ecosystem with a common goal of leveraging the technology for the common benefit of the ecosystem, by creating an elevated level of trust in the business environment, reduces costs, improves productivity and delights customers. For a thorough understanding of this topic, one may refer, the book, BLOCKCHAIN CONSORTIUMS – A Comprehensive Handbook: Analyzing the Business Model of the Future authored by Srinivas Mahankali (Co-author of this Book) & Varun Singhi, Murthy Chitlur (reviewers of this book)

Container

Container technology was born in 1979 with Unix Version 7 and the Chroot system. It picked up steam in early 2000s with Linux VServer and introduction of Docker that led to a massive adoption of this technology. Further momentum came through introduction of Kubernetes – a container orchestration technology in 2017. A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another. A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.

Container images become containers at runtime in the case of Docker containers when they are run on Docker Engines. Available for both Linux and Windows-based applications, containerized software will always run the same, regardless of underlying infrastructure. Containers isolate software from its environment and ensure that it works uniformly despite differences for instance between development and staging.

Contract

A contract is a legally binding agreement, enforceable by law, often documented in writing, between at least two parties that defines and governs the rights and duties of the parties to an agreement. In the Blockchain ecosystem, contracts are encoded in the form of applications triggered on an immutable & tamper evident ledger. These applications are termed as smart-contracts, chaincode, flows etc., and need to be supplemented by legally binding proofs like notarization by court-approved entities to ensure enforceability.

Corda

Corda is an open-source project, promoted by R3 an enterprise software firm, based on distributed ledger technology, designed for businesses to interact with each other in a trusted environment. Its intent is to deliver next generation Blockchain platform that addresses privacy, scalability and security to become DLT platform of choice for Financial Services and other verticals. Corda's smart contract technology allows interoperable business networks that transact value directly with each other in strict privacy. Instead of approving in batches & confirming transactions in blocks, Corda confirms & commits each transaction in real-time. More than 350 institutions have deployed Corda.

Cosmos

Cosmos is a decentralized network of independent parallel blockchains, each powered by Byzantine Fault Tolerance (BFT) consensus algorithms like Tendermint consensus, allowing the Blockchains in its ecosystem to scale and interoperate with each other.

Cosmos has two types of blockchains: Zones and Hubs. Zones are regular Blockchains, while Hubs are Blockchains that connect zones with one another. The Cosmos Hub, is a public, Proof-of-Stake (PoS) Blockchain whose native asset or cryptocurrency is Atom. More than 210 Atoms are in circulation.

CRISP-DM

Cross Industry Standard Process for Data Mining (CRISP-DM) refers to the standards used by Data mining experts while dealing with data across organisations, systems and platforms. Blockchain is an inter-enterprise platform and the data is recorded in Blockchain ledgers. As this data is deemed to be a high quality input for Data Analysis, it is important to strictly adhere to the CRISP-DM, an open standard process that incorporates many open standard processes.

Crypto-anarchy

Crypto-anarchism (or crypto-anarchy) is a political ideology that believes in attaining privacy, political freedom and economic freedom with the help of cryptographic software that achieves confidentiality and security while sending and receiving information over computer networks. In 1988, Timothy C May wrote 'Crypto Anarchist Manifesto which specified basic principles such as encrypted exchanges ensuring total anonymity, freedom of speech and freedom to trade. Bitcoin whose invention has been influenced by this Manifesto, and world's first commercial implementation of Blockchain Technology is considered as a symbol of Crypto-anarchy by eliminating the need of regulators and central authorities for conducting financial transactions. With El Salvador becoming the first country to adopt Bitcoin as legal tender, role of Bitcoin in legitimate and Government backed financial transactions will increase and may bring to fruition the goals and dreams of Crypto-anarchists.

Cryptography

Cryptography, or cryptology, is the practice and study of techniques for secure communication by obscuring adversaries and malicious hackers. It is the process of converting ordinary/plain text to an un-intelligible format by using algorithms, in such a way that only the intended parties can understand the same by applying corresponding decryption method. It is believed that Cryptography was used for correspondence by Spartans as early as 400 BC where they used a cipher device called Scytale for secret communication between various military commanders. Cryptography history can be classified into three phases. Phase 1 – Upto World War 1 where ciphers were limited to few pages or few manual devices. After World War 1, mechanization of ciphers and cryptography began using telephone and telegraph devices resulting in Phase 2. There was also switch from electro-mechanical devices to electronics during this phase with the advent of Data Encryption Standards (DES) and Advanced Encryption Standards (AES). Phase 3 has commenced in the last two decades of Century with appearance of digital signatures and hashing algorithms.

Cryptojacking

Cryptojacking is malicious crypto mining that happens when cybercriminals hack into both business and personal computers, laptops, and mobile devices to install malware. This software uses the computer's power and resources to mine for cryptocurrencies or steal cryptocurrency wallets owned by unsuspecting victims. Cryptojacking malware affects almost 55% of businesses the world over using as much as 65% of CPU power. Coinhive and MassMiner are some of the dangerous Cryptojacking malwares.

Cypherpunks

Cypherpunks are those who supported the Cryptoanarchy concept proposed by Timothy May. The group was founded by Timothy May, John Gilmore and Eric Hughes. Cypherpunks mailing list was started in 1992 covering subjects like computer science, cryptography, political discussions etc. Cypherpunks advocated widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.

CHAPTER 4

D

Daemon

Daemon is a process operating in the background waiting for a specific event or condition in order to be activated. In Blockchain world, Daemons distribute Blocks & Transactions, create new blocks, validate blocks and transactions and also resolve forks as and when they occur.

DAG (Directed Acyclic Graph)

It is a directed graph data structure that uses a topological ordering. The sequence can only go from first to last. DAG is often applied to problems related to data processing, scheduling, finding the best route in navigation, and data compression. DAG technology is often placed together with Blockchain however it is considered to be another form of Distributed Ledger Technology (DLT). It consists of network of individual transactions linked to multiple other transactions. There are no blocks and chain of previously validated Blocks in DAG.

Dai (or DAI)

DAI is a stable coin cryptocurrency which aims to keep its value as close to one United States dollar (USD) as possible through an automated system of smart contracts on Ethereum blockchain. On December 18, 2017, Dai and its associated smart contracts were officially launched on the main Ethereum network. It is maintained and regulated by MakerDAO, a Decentralized Autonomous Organization consisting of owners of MKR which is its governance token. Users will be able to borrow against the deposits of their Ether and receive newly generated DAI in ratio of 1.5:1 i.e. 1 DAI for every 1.5 Ether deposited. As a result, DAI is considered as a good adoption of Decentralized Finance (DeFi). Once the loan and its interest is repaid, the returned DAI is automatically destroyed and collateral is allowed for withdrawal.

DAML (Digital Assets Modelling Language)

DAML is developed by Digital Asset, a company co-founded and led by Yuval Rooz. It is used to build digital assets such as smart contracts for blockchains. This technology complements Digital Asset's existing technology by providing a new, verifiable way for parties involved in a transaction to provide updates to a distributed ledger while preserving data confidentiality. It is a new Haskell-inspired functional programming language that has been under development for a few years, and with latest developments in the fast-changing blockchain environment, DAML has become the most popular programming language for building smart contracts. It offers DAML Connect (complete development and application stack), DAML Drivers (allows application deployment using Distributed Ledgers, Blockchains or Databases) and DAML Hub (a Cloud service that enables rapid distributed application development)

DAO (Decentralized Autonomous Organization)

DAO was an organization that was designed to be automated and decentralized. It acts as a form of venture capital fund, based on open-source code and without a typical management structure or board of directors. To be fully decentralized, the DAO was unaffiliated with any particular nation-state, though it made use of Ethereum network. It had crowd sourced $150 million in cryptocurrency, started in April 2016 and became defunct in September 2016. A vulnerability in The DAO code was exploited by users to siphon off of The DAO's funds to a subsidiary. As a result, Ethereum community hard forked the Ethereum Blockchain to restore all funds to the original contract. The original unforked Blockchain is known as Ethereum Classic and the forked one is known as Ethereum.

DAPPS (Decentralized applications)

Decentralized applications (dApps) are digital applications or programs that exist and run on Blockchain or P2P network of computers instead of a single computer, and are outside the purview and control of a single authority. Chainlink, Brave, EOS Dynasty, Maker DAO and Chainyard are some of the well-known dApps.

DDoS Attacks (Distributed Denial of Service attacks)

Distributed Network Attacks are often referred to as Distributed Denial of Service (DDoS) attacks. This type of attack takes advantage of the specific capacity limits that apply to any network resources – such as the infrastructure that enables a company's website. The DDoS attack will send multiple requests to the attacked web resource – with the aim of exceeding the website's capacity to handle multiple requests and prevent the website from functioning correctly. To preempt DDoS attacks crippling network infrastructure particulary those that are architected on centralized infrastructure principles, decentralized infrastructures based on Distributed Ledger Technology are being considered to prevent single point of failure.

DES (Digital Encryption Standard)

The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data. Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS selected a slightly modified version which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977. The original DES' key size of 56 bits was sufficient when it was developed. To prevent successful brute forces attacks on DES owing to increasing computational power, Triple DES (TDES) came into existence which applies DES algorithm three times to each data block. In May 2002, Advanced Encryption Standard (AES) replaced DES.

De-Fi (Decentralized finance)

Decentralized finance (commonly referred to as DeFi) is a blockchain-based form of finance that does not rely on central financial intermediaries such as brokerages, exchanges, or banks to offer traditional financial instruments, and instead utilizes smart contracts on blockchains, the most common being Ethereum. Maker, Uniswap and Compound are some of the leading DeFi services providers.

Decentralisation

In blockchain, decentralization refers to the transfer of control and decision-making from a centralized entity (individual, organization, or group thereof) to a distributed network. It facilitates Digitization of Trust where trust is contained in a distributed network rather than in a centralized party or entity. It provides trustless environment, promotes data reconciliation, minimizes points of failures and maximizes resource distribution.

Delegated Proof of Stake (DPoS)

Its similar to Proof of Stake since the validators of blocks in Blockchain are required to invest or stake cryptocurrencies on transactions to be validated. These validators are selected via voting by various token holders where votes are proportional to their stakes.

Degen

Refers to cryptocurrency projects that are involved in pumping and dumping schemes. Usually, worthless and junk tokens are hyped up in various communications channels and forums and they are abandoned later through Degens. Tendies, YFI and Yam have been considered as Degen projects.

DevOps

DevOps, a term coined in 2009 by Patrick Debois, is a complementary set of practices to Agile software development where development and operations teams remained separated and siloed. It aims to shorten the systems development life cycle and provide continuous delivery with high software quality by bringing these two teams together right from starting of the project. This replaced the Waterfall Software development model.

DEX (Decentralized exchange)

Crypto funds and balances are maintained by the users. DEX doesn't have any custody. It promotes transactions between two parties using software tools, open blockchains, and internet. DEX is autonomous and run by algorithms and smart contracts. There are more than 35 DEXs like Dydx, Uniswap, Bancor, Changelly and BisQ.

Diamond Hands

It represents cryptocurrency traders or investors who keep holding onto their respective cryptocurrencies even when their price or value drops. They believe that such price drop is only temporary and will be corrected eventually.

DIDs (Digital Identifiers Documents)

DIDs are a type of identifiers that enable a verifiable, decentralized digital identity. They are based on the Self-Sovereign Identity paradigm. A DID identifies any subject e.g., a person, organization, thing, data model, abstract entity, etc. They obviate the need for a central administrative system to manage and control the identifiers and use cryptographic basis to provide Decentralized identification. DIDs are being promoted by World Wide Web Consortium (W3C) to develop next generation Web.

DIEM

Diem is a permissioned blockchain-based payment system proposed by Facebook, Inc. The plan includes a private stablecoin implemented as a cryptocurrency, with 1 Diem pegged at 1 USD and was formerly known as Libra. This yet to come to existence.

Difficulty

Difficulty is a number that regulates how long it takes for miners to add new blocks to the blockchain. In Bitcoin, it determines the difficulty level to mine a Block which is basically finding a hash below a particular target. High difficulty will result in more compute power to mine the blocks. Difficulty is adjusted after every 2016 blocks are mined, based on the time taken to find preceding 2016 blocks. In Bitcoin, a new block is created every 10 minutes, hence 2016 blocks will take exactly two weeks to be mined. Difficulty will be reduced if the previous 2016 blocks took more than two weeks to be found or mined and vice versa.

Digi Cash

Founded by electronic currency pioneer David Chaum in 1989, DigiCash was one of the earliest electronic money companies. Digicash used cryptographic protocols to make the transactions anonymous. This was accomplished through Blind Signature Technology developed leveraging advancements in Public and Private Key technologies. As a result Bank or Government would be unable to trace personal payments conducted online. No wonder, David Chaum was one of the prominent and leading Cypherpunks.

Digital Assets

The definition of a digital asset is “anything that exists in binary data which is self-contained, uniquely identifiable, and has a value or ability to use.” When the term originated in the mid-90s, digital assets were items such as videos, images, audio, and documentation. In today’s world, it is widely used to refer to cryptocurrencies that are decentralized and run on a network that is distributed across a large number of computers.

Digital Signature

It validates the authenticity and integrity of a message, software or digital document using mathematical techniques. It solves the problem of tampering or impersonation in digital communications by using Asymmetric cryptography such as RSA based on public key cryptography. Digital Signatures use security features and methods such as Checksum, Certificate Authority (CA) validation, Trust Service Provider (TSP) Validation.

Disintermediation

Disintermediation is the process of removing the middleman or intermediary from future transactions. DeFi (Decentralized Finance) is a good example of disintermediation as it doesn't rely on central financial intermediaries such as brokerages, exchanges or banks and utilizes smart contracts to create required trust between two unknown parties.

Distributed Ledger

A distributed ledger is a shared database containing digital data that is synchronized at regular intervals even though it is geographically spread across multiple sites, countries, or institutions. It doesn't have a central administrator and allows for public witnesses or consent. They can be either Permissioned or Permissionless ledgers.

DLT (Distributed Ledger Technology)

It's the technology that powers Blockchains. Though it was first outlined in 1991 by Staurt Haber and W Scott Stornetta, it was first conceptualized by a person or group of people known as Satoshi Nakamoto in 2008. It allows for storage of all information in a secure and accurate manner using cryptography in a decentralized database. Once the information is stored it becomes immutable database. It is anticipated that 10% of world's GDP will be processed through DLT by the year 2027.

Docker

Invented by Solomon Hykes in 2013. Its a tool designed to create, deploy and run applications using containers. Containers package applications with all parts it needs such as libraries and deploy it as one package. It brings security to applications running in shared environment.

Dogecoin

It is a peer to peer cryptocurrency predominantly used as a tipping system, in which social media users tip others for providing interesting or noteworthy content. It was created by referencing the face of the Shiba Inu dog from "Doge" meme as its logo and namesake on December 6, 2013, by software engineers Billy Markus and Jackson Palmer. It started as a satire on the growth of various altcoins. It has 1-minute block interval which means its faster than other Blockchains

Double Counting

Double counting in accounting is an error whereby a transaction is counted more than once, for whatever reason.

Double Spending

Double-spending is a unique problem associated with digital currencies, that allows for an online value unit to be spent more than once. This is because the digital information surrounding the value unit can be reproduced relatively easily by tech savvy individuals in absence of a central authority that keeps tab of each and every transaction between parties. Bitcoin, the first commercial application of Blockchain technology, solved this problem by preventing Double-spending on digital value units that are created online, through a unique cryptographically executed process and recording transactions in a distributed ledger needing consensus from all parties before they are finalized and approved. Hence it is called a Cryptocurrency. Bitcoin employs a universal ledger, termed blockchain and provides a way for all nodes to be aware of every transaction confirmed through a game theory inspired process and broadcasted to all the nodes in the form of blocks.

Digital Twin

A digital twin is a virtual representation that serves as the real-time digital counterpart of a physical object or process. The concept of digital twin is widely used to monitor physical assets such as turbines, engines, and telecommunication towers within the boundaries of the enterprise.

A blockchain based Digital Twin is applicable when the asset in consideration is shared or transacts with multiple stakeholders in its lifecycle using a distributed and immutable ledger serving as Single Source of Truth. IOT based products and industrial assets are good contenders for the application of Digital Twin concept using Blockchain.

CHAPTER 5

E

EEA (Ethereum Enterprise Alliance)

The Ethereum Enterprise Alliance (EEA) is a member-led industry organization whose objective is to drive the use of Ethereum blockchain technology as an open-standard to empower enterprises. It was launched in February 2017. The EEA's mission is to deliver an open, standards-based architecture and specification to accelerate the adoption of Enterprise Ethereum. Its members include several organizations across the globe. Founding members and rotating board include Accenture, Banco Santander, BlockApps, BNY Mellon, CME Group, ConsenSys, IC3, Intel, JP Morgan, Microsoft and Nuco.

EIP (Ethereum Improvement Proposals)

EIP is an acronym for Ethereum Improvement Proposal, just as BIP is an acronym for Bitcoin Investment Proposal. The EIPs set out the technical standards (protocol specifications, contract standards, client APIs etc.) for Ethereum blockchain. Martin Becze, Vitalik Buterin andGavin Wood were the original EIP editors from 2015 to end of 2016.

ECC (Elliptic Curve Cryptography)

It is Public Key cryptography based on elliptic curves over finite fields and their algebraic structure. They are able to provide same cryptographic strength as RSA encryption but with much smaller key sizes.

ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA is a digital signature algorithm that makes use of ECC to create the key pairs used in the signing and verification process of digital signatures. Because of its advantages compared to other public-key algorithms, it is commonly used in blockchain applications to sign transactions or events.

Encryption

Encryption is the process of securing information through cryptography. Plain text is converted into an alternative form known as Ciphertext. Only parties possessing the keys will be able to convert ciphertext back into plain text for decrypting and reading the information. AES, Triple DES, RSA (Rivest-Shamir-Adleman), Blowfish and ECC are some of the leading encryption technologies.

Enterprise Blockchain

It's a Blockchain network usually implemented by corporates or companies to manage their business processes like corporate finance, treasury, trade finance, insurance, supply chain, contracts management, international money remittances and global payments. Enterprise Blockchains are permissioned blockchains in nature where partners, peers or suppliers who intend to join the Blockchain, need prior approval from the company that has hosted or commissioned the Blockchain. The company hosting the Blockchain doesn't control the Blockchain as all parties once they are admitted have equal rights and control of the network. R3, Ethereum Enterprise Alliance, Hyperledger Foundation are some famous organizations who are working on development of Enterprise Blockchain.

EOA (Externally Owned Accounts)

Externally Owned Accounts are controlled by private keys. A person possessing the private key of the account will be able to send cryptos (Ether in case of Ethereum) and messages from the account. It doesn't have any associated code unlike the Contract Accounts (CA) that are controlled by code. Transaction Validation involves checking the timestamp and nonce combination to establish validity, and the availability of sufficient fees for execution.

EOS Blockchain

Entrepreneurial Operating System, (EOS) is a blockchain-based decentralized operating system that is designed to create, host and support secure, decentralized autonomous applications (dApps) and smart contracts. It was designed to meet large scale decentralized applications and developed by Daniel Larimer and Brendan Blumer. It was released as open source software by the company Block.one which distributed one billion tokens based on its native currency EOS.

EPOCH

An epoch is the target time period for which a given group of Miners is elected to serve as the consensus group. It also defines period of time taken for pre-specified number of blocks to be confirmed on the chain. In Ethereum Blockchain for every 30,000 blocks, a new piece of data (a DAG) is used for mining new blocks. Each new group of 30,000 blocks is known as an epoch.

ERC 20 (Ethereum Request for Comments - 20)

ERC 20 is defined as the standard protocol for issuing tokens on the Ethereum network. According to the official sources, the protocol governs the tokens on the Ethereum blockchain. The suffix "20" is used for the sole purpose of representing the unique proposal ID. Developers use the ERC20 token to develop their project. It is a way to tokenize their project and at the same time offers them a way to raise funds for their respective projects. ERC 20 defines six different functions for benefit of other tokens within the Ethereum system and has led to the birth of several alternate tokens (Alt Tokens) or Alternate Coins.

ERC 721 (Ethereum Request for Comments 721)

ERC 721 tokens, more commonly referred to as Non-Fungible tokens (NFTs) allow developers to tokenize ownership of any arbitrary data, digital assets or digital collectibles there by increasing the design space of what can be represented as a token on the Ethereum blockchain. They were proposed by William Entriken, Dieter Shirley, Jacob Evans and Nastassia Sachs in January 2018.

Escrow

Escrow is a legal arrangement in which a third party temporarily holds large sums of money or property until a particular condition has been met. Escrow services are now playing a major role in the field of Blockchain. Escrow can always pay obligations or debts, with the help of signature funds, allocated to pay those debts. Escrow's main responsibility is to help dispense money or documents as a neutral third party in different exchanges. BTC Asia, IBC Group, Bitrated andGlobal Escrow are well known Bitcoin Escrow service providers.

Eth (Ether)

Ether is next most popular cryptocurrency after Bitcoin. It is the currency that powers Ethereum applications and is decentralized. In addition to being a tradeable cryptocurrency, it powers the Ethereum network by paying for transaction fees (referred to as Gas) and Computational services. As it is programmable, developers are using it in many ways. It can be used to send and receive funds in real time, swap tokens , earn interest and get stablecoins. Infact, Ether is paving the way for a more intelligent financial platform based on Decentralised Finance (DeFi) concept.

Etherbase

Etherbase, also called coinbase, is the public key of an Ether account, which is needed by the miner to receive a mining reward known as Ether money.

Etherhash

Etherhash is a wallet creating platform allowing users to create wallet by typing password only. Users can create anonymous wallets by creating security password. Users need to store passwords in a secure place, as any one else who has access to password can take the funds away from the wallet. Platform uses EtherHasa to create hashes of passwords and stores them using smart contract. Users can deposit ETH only on the deposit hash that begins with '0x'. After withdrawal, password and deposit hash will be deleted, and they cannot be reused for security reasons. New accounts need to be created for new deposits and withdrawals.

Ethereum

It is an open source Blockchain that introduced smart contracts functionality. Its native currency is called as Ether. Vitalik Buterin, Co-founder of Bitcoin Magazine, proposed Ethereum in 2013. Joseph Lubin, Gavin Wood & Jeffrey Wilcke joined as Co-Founders of Ethereum in 2014. It went through many protocol upgrades since its launch with various code name projects like Frontier, Ice Age, Homestead, Spurious Dragon, Istanbul and others. Ethereum fueled many innovations in world of Blockchain that include Alt Coins, Initial Coin Offerings (ICOs), Smart Contracts, Ethereum Virtual Machine (EVM), Decentralize Finance (DeFi) and Non Fungible Tokens. Ether is the second most valued cryptocurrency after Bitcoin.

Ethereum_J

Ethereum(J) is a pure-Java implementation of the Ethereum protocol. It is provided as a library that can be embedded in any Java/Scala projects and to offers full support for Ethereum protocol and sub-services. Ethereum(J) was first developed by Roman Mandeleil.

EVM (Ethereum Virtual Machine)

Ethereum functions like a distributed state machine instead of being a distributed ledger. Ethereum has this machine state in addition to all accounts and balances. The data structure can change from block to block to a predefined set of rules which can execute machine code too. Every node in Ethereum network runs an EVM instance. EVM defines rules that govern changing the state from Block to Block. It allows developers to create Decentralized applications (DApps) using a specialized language called Solidity.

Exchange

A digital marketplace where buyers and sellers can exchange cryptocurrency for fiat or other cryptocurrencies. It usually is an online platform and acts as intermediary. There are over 10,000+ cryptos that trade currently in over 375 exchanges with a total market capitalization of USD 2 Trillion.

EXMO

EXMO is a British cryptocurrency exchange. EXMO has estimated 1.8 million users, 8 fiat currencies (USD, EUR, GBP, RUB, PLN, UAH, KZT, TRY), SEPA, SWIFT, Credit/Debit cards on the platform. EXMO exchange is registered in London, with offices in London, Moscow, and Kyiv, and employs a project team of 150+ people.

Explorer

Explorer is a Blockchain module explicitly designed for developing user-driven web applications. It can be used for viewing, deploying, invoking/querying blocks, network information, transaction data, chaincodes and other relevant data that is stored in a Blockchain ledger. Blockchain.com, Blockcypher, Tokenview and Tradeblock are good Blockchain explorers.

CHAPTER 6

F

Fast sync

Fast sync helps synchronization at a node level by avoiding download of entire blockchain and processing one link at a time. It helps in faster syncing with the chain by just downloading blocks and checking the merkle tree of validators. Many Blockchain protocols offer Fast Sync nodes.

Faucet

A faucet in cryptocurrency world is a website that either gives out small amounts of native cryptocurrency in exchange for users completing certain small tasks, or pays out a set quantity of a native cryptocurrency's coins on a testnet (a test network) which can be used for testing smart contracts and dApps, before deploying them on the main net (the main network). Cointiply, Bonus Bitcoin and Bchain Poker are well known Bitcoin faucets.

Fault Tolerance & types

Fault tolerance refers to the ability of a system (computer, network, cloud cluster, etc.) to continue operating without interruption when one or more of its components fail, thus affecting Reliability, Availability & Security.

Crash faults happen due to failure of the hardware, software and network due to system and electricity failure etc., while Byzantine faults happen due to unauthorized access and malicious nodes.

Byzantine Fault Tolerance in a cryptocurrency is the feature of reaching an agreement or consensus about particular blocks even when some nodes fail to respond or give out malicious values to misguide the network.

Crash fault tolerance (CFT) is one level of resiliency, where the system can still correctly reach consensus if components fail. Byzantine fault tolerance (BFT) is more complex and deals with systems that may have malicious actors.

Practical Byzantine Fault Tolerance is a consensus algorithm introduced in the late 90s by Barbara Liskov and Miguel Castro. pBFT was designed to work efficiently in asynchronous (no upper bound on when the response to the request will be received) systems. It is optimized for low overhead time.

Asynchronous byzantine fault tolerance (ABFT) is a property of Byzantine fault tolerant consensus algorithms, which allows honest nodes in a network to agree on the timing and order of a set of transactions, fairly and securely.

Federated Identity

A federated identity is a single identity used by a party on a blockchain network to access multiple services across the distributed network. It involves using a single key – digital or biometric to sign into systems across multiple departments within an organization or multiple organizations. With the use of a federated identity, the service providers can track usage of their services, while the owner of the identity can trace its use across the network. It helps in providing transparency, control of identities and prevents misuse or unauthorized access

Fiat Currency

When the government or the central bank of a nation issues a nation-wide currency, that is called a fiat currency. Fiat currency may not be backed by gold, silver, oil etc., its value is rather based on the faith that citizens have on the central authority issuing such currency. United States Dollar, Indian National Rupees, Canadian Dollar and Japanese Yen are examples of fiat currencies.

Filecoin

Filecoin is a community-based data storage and retrieval solution, enabling users to rent their unused storage space on their devices, based on Inter-Planetary File System. It was started by Protocol Labs and its CEO Juan Benet. The payment by and to the users is via FIL, the native currency of the Filecoin blockchain. It uses the proof of replication (PoRep) and proof of spacetime (PoST) mechanisms. It is mainly written in Go Language and integrates Rust, Javascript and Python too. Filecoin raised US $200 Million within the first 30 minutes of its launch.

Flow

Flow is a Blockchain that is relevant for NFT collectibles and crypto games. Dapper Labs that developed NBA (National Blockchain Association) Topshots – a leading NFT in sports, developed Flow. It came into existence when NFTs like Cryptokitties were choking Ethereum circa 2017.

FOMO

Fear-Of-Missing-Out is a phenomenon defined by a network effect that comes into play when many people from the community start showing interest towards a new product, entity, or process, and that's when other 'prospective users' in the network start feeling the need to get onto the bandwagon, before it's too late. Many products throughout history have gained tremendous traction in terms of pricing or demand owing to FOMO which is purely based on emotions rather than underlying valuations. Sudden increase in cryptocurrency prices, or sudden interest in a particular cryptocurrency and surge in its price is usually on account of FOMO. Crypto FOMOs have resulted in as high as 350% premium on Bitcoins.

Fork

A fork in a blockchain network happens when any changes to the underlying protocol take place or fundamental aspects pertaining to cryptocurrency need to change. There are two kinds of forks – Soft fork and Hard fork. Soft fork occurs when the change is backward compatible, and users only need to upgrade their software. Hard fork takes place when the change is not backward compatible, and the users have to move to the new chain or else take the risk of not being able to mine any blocks further. Hard forks usually arise on account of disagreements in the community with respect to proposed changes and their implementation. Bitcoin Cash, Bitcoin Gold and Ethereum Classic are examples of cryptocurrencies that have appeared owing to Hard Forks.

Frontier

Frontier is a blockchain platform introduced with the goal of aggregating DeFi services from multiple platforms into a single chain-agnostic DeFi layer. Its chain agnostic, supports DeFi on Ethereum, Binance Chain, Band Chain, Kava and Harmony and hasa native currency called as FUSD. Usecases include liquid provisions, staking, asset swapping, protocol tracking and management of assets.

FUD

FUD stands for Fear, Uncertainty, and Doubt; it occurs when a particular cryptocurrency or the market faces a downward trend because of a propaganda tactic that involves spread of negativity and false information by certain individuals or entities. FUD categories in cryptocurrency world includes:

No intrinsic value,

Criminal usage,

Highly Volatile,

Market Manipulation,

Loss of Custody,

Product deficits,

Government Bans

Fungible

Fungibility means that a particular variety of tokens or assets are interchangeable between themselves. Bitcoin, Ethereum, Litecoin, Ripple are fungible tokens – they can be exchanged with each other or with fiat currencies. CryptoPunk, Metarift, Art Blocks and Hashmasks are Non-Fungible Tokens.

CHAPTER 7

G

Game Theory

Originally developed by Mathematician John von Neumann and Economist Oskar Morgenstern, the Game Theory includes study of mathematical models that govern strategic interaction between various decision makers and helps in determining most likely outcomes in a situation that involves known payouts or quantifiable consequences. Basically, its a study of why and how people make decisions. It has been applied in Bitcoin network, by promoting good behavior through incentivizing miners to use their computing power to secure the network and intentionally making mining difficult and expensive for malicious actors. It helps in decision making by promoting consensus through Proof of Work. In Ethereum's proposed Proof of Stake, game theory has been used to not only reward good behavior but also punish bad actors. Combining punishments and rewards strengthens protocol security.

Gas

Gas refers to the fee or pricing value, required to successfully conduct a transaction or execute a contract on the Ethereum blockchain platform. In essence, it measures computational effort required to run operations on Ethereum network. Gas fees are paid in Ethereum's native currency Ether and are denominated in Gwei. Each Gwei is One-billionth of Ether.

Gas Limit

The term Gas Limit refers to the maximum price a cryptocurrency user is willing to pay while sending a transaction, or performing a smart contract function on Ethereum blockchain. Average Ethereum block has a gas limit of 1.5 million Gas.

Gas Price

A general reference to the approximate transaction fees to be paid on Ethereum Blockchain. It is measured in Gwei and is determined by an auction-type mechanism, where miners look for highest fees attached to a transaction, process them first and then process transactions from there-on in descending order.

Gas Price Oracle

It is a tool that helps users to make a prediction on Gas price that needs to be made in order to make a transaction confirmed within a certain time or number of Blocks in Ethereum. It makes predictions by looking at previous blocks utilization and gas limits. It helps users to interpret that paying lower gas prices may result in transactions not being selected by miners for validation within required time and helps them to modify gas prices accordingly.

Genesis Block

Genesis Block is the name of the first block of blockchain ever mined. The Genesis Block forms the foundation of entire blockchain transaction system and is the prototype for all other blocks in the blockchain. The Genesis Block for Bitcoin was created in January, 2009 that had a reward of 50 Bitcoins. Ethereum's genesis block was mined into existence in July, 2015

Geth

Geth (Go Ethereum) is a command line interface for running Ethereum nodes implemented in Go Language. Using Geth, one can join Ethereum network, transfer ether between accounts, mine ethers and interact with smart contracts. It creates software that runs on the Ethereum Virtual Machine.

Ghost (Greedy Heaviest Observed Subtree)

GHOST originally was a protocol modification, a chain selection rule, that makes use of blocks that are off the main chain to obtain a more secure and scalable system. It adopts orphan blocks – the valid blocks that did not make it to the main chain, as uncle blocks so that work from these blocks is included on the main chain. This prevents the attacker to overtake the mainchain. It is more relevant and applicable in Blockchains where time taken to create new blocks is quite less. Eg: In Ethereum, block time is 10 to 20 seconds while in Bitcoin it is 10 minutes. Hence, in Ethereum the chances of orphan blocks or stale blocks are very high. Instead of ignoring these blocks, Ghost protocol considers them while determining the longest chain to ensure network security and prevent centralization.

Github

GitHub is a code hosting platform for version control and collaboration. It lets users work together on projects from anywhere and is home to 60 million repositories accessed by over 56 million developers. Github helps in Easy Project Management, Effective Team Management, Improved Code Writing, Easy Code Hosting and Enhanced Code Safety. It began with Git, an open source project started by Linux creator Linus Torvalds. It is the one of the most prominent DevOps tools used for source code management and tracking changes in source code by enabling multiple developers to work simultaneously and contribute to non-linear development.

Go Lang

Go, or Golang, is an open-source programming language. Its statically typed and produces compiled machine code binaries. Designed at Google in 2007, by Robert Griesemer, Rob Pike, and Ken Thompson; syntax wise it is similar to C language. The main goal of creating Go was to combine the best features of other programming languages to accomplish Ease of use together with State-of-the-art productivity especially for scalable servers and software systems.

Goerli

Görli Testnet is the first Proof-of-Authority cross-client testnet, syncing Parity Ethereum, Geth, Nethermind, Hyperledger Besu (formerly Pantheon), and EthereumJS. This testnet is a community-based project, that is completely open-source.

Gossip

In technical terms, for a blockchain, Gossip is the information relayed by each participant repeatedly to another member chosen at random and tells them all they know about the transaction. For example, Peer A interacts with B, learns about the existence of Peer C and Peer D and connects with them. It mimics the way epidemics spread. Different protocols exist for Gossip like Dissemination and Compute aggregate protocols. Hedera Blockchain that uses Hashgraph consensus is based on Gossip protocol.

Governance

It refers to the structure that every user or participant in Blockchain agrees to follow. It lays down mechanisms for Blockchain to adapt and stay relevant with changing times and requirements. Core developers, Node holders and Token holders are responsible for governance, including Off-chain governance and On-chain governance.

Governance may also be spoken in the context of consortium formation in a federated blockchain deployment. Such a governance is the framework adhered to by the lead participant of a permissioned blockchain network. The governance framework helps in providing business rules, guidance and contractual conditions amongst consensus forming organizations.

Gwei

A Gwei or gGigawei is defined as 1,000,000,000 wei, the smallest base unit of Ether. One gwei equals 0.000000001 ETH or 1 billion gwei equals 1 Ether.

Grid

Grid is Hyperledger's solution designed to solve supply chain challenges. Interestingly enough, Grid is not a Blockchain framework or an application. In essence, it is an ecosystem of frameworks, libraries, and technologies that allow developers to choose appropriate components for building specific business models. It packages various Hyperledger stack components into a single effective business solution. Cargill, Target, Intel and Bitwise IO are main users of Grid.

Greedy

Greedy contracts are contracts that remain alive and lock Ether indefinitely. It does not release Ether in any condition. This happens in case of Multisig wallet using a parity contract to release Ether to owners. In case parity contracts get killed, wallet contracts will not be able to access libraries and will be stuck in a situation of greed.

CHAPTER 8

H

Hal Finney

Harold Thomas Finney was a developer and first employee of PGP Corporation, a cypherpunk and early contributor to Bitcoin development. He developed Reusable Proof of Work System (RPoW) modelled on Adam Back's Hashcash protocol. He is credited with operating first Bitcoin software after its release and is also the beneficiary of the first Bitcoin transaction wherein he received 10 BTC from bitcoin's creator Satoshi Nakamoto, registered in Block 170. He continued to code even after being paralyzed by Amyotrophic Lateral Sclerosis in 2009 and wrote software for Bitcoin with a computer that tracked his eye movement.

Halving

Halving is an event when the reward for mining a new block of cryptocurrency is reduced to half. Halving ensures that supply of cryptocurrencies is restricted which creates scarcity and more valuation. In Bitcoin halving happens every 4 years or after every 210,000 blocks are mined. Block reward that started with 50 BTCs in 2008 for Bitcoin will halve every 4 years or after every 210,000 blocks are mined. Halving will continue till Bitcoin is halved to its smallest value – 0.00000001or Bitcoin mining reaches it supply limit or cap of 21 million which is expected to occur in the year 2140.

Hard Fork

A hard fork in blockchain technology, is a radical change to a network's protocol that makes previously invalid blocks and transactions valid, or vice-versa. A hard fork requires all nodes or users to upgrade to the latest version of the protocol's software. Forks may be initiated by developers or members of a crypto community who are dissatisfied with functionalities in existing blockchain implementations. Hard forks are also used as a channel to crowdsource funding for new technology projects or cryptocurrency offerings. Bitcoin Gold, Bitcoin Cash and Ethereum Classic have come into existence on account of Hard forking of their genesis Blockchain networks.

Hard Wallet

Also known as hardware wallet, it is a cryptocurrency wallet which stores the user's private keys in a secure hardware device like drives or USBs. They facilitate cold storage as they are not connected to internet and are not online. They will be connected to internet or other devices only when funds are required to be transferred. Ledger, Ledger Nano S, Trezor and KeepKey are some of the hardware wallets available for use in the market.

Hash

It is created by Hashing algorithm which takes large sets of data and large range of values and converts them into a smaller set of values like 128 bit, 256 bit outputs. Hashing algorithms are usually one way function – can be used to convert an input into a Hash but cannot be reverse engineered to decipher the input based on the hashed algorithm output or hash. It acts as the backbone of blockchain network and provides immutability to transactions recorded on Blockchain. A hash is developed based on the information present in the block header.

Hash Function

A hash function is any function that can be used to convert data of arbitrary sizes to fixed-size values. Values returned by a hash function are called hash values, hash codes, digests, or simply hashes. The values are usually used to index a fixed-size table called a hash table. MD5, SHA-1, SHA-2 are examples of different hash functions. Bitcoin uses hash function called double SHA-256. Hyperledger Fabric uses SHA-2 as the default hash function.

Hash Tables

It is used to store keys or value pairs. It uses a hash function to convert the key into a hash value or hash which is then used as an index for a respective key value pair in the table, that contains several other indexes. They consist of Hash function and Array that holds key value entries in the table. They help in storing increasing list of records without the possibility of being tampered or revised. They also help in reducing the size of data structures and increase the data processing speeds.

Hashcash

Hashcash is a proof-of-work system, based on SHA-1 algorithm and invented by Adam Back in 1997. Its bedrock is based on the concept that some mathematical results are easy to verify but difficult to discover values that went into calculating the results. It is used to identify duplicate emails, limit email spam and reduce denial of service attacks. Hashcash based on Proof of Work, became foundation of Bitcoin to solve double counting problem that existed in decentralized cryptocurrencies.

Hashing

Hashing means taking an input string of any length, data or information and giving out an output of a fixed length. In the context of cryptocurrencies like bitcoin, the transactions are taken as input and run through a hashing algorithm (bitcoin uses SHA-256) which gives an output of a fixed length. Its usually a one-way function where output cannot be used to predict the input. However same output can be generated by using the source data that went in to create the output. Hence, hashing can be used easily to verify authenticity of data by computing its hash value multiple times over but cannot be used to infer the data, that was used to create it.

Hashrate

The hash rate is a measurement of number of times the cryptocurrency network is able to attempt to complete the calculations in every second. Its the approximate average of all hash rates of every individual mining machine that is involved in the network. Its an important metric used to assess the strength of a Blockchain network and its security. Higher the hash rate, harder it becomes for malicious users or attackers to manipulate Blockchain network. Hash rates are measured in kilo (1000 hashes per second), mega (1 million hashes per second), giga (1 billion hashes per second) or tera (1 trillion hashes per second). Ethereum has a hash rate of 400 TH/s (Tera Hashes per second) and Bitcoin's hash rate is 102 TH/s.

Haskell

First appeared in 1990 and stable release in 2010, Haskell is a blockchain programming language. Designed for safety, Haskell provides for mandatory automated checks, ensuring the elimination of certain kind of mistakes in the code. Prominent features of Haskell include memory safety, ease of understanding code, and absence of unwanted side-effects. Cardano Blockchain and DAML are based on Haskell.

Hexadecimal

The hexadecimal numeral system, often shortened to “hex”, is a numeral system made up of 16 symbols (base 16). The standard numeral system is called decimal (base 10) and uses ten symbols: 0,1,2,3,4,5,6,7,8,9. Hexadecimal uses the decimal numbers and six extra symbols A, B, C, D, E and F. It is very compact and makes conversion with binary easy. In Blockchain world, 256 bit hash is expressed as a number in hexadecimal format.

HLL (Higher Level Language)

The term HLL refers to the computer programming languages that not only allow the use of symbolic operators to signify operations and symbolic names to represent data and data structures, but are also structured with syntax and semantics to describe the computing algorithm. They enable program development in a much more user friendly manner and not dependent on computer's hardware and architecture. Examples include Python, Visual Basic, Ruby, C#, Java and others.

HODL

HODL is one of the most frequently used slang terms in the crypto community. It has been derived from misspelling of “hold” and originated in 2013 when user Gamekyuubi posted an entry that ‘I am Hodling’ in a Bitcoin forum. He used it to indicate that he is holding onto Bitcoin even after prices are falling, owing to his poor trading skills. Now HODL is used to indicate holding Bitcoins or cryptocurrencies rather than selling it when prices drop.

Homestead

Homestead is the second major version of the Ethereum platform and is the first production release of Ethereum. It includes several protocol changes and a networking change that provides the ability to carry further network upgrades, however it has few backward incompatible protocol changes. Hence, it required a Hard Fork. The first version of Ethereum release was referred as Frontier.

Hot Wallet

A hot wallet is a tool that allows a cryptocurrency owner to receive and send tokens. It is connected to the internet unlike a cold wallet and exists in Software formats too called as Software wallets. Metamask, Coinbase, Binance andGemini are examples of Hot Wallets.

Huobi Global

Huobi is a Seychelles-based cryptocurrency exchange providing trading, storage and wallets. Founded in China, financed by ZhenFund and Sequoia Capital, the company now has offices in Hong Kong, South Korea, Japan and United States. In August 2018 it became a publicly listed Hong Kong company. It supports trading of over 350 cryptocurrencies.

Hyperledger Fabric

Hyperledger Fabric, an open-source project from the Linux Foundation, to develop modular blockchain framework, started in the year 2015. With initial contributions from IBM, SAP, Intel and others, it has become the de facto standard for enterprise blockchain platforms. Has been focused on developing enterprise-grade applications and industry solutions, open, modular architecture uses and plug-and-play components to accommodate a wide range of use cases. Hyperledger Fabric is part of Hyperledger Foundation that supports other distributed ledger frameworks like Sawtooth, Indy, Burrow, Besu, Iroha; tools like Caliper, Cello, Avalon, Explorer and libraries like Ursa, Aries, Quilt and Transact. Hyperledger currently has more than 250 members.

CHAPTER 9

I

IBFT (Istanbul Byzantine Fault Tolerance)

Istanbul Byzantine Fault Tolerant (IBFT) consensus is inspired by Castro-Liskov 99 paper. IBFT inherits from the original Practical Byzantine Fault Tolerance by using a 3-phase consensus; Pre-prepare, Prepare and Commit. The system can tolerate at most F faulty nodes in an N validator network, where N = 3F + 1. It is considered as an alternative to Proof of Work in Ethereum and is quite appealing for Consortium and Private Blockchains. It was first implemented in Geth and then in Quorum.

ICAP (Interexchange Client Protocol)

ICAP is the world's largest interdealer broker network for over-the-counter (OTC) trading. ICAP, which matches buyers and sellers of bonds, swaps and currencies, has become the first company to distribute data on trades to customers using the same blockchain technology that powers the virtual currency bitcoin.

ICO (Initial Coin Offering)

Initial Coin Offering refers to raising funds by selling new cryptocurrency offerings. Its similar to an IPO (Initial Public Offering) that raises funds, when a new company ventures onto the stock market. In ICO, the company raising funds defines exchange price between their native cryptocurrency (offering) with other cryptocurrencies especially Bitcoin, Ether and also with various other fiat currencies. NEO, Ethereum, Stratis and Filecoin had successful ICOs. Some ICOs provided good returns to investors but many turned into fraud or failed to provide any returns.

IEO (Initial Exchange Offering)

IEOs appeared on the horizon as many ICOs failed. Unlike ICO, where fund raise is carried out by the promoter or project team, IEO has fund raise administered by a cryptocurrency exchange. This helps in adequate validation of a new Cryptocurrency or Blockchain project that is raising funds and also creates required confidence or trust in the project. Binance Launchpad, Gate.io and Bittrex IEO are leading IEO platforms in the world. Sero, WazirX, HyperDAO and Mattic are examples of successful IEOs completed till date.

Immutable

Immutability is the ability of a blockchain ledger to remain a permanent, indelible, and unalterable history of transactions. Immutability has the potential to transform auditing process into a quick, efficient, and cost-effective procedure, and bring more trust and integrity to the data businesses use and share every day.

Indy

Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. It supports Self Sovereign Identity that empowers individuals to control their identity information by allowing them to use it online or offline whenever they want and revoke access to such information whenever they don't want to share such information. This is quite different compared to existing systems where owners cease to have visibility into the shared identity documents and how they are being used or how many times they have been used. Developers can use the tools and libraries from Hyperledger Indy to create identity solutions that are interoperable across jurisdictions and agencies.

Interledger Protocol (ILP)

It is a protocol created by Stefan Thomas and Evan Schwartz, from the blockchain company Ripple, to move money in easy and simple way between two ledgers. ILP does not have a ledger of its own and promotes interoperability between different Blockchain networks.

Interoperability

Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, at present or in future, without any restrictions. Interoperability is essentially the ability to see and access information across various blockchain systems. The ability of different decentralized networks to communicate with one another without any intermediaries will go a long way in giving rise to fully decentralized systems.

World Economic Forum has identified three main categories of interoperability methods as on 2021: Cross Authentication, Oracles and API gateway. Currently, Blockchains are not interoperable and one can operate on only one Blockchain at a time. Eg: Either Bitcoin or Ethereum. Blockchain interoperability projects like Polkadot Blockchain and Cosmos Blockchain are working hard to change this and make various Blockchains interoperable.

IPFS (Inter Planetary File System)

Created by Juan Benet, The Inter Planetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices. IPFS allows users to not only receive but also to host content, in a similar manner to BitTorrent. As opposed to a centrally located server, IPFS is built around a decentralized system of user-operators who hold a portion of the overall data, creating a resilient system of file storage and sharing. Brave (browser solution) and Filecoin (co-operative storage solution) have used IPFS protocols for designing their services and offerings.

Iroha

Hyperledger Iroha is designed to incorporate Blockchain or Distributed Ledger Technology (DLT) into Mobile or IoT devices. It is based on YAC Consensus, Multisignatures and supports Windows, Linux and MacOS environments. It provides alternate design solution for mobile based use cases in Identity management and Finance.

IOTA

Created in 2015 by David Sonstebo, Dominik Schiener, Sergey Ivancheglo, and Serguei Popov, IOTA is an open-source distributed ledger and cryptocurrency designed for Internet of things. It uses a directed acyclic graph (also known as Tangle) to store transactions on its ledger that provide higher scalability over blockchain based distributed ledgers. It is designed to promote microtransactions as it does not use miners to validate transactions. In lieu of miners, nodes that enable new transactions on the network also approve previous transactions. MegaIOTA units represent IOTA trading on different crypto-currency exchanges.

IBM Blockchain Platform

IBM Blockchain Platform is built on the open source, community-based Hyperledger Fabric platform from Linux Foundation. Several companies have started their Blockchain journey and implementation with IBM Blockchain Platform. IBM offers Food Trust (ecosystem of producers, suppliers retailers and manufacturers to create safe and sustainable food system for all), Blockchain Transparent Supply (anti-fragile and transparent supply chain solutions), TradeLens (transforming container logistics by overcoming challenges arising from legacy data systems, manual handling of documents and poor visibility).

IaaS (Infrastructure as a Service)

Cloud infrastructure services, known as Infrastructure as a Service (IaaS), are made of highly scalable and automated compute resources also known as Cloud Computing. IaaS is fully self-service for accessing and monitoring computers, networking, storage, and other services. IaaS providers maintain infrastructure and users buy cloud computing services based on 'On Demand' and 'Pay as you Go' business models. Amazon AWS, Digital Ocean, Microsoft Azure, Google Cloud and Cloud Stack are some well known IaaS service providers.

CHAPTER 10

J

Jaxx

Jaxx is always free to use digital wallet for Bitcoin, Bitcoin Cash, Ethereum, Ethereum Classic, Litecoin, Dash, Zcash and a long list of other blockchain assets and cryptocurrencies. Users can trade in cryptocurrencies, spend, and receive them using Jaxx. It supports third party apps like Changelly and Simplex.

Jaxx Liberty

Jaxx Liberty is more than a cryptocurrency wallet. It has features like cryptocurrency holdings, pricing, news and rewards in the same app and acts as a one-stop gateway to manage cryptocurrency wealth. It is available and synced across Android, iOS, macOS, Windows, Linux and the Chrome browser.

JSON

Java Script Object Notation (JSON) is a text format used for storing and transporting data between computers. It is language independent and very similar to the code used for creating JavaScript objects. JSON makes it possible to store JavaScript objects as text. JSON files are used to store Blockchain.

CHAPTER 11

K

Kafka

Kafka, created and open sourced by LinkedIn in 2011, is a community distributed event streaming platform capable of handling trillions of events a day. Initially conceived as a messaging queue, Kafka is based on abstraction of distributed commit logs. Commit log is basically a data structure that only appends; modifications or deletions are not possible. Later, Kafka evolved into a full-fledged event streaming platform. In Blockchain implementations, it helps in scalability, reliability, durability and high performance. It is designed to handle high loads of transactions. For lesser loads, message queues like RabbitMQ can be used.

Keyfile

A Keyfile in a blockchain is an encrypted version of a private key. It is generated using a private key and a password that one uses to encrypt it. If one opens up a keystore file in a text editor, it will show data pertaining to encryption of the private key.

Keys

There are two types of keys in Blockchain - Public key and Private key. Public key usually reflects address used for transactions in blockchain. Private key provides access to cryptocurrencies or ownership of funds contained in such a given address. A Blockchain wallet automatically generates and stores private keys. Private Keys establish ownership and helps in signing transactions to spend the funds.

Klaytn

Kakao's (Korea's largest mobile platform) global public blockchain project Klaytn is an enterprise-grade, service-centric platform that brings user-friendly blockchain experience to users. It combines best features of both public and private blockchains via an efficient 'hybrid' design. Klaytn is secured by participation from numerous highly-reputed brands around the globe, working together to create a reliable business platform along with robust system of decentralized trust. Klay is its native asset that fuels and secures the protocol.

Kraken

Kraken is a United States-based cryptocurrency exchange and bank, founded in 2011, and owned by Payward Inc. It supports crypto-currency to fiat-money conversion and trading for 40 cryptocurrencies. It streams cryptocurrencies' price information to Bloomberg Terminals. As of 2020, Kraken's services are available to residents of 48 states in the USA and 176 countries.

Kubernetes

Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and clustering groups of hosts running Linux container and services. It was designed by engineers at Google in 2014 and has a large, rapidly growing ecosystem. The name Kubernetes originates from Greek, meaning helmsman or pilot. It is often called as K8s as there are exactly eight letters between K and S.

KYC (Know Your Customer)

KYC is a set of activities or guidelines in financial services where service providers make an effort to verify identity of customers, their suitability, and risks involved in maintaining a business relationship with them. KYC documents usually encompass Proof of Identity and Proof of Address documents like Passport, Driving License, Voters' Identity and others. KYC helps Banks, Financial Institutions and Cryptocurrency exchanges to enforce and accomplish Anti-Money Laundering policies. eKYC refers to using internet or digital means to complete identity verification.

Kimchi premium

Kimchi premium is the difference in crypto prices in South Korea compared to rest of the world. The kimchi premium is most commonly seen in Bitcoin prices and peaked at 55% in January 2018. Lack of other high return investment avenues, deep interest in technology and online gambling have led to occurrence of this Kimchi premium in South Korea.

CHAPTER 12

L

Ledger

A ledger is a book containing accounts in which classified and summarized information from journals is posted as debits and credits. Blockchain is a public electronic ledger built around a Peer to Peer (P2P) system that can be openly shared in case of Public Blockchain and with permission in case of Private Blockchain. It is shared amongst disparate users to create immutable or unchangeable record of transactions, each-one, time-stamped and linked to previous one.

Libra (Now, Diem)

Libra a.k.a., Diem, is a cryptocurrency created by Facebook and intended to be used as a simple, low-fee medium of exchange around the world. It is backed by a basket of assets, which include major currencies and government debt securities that provide pricing stability. Hence it is a stable coin. Diem has 26 members that include financial firms, non-profits and Facebook's digital wallet company Novi.

Light Client

Light clients, also known as partial nodes or lightweight clients, are crucial elements in blockchain ecosystems. They help users access and interact with a blockchain in a secure and decentralized manner without having to sync the full blockchain. They are based on light nodes that download only block headers to establish authenticity of transactions. They are served by full nodes when connected with entire Blockchain network.

Light Node

Lightweight nodes verify transactions using a method called simplified payment verification (SPV). SPV allows a node to verify if a transaction has been included in a block, without having to download entire blockchain. With SPV, full nodes serve lightweight nodes by allowing them to connect and transmit their transactions to the network and will notify them when a transaction affects them. A lightweight node needs to download only the headers of all blocks on the blockchain, which means that its download and storage requirements are significantly less intensive compared to a full node.

Lightning Network

The Lightning Network is a layer 2 payment protocol that operates on top of a blockchain-based cryptocurrency. It is intended to enable fast transactions amongst participating nodes and has been proposed as a solution to address bitcoin scalability problem. Transactions between parties will be executed off the Blockchain i.e. as off-chain transactions. It will reduce transaction processing times and associated costs. Thaddeus Dryja and Joseph Poon formulated Bitcoin Lightning Network in 2015.

Linux Foundation

The Linux Foundation, headquartered in San Francisco, USA, is a non-profit technology consortium founded in 2000 as a merger between Open-Source Development Labs and Free Standards Group to standardize Linux, support its growth and promote its commercial adoption. It promotes adoption of Open or Open source technology. 1.15 billion lines of code, 235000+ developers and 19000+ contributing companies constitute the power and global impact of Linux Foundation. Cloud Foundry, Delta Lake, Drone Code, Hyperledger Blockchain, Node.js and Open Chain are well known projects under the aegis of Linux Foundation.

Lite Coin

Litecoin (LTC or Ł) is a peer-to-peer cryptocurrency and open-source software project released under the MIT/X11 license. Litecoin was an early bitcoin spinoff or altcoin, that started in October 2011. Litecoin was released via an open-source client on GitHub on October 7, 2011 by Charlie Lee, a Google employee who later became the Engineering Director at Coinbase. The Litecoin network went live on October 13, 2011. It was forked from Bitcoin Core client and uses new algorithm Scrypt unlike SHA-256 in Bitcoin.

Liquidity mining

Liquidity mining (or yield farming) is a key feature of DeFi that allows people to deposit (or "stake") one cryptocurrency or token on a Decentralized Exchange (DEX) or dApp for rewards. It was popularized by DEXs like Uniswap and Compound. Trading is done through token swapping within a liquidity pool. Every time a user trades, user will pay a certain fee. Automatic Market Maker (AMM) collects fees and grants them to Liquidity Providers as rewards.

Liquidity_pools

Liquidity pools are a feature of DEXs that allow people to trade between each other without any middlemen.

CHAPTER 13

M

Main Net

Mainnet is the term used to describe when a blockchain protocol is fully developed and deployed as a live network unlike Testnet. Mainnet has cryptocurrency transactions that are being broadcasted, verified, and recorded on a distributed ledger technology. A mainnet is a blockchain that performs the functionality of transferring a digital currency from a sender to a recipient. It is also deemed as the final outcome of the project and fulfilment of the commitments made in white paper of respective Blockchain project.

Market Cap (Market capitalization)

Market capitalization, or market cap is the aggregate market value of a company represented in dollar amount or any other applicable fiat currency. Since it represents the market value of a company, it is computed based on the current market price of its cryptocurrency and the total number of issued cryptocurrencies that are in circulation. Coinmarketcap.com tracks market capitalization of almost 5000 cryptocurrencies in addition to cryptocurrency prices, price changes in 24 hours and 7 days duration and their circulating supply.

Merkle Tree

Merkle tree, also known as Hash tree, is a data structure that securely and efficiently encrypts large amounts of data. It is represented as a tree of hashes, in which every leaf node is labelled with the cryptographic hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees are a generalization of hash lists and hash chains and allow for verifications of large amounts of data. They provide secure and efficient verification of large amounts of data.

Merkle Patricia Tree

Merkle Patricia Tree or Merkle Patricia Trie, is a modified form of Merkle tree used by Ethereum to optimally store large amounts of data including the ability to save states. Merkle Patricia tries to provide a cryptographically authenticated data structure that can be used to store all (key, value) bindings. It combines the characteristics of a Patricia Trie and Merkle Tree.

Patricia trie is a data structure which is also called Prefix tree, radix tree or trie and is commonly used for implementing routing tables and systems that are used in low specification machines like the router.

Merkle Root

It is the hash of all hashes of all transactions contained in the block. It is part of the Block header. By just downloading the small block headers and merkle tree, it is possible to establish that a transaction has been accepted by Blockchain network. There is no need to download entire Blockchain to establish validity of a transaction.

MetaMask

MetaMask is a software cryptocurrency wallet developed by Consensys, used to interact with Ethereum blockchain. It has web browser extensions available for Chrome, Firefox and Brave and is used to for Ethereum and ERC 20 only. It doesn't support Bitcoin transactions. It allows users to execute Ethereum transactions through regular websites.

Metropolis

Metropolis is the 3rd stage in the 4-stage evolution of Ethereum, after Frontier and Homestead. It has lot of interesting features such as:

ZK-Snarks. (Zero Knowledge Succinct Non-interactive arguments of Knowledge) that allow verifiers to establish authenticity of claims without explicitly exposing the information. i.e. it is based on Zero Knowledge Proof

Proof of Stake early implementation

Flexibility and robustness of smart contracts

Account Abstraction

Micro chain

Microchain which is a variation of sidechain enables assets of a chain to be transferred to another blockchain. In reality, there is no actual transfer of assets from one chain to another. They are locked on originating chain and created on destination chain. They also extend the consensus rules and logic of smart contracts from one chain to another. The side chain is strongly coupled with parent chain and serves as a full validator of the parent chain's consensus rules.

Micropayment

A micropayment is a small transaction, often carried out online, that can be as small as a fraction of a cent. Depending on the payments system, a "micropayment" may be defined as any transaction size less than $1.00, $5.00, or more. Blockchain technology has brought the idea of viable online and instantaneous micropayments back from the dead state and it offers a new way to make these tiny payments work. Blockchain removes high transaction charges to make micropayments successful. This has been amply demonstrated by BuffiDai, a conference coin built on MakerDAO's Dai stablecoin. It demonstrated processing cost of all transactions at USD 0.20 only, as compared to a cost of USD 2400 that would be incurred if vendors accept credit cards based payments.

Miners

A miner is a node in a Blockchain network that collects transactions and organizes them into blocks. Whenever transactions are made, all network nodes receive them and verify their validity. Then, miner nodes gather these transactions from the memory pool and begin assembling them into a block after validation. In Bitcoin network, miners receive two kinds of rewards – New Bitcoins (for finding new Bitcoin blocks, solving mathematical problems successfully to obtain private keys pertaining to the blocks so that blocks can be confirmed and transactions can be written into them) and Transaction fees (for validating transactions so that Bitcoin involved in the transaction can be spent).

Mining

Cryptocurrency mining is the process in which transactions between users are verified and added to the blockchain public ledger. The process of mining is also responsible for introducing new coins into the existing circulating supply, by solving complex mathematical problems with the help of computers' processing power. It is one of the key elements that allow cryptocurrencies to work as a peer-to-peer decentralized network, without the need for a third-party central authority.

Mining Difficulty

Mining difficulty is a relative measure of the amount of computer resources required for mining, Eg: fresh bitcoin. It either increases or diminishes roughly every 2,016 blocks in Bitcoin. If previous 2016 blocks were mined easily, the mining difficulty increases for next 2016 blocks and vice versa. In Ethereum, difficulty is measured based on how many hashes or miners are involved in finding a valid solution to solve next Ethereum Block. As more miners or hashing power is added to the network, difficulty will increase automatically ensuring new blocks are not added to the network quickly.

Mining Pool

In cryptocurrency mining, a mining pool is the pooling of computer resources or compute power by miners, who share their processing power over a network, to solve mathematical problems to find new blocks. They split rewards equally, according to the amount of compute power and work they contributed to finding and solving new blocks. Slush Pool (1.25 million BTC mined), ViaBTC, AntPool and BTC.com are some of the leading Bitcoin mining pools in the world. SparkPool, Ethpool, Nanopool and Dwarfpool are some of the leading Ethereum Mining pools.

Mint

Bitcoin.com has launched Mint, a free platform that empowers anyone to create tokens quickly and easily. Combined with other pro-token products by Bitcoin.com, Mint is expected to drive blockchain adoption, as it fuels the development of a vast new token ecosystem. Mint is being upgraded to Pitco 2.0.

Mist

Mist is an all-in-one software to manage all assets and contracts of an individual in Ethereum Blockchain. Mist can browse DApps, manage contracts, manage Ether and other digital assets. It acts like a window to the Blockchain network and accesses different applications and services provided in the network. It also supports Whisper (decentralized communication protocol) and Swarm (decentralized storage platform).

Morden

Ethereum version 0.9 was launched under the name Olympic in early 2015. It was the first Public Testnet. By mid 2015, Olympic became deprecated and was replaced by Morden. Later, Frontier official Ethereum version 1 was launched as public main network in 2015 and was forked to Homestead in 2016. Morden was equivalent to Frontier from a test net perspective. It became deprecated in late 2016 and was replaced by Ropsten.

Multisig (Multi-signature)

Multi-signature (Multisig) refers to using multiple keys to authorize a blockchain transaction, rather than a single signature from one key. It avoids a single-point of failure, making it substantially more difficult for the wallet to be compromised. So, a multisig wallet can be programmed in such a way that a transaction can be authorized if atleast 2 out of 3 keys are used. Electrum, Armory and BitGo are examples of Multisig wallets.

CHAPTER 14

N

NAT (Network Address Translation)

NAT translates the IP addresses of computers, registered or unregistered, in a local network to a single IP address. This address is often used by the router that connects computers to Internet. The router can be connected to a DSL modem, Cable modem, T1 line, or even a Dial-up modem. Blockchain is empowering Smart NAT management scheme to overcome limitations that exist in vertical model. With Blockchain implementation for NAT, every peer will agree on necessary parameters required to manage complicated NAT and Mobility management procedures.

Neo bank

A neobank is a kind of digital bank without any branches. Rather than being physically present at a specific location, neobanking is entirely online. Neobanks are also called as fintech firms that provide digital and mobile-first financial solutions payments and money transfers, money lending and more. Chime, Monzo, Revolut, N26 and Klarna are some of the top Neo Banks globally.

Network Value Model

In Blockchain network, every participant has to have their own value but the network itself should be setup to facilitate it. So, the value model is based on principles to create value for 1) everyone funding the network 2) everyone who needs this network and 3) everyone using the network regularly. Usually, we see a major company building a permissioned or permissionless blockchain network, but it's really the vendors using it who drive the adoption and usage of such blockchain network. Hence, the value has to be created for all parties and should be done in the design phase of the prototype or the minimum viable product (MVP) or network stage. If its not accomplished during MVP stage, it should certainly be done in the Go-To-Market stage while scaling from MVP stage to ecosystem production state.

Nexledger

Nexledger is an open-source hybrid, private-permissioned blockchain platform developed by Samsung SDS. Nexledger is a full-features platform with a core that integrates a range of components such as monitoring tools, external linkages, application programming interfaces and a structured DevOps environment. It comes in versions that are compatible with Ethereum (Nexledger E) and Hyperledger Fabric (Nexledger F). It has two offerings – Nexledger Universal that provides API libraries to integrate multitude Blockchain consensus algorithms and Nexledger Accelerator that helps in increasing Transaction Per Second (TPS) upto 15 times.

NFT (Non Fungible Token)

A non-fungible token (NFT) is a unit of data on Blockchain digital ledger, where each NFT can represent a unique digital item; hence they are not interchangeable. NFTs can represent digital files such as art, audio, videos, items in video games, virtual assets and other forms of creative work. The NFTs can be bought on an NFT marketplace. NFTs have led to a significant growth in Digital Collectibles also referred to as Crypto collectibles. Cryptokitties, Cypherpunk, Topshots are some of the leading NFTs. They are sold on various market places – NBA Top Shot (Basket Ball), Sorare (Soccer), Decentral Land (Virtual Real Estate), Axie Infinity (Video Games).

NGMI (Not Going to Make It):

Its a crypto slang used to indicate that a crypto trader or investor is going to miss a huge profit in a particular trade. It is also used as a name for a meme crypto, where in a person selling a NGMI token will not be allowed to buy back.

Nick Szabo

Nick Szabo is a computer scientist and cryptographer known for his research in digital contracts and digital currency. He graduated from the University of Washington in 1989 with a degree in computer science and received a law degree from George Washington University Law School. The phrase and concept of smart contracts was developed by Szabo. He proposed Bit Gold in 1998 – one of the initial efforts aimed at creating decentralized virtual currencies. Bit Gold principles resemble Bitcoin closely in terms of time stamped Blocks that are stored in title registry and created using Proof of Work (PoW).

NIPoPoW (Non interactive Proofs of Proof of Work)

Developed by Universities of Athens, Edinburgh, Illinois and others. These are used to verify whether an event has occurred in a Blockchain network that runs on Proof of Work (PoW) consensus mechanism. These can be verified by various nodes in the network without connecting to the Blockchain network and without downloading block headers. They support side chains and lightweight blockchain wallets on mobile phones.

Node JS

Node.js is an open-source, cross-platform, back-end JavaScript runtime environment that runs on the V8 engine and executes JavaScript code outside a web browser. It was written by Ryan Dahl and released in 2009. Node.js lets developers use JavaScript to write command line tools and for server-side scripting—running scripts server-side to produce dynamic web page content before the page is sent to the user's web browser. In addition to Java Script, it is also written in C, C++. Node JS is being used to develop Cryptocurrencies and set up Blockchains.

Nodes

Nodes form the infrastructure of a blockchain. They store, spread and preserve blockchain data, so theoretically a blockchain exists on nodes. A full node is basically a device (like a computer) that contains a full copy of transaction history of blockchain. Peer to Peer (P2P) protocol allows nodes to interact, communicate with one another in Blockchain network and propagate information about new blocks and transactions. Nodes are of three types – Miner Nodes, Light Nodes and Full Nodes.

Nonce (Number only Used Once)

Nonce is a random whole number, which is a 32-bit (4 byte) field. It represents the number that miners compete to solve and receive cryptocurrency. Miners adjust Nonce so that it becomes a valid number to be used for hashing the value of a block. Nonce is the number which can be used only once. Once the perfect Nonce is found also known as Golden Nonce, it is added to the hashed block. This completes the Block and its addition to Blockchain. Along with this number, the hash value of that block will get rehashed to create a difficult algorithm that makes Blockchain stronger and secure.

Notary

In the traditional world, a notary is a person authorized to perform acts in legal affairs, in particular witnessing signatures on documents. Distributed Ledger Technology firm R3 uses the 'notary service' to prevent double spending in its Corda Blockchain network. A notary cluster is a network service that provides uniqueness to consensus by attesting it for a given transaction. Its applicable only to transactions that are not signed and those that do not consume any of the proposed transaction's input states. If the transaction has already been signed, it rejects the transaction and flags it with a double-spend attempt. It represents point of finality for transactions as valid or invalid in the system.

NVT ratio

NVT stands for Network Value-to-Transactions and is calculated by dividing Network value with Daily transaction volumes. It was introduced by Willy Woo in 2017. NVT, for cryptocurrencies, can be considered as equivalent to Price to Earnings (P/E) ratio that is used to calculate equities' valuations. NVT implies whether Blockchain network or cryptocurrencies overvalued or not. If the value of a Blockchain network is too high and it is not substantiated by proportionate amount of transactions or coins exchange, it indicates a potential pricing bubble that will be corrected soon.

CHAPTER 15

O

OAuth (Open Authorization)

OAuth is an open standard for Single Sign On (SSO) and access delegation. It is commonly used as a way for Internet users to grant websites or applications authorization or permission to access their information on other websites, but without giving them passwords. Eg: Using one's Google or Facebook Id / Authentication to login to other websites or applications. It enables limited access to user's data. Currently there are two versions of OAuth – Version 1 and Version 2.

Off Chain Governance

Off-chain Governance refers to those rules that apply to transactions occurring in a Blockchain or Cryptocurrency network that moves value outside of the blockchain. Off-chain transactions are primarily supported to make transactions faster, cheaper and more private. They are most suited for non-cryptocurrency transactions. For eg: A Digital Identifier can be stored On-chain in Public or Private Blockchain and information supporting it like a Passport, Drivers License and Personally Identifiable Information (PII) contained in these documents can be stored Off-chain.

Offline Wallet

Also known as Cold Wallet, it is a wallet not connected to internet, therefore has a far lesser risk of being taken over or compromised. Electrum Cold Wallet, Ledger Nano S, Trezor Model T and Coinbase Vault are good examples of Offline Wallets.

On Chain

On-chain transactions are transactions that occur on a blockchain and are reflected on the distributed, public or private ledgers as applicable. These transactions cannot be reversed after they are verified and confirmed on Blockchain. They can be reversed only if majority of the network agrees to do so. Hence they offer very good security and transparency.

On chain Governance

On-chain governance is a system for upgrading blockchains in which code changes are encoded into the protocol and decided by stakeholder voting i.e. every node votes on whether to accept or reject proposed changes. It promotes Transparency, Faster Consensus, Lasting and Binding Code Changes and Decentralized Decision Making.

Onclave

Onclave Networks, Inc. is a global cybersecurity leader that specializes in protecting operational technology (OT/IoT) through private networks. It provides Zero Trust secure communications platform that protects OT / IoT devices from unauthorized access and cyberattacks.

Online Wallet

Also referred as Hot Wallet, which is connected to the Internet and is far more vulnerable to hacks. Exodus and Mycelium Hot wallet are examples of Online wallets.

OpenShift

OpenShift is a family of containerization software products developed by Red Hat. It is a Kubernetes distribution focused on developer experience and application security which is platform agnostic. OpenShift helps to develop and deploy applications to one or more hosts. These can be public facing web applications, or backend applications, including micro services or databases. Some Blockchain application providers have enabled using of OpenShift in a turnkey way to deploy Blockchain capabilities.

Open Zeppelin

Open Zeppelin provides a battle-tested library of smart contracts for secure smart contract development on Ethereum. It includes the most used implementations of ERC standards. Coinbase, Augur, Bitgo, Brave and Ethereum Foundation are powered by Open Zeppelin.

Oracles

Oracles are third-party services that provide smart contracts with external information so that decisions can be made by smart contracts. They serve as bridges between blockchains and systems in outside world. Cryptocurrency Exchange Pricing and Agriculture Insurance are two well known use cases that have proven the importance of Oracles to authenticate origin and sanctity of external data sets for smart contract execution. For eg: If there is a decentralized crop insurance that covers farmers from natural calamities, Oracles sends data to Smart contract governing such insurance about extent of damage, so as to authorize or decline insurance claims and dispense claims accordingly.

Orchestration

Orchestration is the automated configuration, management, and coordination of computer systems, applications, and services. Blockchain can be used to secure Virtual Machine Orchestration for cloud computing and network virtualization.

Orderer

Ordering service provides a shared communication channel to clients and peers, offering a broadcast service for messages containing transactions. It helps in collating transactions into Blocks and distributing them to Anchor peers in the Blockchain network. Ordering service, an important functionality of Hyperledger Fabric, also facilitates Channel creation by maintaining a list of organizations that are allowed to create them. Such list of organizations is called as Consortium.

Orphan Block

Orphan blocks, often referred to as stale blocks, are blocks that are not accepted into the blockchain network due to a time lag in the acceptance of such block into the blockchain. These also refers to blocks that are submitted to a node without its entire ancestry (previous Blocks), hence they cannot be validated. Miners don't get rewarded or incentivized for these Orphan Blocks.

OpenChain

OpenChain is a public blockchain platform developed by Coinprism. This powerful environment helps companies create Blockchain systems for experimentation. Anyone can spin up a new instance of blockchain on the environment within seconds. Additionally, end-users can exchange values on the ledger according to rules identified by the administrator of Blockchain. It is most suited for issuance and management of Digital Assets, also supports Land titles ownership and management, Music licensing, Gifts cards and Loyalty points.

Overbought

A crypto is said to be overbought if its price has gone up over a period of time without any rationale. An overbought crypto is considered to be trading above its fair value. Tools like Relative Strength Index are used to identify whether a Crypto is Overbought or Oversold and is based on recent momentum in pricing, typically over a 14 day period.

CHAPTER 16

P

P2P (Peer to Peer)

Peer-to-peer is a decentralized interaction where in two individuals interact directly with each other without any intermediary or 3rd party in between. P2P computing or networking is a distributed application architecture that distributes or divides tasks or workloads between different personal computers also known as peers. P2P network shares processing power, network bandwidth and storage space. A Blockchain network operates using a P2P network which runs the protocol and maintains identical copies of ledgers with recorded transactions.

Pancake Swap

It is a decentralized exchange built on Binance Smart Chain and enables users to trade cryptocurrencies without any intermediary. It is powered by automated Smart contracts and taps into user generated liquidity pools.

Parity

Parity is an open-source software solution written in Rust programming language. It offers an alternative to Geth Ethereum client and allows individuals to run nodes on public Ethereum network, or any other blockchain network that uses Ethereum. Parity offers Miners, Node operators, and Exchanges, benefits like fast synchronization and maximum uptime.

PDOs (Private Data Objects)

Used in Hyperledger implementations, Private Data Objects (PDO) enables sharing of data and facilitates coordination amongst parties that do not trust one another. Interaction is facilitated through smart contracts that are enforced through execution in Trusted Execution Environment (TEE). PDOs perform contract execution and storage off the Blockchain. Only the hash representing the Blockchain state is stored on the distributed ledger. PDOs help in implementing privacy preserving distributed ledgers.

Pegging

Linking cryptocurrencies value to fiat currencies, gold or other commodities is known as pegging. This provides pricing stability to cryptocurrencies that are linked and insulates them from significant changes in value. Such linked cryptocurrencies are also known as Stablecoins. True USD (TUSD), Tether (USDT), Paxos Standard (PAX) are pegged with United States Dollar.

Permissioned Blockchain

A Blockchain requiring permission or prior approval before using it is known as Permissioned Blockchain. It is also known as Private or Enterprise Blockchain where Blockchain is hosted by a company or an enterprise or an industry body, technically referred to as Central Authority that authorizes others to join the Blockchain as trusted validators. Hyperledger Fabric, Corda and Quorum are examples of Permissioned Blockchains.

Permissionless Blockchain

Permissionless blockchains are blockchains that require no prior permission to join or use them. They are also known as public blockchains. They digitize trust and eliminate the need for intermediaries who otherwise are required to mediate transactions or foster trust in them. Bitcoin and Ethereum are examples of Permissionless Blockchains.

PKI (Public Key Infrastructure)

PKI made its first appearance in 1990s to administer and manage encryption keys through digital certificates. These digital certificates confirm the identity of people, devices or applications that own private keys and corresponding public keys. This ensures that people who are sending information through encryption gain required confidence that desired recipients of such information are actually the ones who will receive and read it. Anyone else who is not the intended recipient, will not have the ability to intercept and interpret such information. PKI assigns identities to keys so that senders and receivers of information can accurately verify one another. Verisign, Gemalto, GlobalSign, WISekey, ENIGMA and eMudhra are leading PKI providers in the world.

Plasma

Created by Vitalik Buterin, Co-Founder of Ethereum, Plasma refers to a framework that allows creation of child blockchains that use the main Ethereum chain for arbitration and creating trust. It uses smart contracts and verification to offload transactions from the main Ethereum chain into a side chain. These side chains or plasma chains enable fast and lower cost transactions and their validation is preserved on the main Ethereum chain. In essence, Plasma will help Ethereum Blockchain handle much larger transactions and speed, thereby addressing the performance challenges.

PoET (Proof of Elapsed Time)

PoET is a blockchain network consensus mechanism algorithm, used frequently on permission blockchain networks. It is based on Intel's CPUs called SGX – Software Guard Extensions. It prevents high resource utilization and high energy consumption and keeps the process more efficient by following a fair lottery system. The algorithm uses a randomly generated elapsed time to select the node that will win the new block. Miners generally go to sleep and don't participate in mining while waiting for their turn. Hence it facilitates energy efficient mining.

Polkadot

Polkadot is a heterogeneous multi-chain interchange possessing a translation architecture that enables customized side-chains to connect with public blockchains. It allows data and tokens to be transferred across Blockchains thereby facilitating cross-chain registries and computations. Polkadot's first token sale closed on October 27, 2017 raising a total of 485,331 ETH. Gavin Wood, Thiel Fellow Robert Habermeier and Peter Czaban are the co-founders of Polkadot. Gavin Wood was previously the Chief Technology Officer and is co-founder of the Ethereum Project. It is also a flagship project by Web3 Foundation to build a fully functional and decentralized web.

Private Blockchain

A private blockchain is an invitation-only blockchain. The blockchain is governed by a single entity. The participating parties require permission to read, write, or audit the blockchain. The blockchain can have multiple layers of data access to keep certain pieces of data confidential. Also known as Permissioned Blockchain.

Private Keys

A private key, also known as a secret key, is a variable in cryptography that is used with an algorithm to encrypt and decrypt messages or information. Secret keys are only shared with the key's generator, making it highly secure. Private keys play an important role in symmetric cryptography, asymmetric cryptography and cryptocurrencies.

Proof of Activity (PoA)

Decred, a well known cryptocurrency, uses Proof-of-activity which is a hybrid consensus algorithm. PoA is a combination of two other blockchain consensus algorithms: Proof-of-Work (PoW) and Proof-of-Stake (PoS). It is used to ensure that all transactions occurring on the blockchain are genuine and that all miners arrive at a consensus. Blocks that are mined do not contain transactions; they contain only header information and mining reward addresses. Network fees or rewards are shared between miners who find the blocks and validators who sign the blocks.

Proof of Authority

Proof of Authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks, especially the private ones. The term was proposed in 2017 by Ethereum co-founder and former CTO Gavin Wood. Rights to generate new blocks are given to nodes that have proven their authority; authority is obtained through clearing preliminary authentication. Benefits of PoA include –

No need for high performance hardware

High transaction rates

New blocks generation time or intervals are predictable

IOTW Blockchain uses PoA consensus algorithm.

Proof of Burn

Proof-of-Burn (PoB) is a blockchain consensus mechanism that requires minimal energy consumption compared to proof-of-work (PoW). In this mechanism, miners burn coins by sending them to addresses from which coins cannot be retrieved instead of investing in expensive computers to mine. This burning provides miners a privilege to mine based on random selection process. Slimcoin and Third Generation Coin (TGCoin) use Proof of Burn consensus mechanism.

Proof of Stake

A consensus mechanism used to achieve distributed consensus. In case of Ethereum, it requires users to put on stake their Ether to become a validator. Validators are chosen randomly to create blocks and are responsible for checking and confirming blocks they do not create. This confirmation or validation is like attestation. Validators obtain rewards for proposing new blocks that are good and not malicious and lose their stake in-case they attest malicious blocks. Proof of Stake consensus mechanism is better than Proof of Work in energy utilization and providing higher immunity to centralization. Owing to energy efficiencies, cryptos using Proof of Stake are also knows as green cryptos like Cardano, Polkadot, Neo and Cosmos.

Proof of work

Proof of work (PoW) is a decentralized consensus mechanism used to secure cryptocurrencies like Bitcoin, Ethereum and others. It is used for validating transactions and mining new tokens or coins. It is based on the premise that there are set of values which are difficult to produce but easy to verify. Miners club group of transactions into a block and try to mine. To mine the block, hard mathematical problem called 'Proof of Work' has to be solved. The solution lies in finding a number lower than the hash of the block, which is also known as target hash. Lower the target is, higher the difficulty to generate a block. Miners continue testing various values known as Nonces using compute power till the right value is found to solve the problem. Miner who solves the problem successfully gets the Block reward and adds the block to the network and broadcasts that block has been mined. Once the problem has been solved others can verify it easily based on Proof of Work algorithm. SHA 256, Scrypt and SHA-3 are some of the well-known algorithms powering Proof of Work.

Protocol

Protocols are basic sets of rules governing sharing of data between computers. For Cryptocurrencies, they establish guidelines pertaining to structure of the blockchain, consensus mechanisms and distributed database that allows digital money to be securely exchanged in the network and over the internet.

Public Blockchain

A public blockchain is also known as Permissionless Blockchain. Anyone can join the Blockchain network and information is available in a public domain. Due to its permissionless nature, any party can view, read, and write data on the blockchain and such data is accessible to all. No particular participant or a node in the network has full control over the data contained in a public blockchain. Bitcoin and Ethereum are good examples of Public Blockchain.

Public Keys

A public key is a large numerical value that is used to encrypt data or information. This key can be generated by a software program but in practice is usually provided by a trusted, designated authority known as certification authority. The messages encrypted by public keys can be deciphered using a private key which is held by recipient of information and the key is known only to them. Every public key matches with only one private key.

Pyethereum

Pyethereum is the Python core library of the Ethereum project. In other words, it refers to implementation of Ethereum Virtual Machine using Python programming language. It was written by Vitalik Buterin

Python

Invented by Guido van Rossum in the year 1991. It is a high-level object oriented programming language with dynamic semantics. It has gained popularity and wide adoption owing to simple programming syntax, English like commands and readability of its code. It is widely used for web development, machine learning, artificial intelligence and mobile application development. Latest version of Python is version 3.9 released in October 2020. Python allows developers to create Blockchain using only minimal lines of code and also comes with several free packages that make Blockchain code more efficient.

PaaS (Platform as a Service)

It's a business arrangement or model where users of PaaS need not install in-house hardware and software to develop or operate applications. The PaaS provider delivers software and hardware tools to users over the internet using cloud computing technology. Users will pay based on their usage – "Pay as you Go" pricing model. PaaS is delivered through public, private or hybrid cloud platforms. Various types of PaaS include Open PaaS, Mobile PaaS, Hybrid PaaS, Private PaaS and Public PaaS. Google, Red Hat, Oracle, IBM, Amazon Web Services (AWS) and Microsoft are leading PaaS providers.

Pump and dump

It refers to buyers accumulating cryptocurrencies or tokens with an intention to manipulate the pricing upwards by creating bullish sentiments and spreading wrong information, leading to price inflation (pumping) and then selling them all at once which causes prices to crash (dumping).

PGP (Pretty Good Privacy)

Developed by Phil Zimmermann in 1991 as free email security program, Pretty Good Privacy is an encryption program used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions. PGP uses International Data Encryption Algorithm (IDEA) invented by Xuejia Lai and James Massey in 1991, which is the private key protocol and uses RSA as public key encryption system. It uses both Public and Private cryptosystem to increase the security and privacy of data and e-mail communications.

PGP survived law suits from NSA and US Government in its early days as it helped people and enterprises to secure their communications and insulate them from trapdoors that would have existed in secure communications equipment so that messages could be decrypted and read by the Government.

CHAPTER 17

Q

Quartz

Quartz is a startup incubated by TCS, and provides foundational technology, tools and business components for creating distributed ledger through their offering The Smart Ledgers. It comprises Quartz Smart Solutions – set of business solutions for various industries, Quartz Devkit – smart contracts development kits, Quartz Gateway – helps in easy integration of existing applications with Blockchain networks and Quartz Command Center – helps in monitoring entire ecosystem.

Quantum Computing

Quantum computing is the use of quantum phenomenon such as superposition and entanglement to perform computations at a much faster rate compared to classical computers that we use today. Computers that perform quantum computations are known as quantum computers. The most widely used Quantum computer model is the quantum circuit, based on the quantum bit, or "qubit", which is somewhat analogous to the bit in classical computation. A qubit can be in a 1 or 0 quantum state, or in a superposition of the 1 and 0 states. When it is measured, however, it is always 0 or 1; the probability of either outcome depends on the qubit's quantum state immediately prior to measurement. Quantum computing movement began in 1998 when Isaac Chuang, Neil Gershenfeld and Mark Kubinec created the first quantum computer with 2 Qubits. IBM Q, Google Sycamore and Intel Tangle Lake are well known Quantum computers with close to or greater than 50 Qubits. D-wave has Quantum computers with greater than 128 Qubits but based on Quantum Annealing. Quantum computers are expected to transform medicine by increasing drug discovery speeds, transform communications and artificial intelligence. In Blockchain world, they are expected to impact the cryptographic principles that power Blockchains.

Quorum

Quorum, originally created by JP Morgan and now overseen by Consensys, is an open source blockchain protocol, derived from fork of Ethereum by modifying the Geth client. It is specially designed for use in private blockchain networks. Quorum protocol can be used when there is only a single member owning all the nodes, or, a consortium blockchain network, where multiple members each own a portion of the network. It is transforming use cases pertaining to Trade Finance, Supply Chain Finance, Commercial Bank Payments, Institution Trading, Debt Issuance, Loan Marketplaces, Insurance, Healthcare and Digital Identity.

Quilt

Hyperledger Quilt is a one of the business Blockchain tools that aims to facilitate interoperability between ledger systems by implementing the Interledger protocol (ILP), which is a payments protocol used for moving value across both distributed and non-distributed ledgers. It facilitates distributed atomic transactions (data movement to validate transactions) between IOT companies' wallets, Financial Institutions Ledgers and different supply chain systems. Everis, NTT Data and Ripple are pioneering development.

CHAPTER 18

R

R3

R3, founded in 2014 by David E Rutter and Todd McDonald, is an enterprise software firm that is pioneering digital transformation through Enterprise Blockchain Technology. R3's solutions deliver trust across Financial Services industry and other verticals too where there was a trust deficit pertaining to how enterprises or firms collaborated and transacted with one another. R3's purposely built Enterprise blockchain platform Corda is digitalizing processes and systems that firms rely on, to connect and transact with each other through Blockchain networks in Trade Finance, Insurance, Banking and Capital Markets. More than 350 institutions are deploying, servicing and building on R3's offerings. R3 has also developed Conclave – a Confidential Computing Platform to foster privacy in Enterprise applications where multiple users can securely share and analyze data.

Rabbit MQ

RabbitMQ, owned by VMware, is an open-source message-broker software that 1. Supports Asynchronous Messaging covering multiple messaging protocols, message queuing and flexible routing to queues, 2. Helps in developing cross language messaging with languages like Java, .NET, PHP, Python, Javascript and others 3. Comes with Distributed Deployment and 4. Is Enterprise & Cloud Ready. Rabbit MQ was originally implemented with the Advanced Message Queuing Protocol and later it has been extended to support Streaming Text Oriented Messaging Protocol (STOMP), MQ Telemetry Transport and other protocols.

React JS

Created by Jordan Walke in 2011 while working for Facebook, is primarily used to build web applications and handling the view layer for Web and Mobile Apps. It allows developers to create large web applications that can change data without reloading the page and supports server-side. In Blockchain world, it is being extensively used to develop Cryptocurrency dashboards and building Ethereum Decentralized Applications (dApps)

RxJS

Reactive Extensions for Java Script (RxJS) is a JavaScript library for transforming, composing and querying asynchronous streams of data or call back code. RxJS can be used both in the browser or on the server-side.

REKT

REKT is an internet slang for “wrecked,” meaning severely damaged or utterly destroyed and ruined. In crypto world, REKT refers to someone who has experienced a heavy financial loss due to a wrong trade or investment. It is also used to refer digital assets that lose value.

Relayer

Relayer is an entity that enables hosting a 0x order book that is filled with a number of individually signed orders from various Ethereum addresses. For order fulfillment, direct settlement is carried out on Ethereum Blockchain using deployed 0x smart contracts. Fees for hosting and facilitating orders are collected in ZRX tokens.

Reputation

Reputation is used as an incentive to increase overall trustworthiness in Blockchain whereby miners or validators urge to add a block into blockchain when it has the highest trust value. The authors do not make any assumptions about nodes behavior, and thus, malicious behavior can compromise required consensus.

Rest API

Created by computer scientist Roy Fielding, a REST API is an application programming interface that adheres to the constraints of REST architectural style and allows for interaction with RESTful web services. An API is a set of definitions and protocols for building and integrating application software. REST API is also known as RESTful API. It was created with an intention to establish standard that allows two servers located anywhere in the world to communicate and exchange data.

Rinkeby

Rinkeby is an Ethereum testnet. Testnets are typically used by developers to test their applications or software before deploying them in production or mainnet. Crypto-currencies held on testnet does not contain any value. Rinkeby testnet, unlike Ethereum mainnet, is a Proof-of-Authority network, as opposed to a Proof-of Work network like Ethereum mainnet. Rinkeby has average block time of 15 seconds and average network hashrate of 0.1 Hexa hashes per second.

Ripple

Founded in 2012 by Chris Larsen and Jed McCaleb, Ripple was initially known as Opencoin before the name was changed to Ripple Labs in 2015. Ripple Labs created Ripple as a real-time gross settlement system, currency exchange and remittance network. It is built upon a distributed open-source protocol, and supports tokens representing fiat currency, cryptocurrency, commodities, or other units of value. XRP is the native currency. Its RippleNet hosts payment providers like Banks, Financial Institutions and Money Remittance providers who use Ripple solutions to transfer money globally at lower cost and increased speeds.

RPC (Remote Procedure Call)

Bruce Jay Nelson is believed to have coined the term RPC in 1981. It helps in building distributed, client-serverbased applications and is architected on local procedure calling where in the called procedure may not exist in the same environment or network as the calling procedure. In Blockchain network, RPC facilitates more direct connection, it is initiated by the client and sends a message to the Blockchain node. Users can query for blockchain related information such as block number, blocks, node connection through RPC interface and send transaction request.

Ropsten

Ropsten is a proof-of-work testnet launched in 2016 due to multiple issues in the old testnet and resembles the current Ethereum blockchain. Ropsten Ethereum, also known as Ethereum Testnet, as the name implies is a testing network that runs the same protocol as Ethereum does and is used for testing purposes before deploying on the main network called Mainnet. Ropsten was attacked in February 2016 with Ropsten address swarming the Blockchain with thousands of auto generated, faulty transactions. It was revived on March 2017 with developers rewriting Ropsten Blockchain.

RSI (Relative Strength Index)

It is an important indicator used in Technical Analysis where in quantum of recent price changes are used to ascertain oversold or overbought conditions for stocks and other assets. RSI value of 70 and above indicates overbought or overvalued situation and may indicate trend correction and price adjustments downwards. RSI reading of 30 indicates undervalued situation. In Cryptocurrencies, RSI indicator is based on crypto's price change and speed of this change.

Rugging / Rugpull

This occurs when developers abandon a cryptocurrency or blockchain project and escape with investors' funds. Many rugpulls have occurred on Decentralized Exchanges (DEXs) as DEXs allow easy listing of tokens without any prior due diligence. Rugging also refers to liquidity being removed from liquidity pools. To prevent rugging, projects have implemented measures to commit liquidity through locking contracts and token burn related to liquidity pools. DeFi100 coin creators have rug pulled close to USD 32 million. SushiSwap has also suffered from rugging.

CHAPTER 19

S

Satoshi

A Satoshi is the smallest unit of a bitcoin, equivalent to 100 millionth of a bitcoin. Bitcoins can be split into smaller units to facilitate smaller transactions or micro payments. It has been coined in the honor of Bitcoin's founder - Satoshi Nakamoto.

Satoshi Nakamoto

Satoshi Nakamoto is the name used by the presumed pseudonymous person or persons who developed world's first decentralized cryptocurrency called Bitcoin using Blockchain or Distributed Ledger Technology. Satoshi Nakamoto authored the Bitcoin white paper called 'Peer-to-Peer Electronic Cash System', created and deployed Bitcoin's original implementation. As part of the implementation, Nakamoto also devised the first blockchain database and mined first Bitcoin. It is estimated that Satoshi Nakamoto possesses 1 million Bitcoins.

Sawtooth

Hyperledger Sawtooth is an open-source enterprise blockchain-as-a-service platform that can run customized smart contracts without the need to know the underlying design of the core system. It uses Proof of Elapsed Time (PoET) consensus mechanism and allows smart contract development using Python, Javascript, Rust, Go & C++ languages. It can be deployed as Permissioned or Permissionless Blockchain. Intel, T Mobile, IBM and Amazon Web Services (AWS) are major users of Sawtooth.

Schnorr

A Schnorr signature is a digital signature produced by the Schnorr signature algorithm that was described by Claus Schnorr. It is a digital signature scheme known for its simplicity, whose security is based on the intractability of certain discrete logarithm problems. It is efficient and generates short signatures. It was covered by US patent, which expired in 2 years on Feb 2008. It is used to implement 'Proof of Knowledge'

Scrypt

Created by Colin Percival, it's a password based key deciphering or interpretation algorithm. It was originally used to make large scale hardware attacks unviable. Authorized users need to perform only once while authentication, however a brute force attacker will need to perform the operation billion times within the given time interval making the attack unviable and unsuccessful. Scrypt algorithm has been designed in such a way that it uses large amount of memory unlike other password Key Derivation Functions (KDF) like PBKDF2. Many cryptocurrencies like Litecoin, Dogecoin, Viacoin and Gulden have adopted simplified version of Scrypt for Proof of Work based consensus in their respective protocols.

SDK (Software Development Kit)

A software development kit (SDK) represents set of tools and programs provided by vendors to help developers and build applications for various uses. SDKs are usually associated with mobile apps. Eg: Android tool kit is used to build Android apps and iOS SDK is used to build Apple apps. APIs, Integrated Development Environment, tools pertaining to building, running, testing and debugging are included in SDKs. There are over 1000 SDKs available to build Blockchain and Cryptocurrency applications. Eg: Hyperledger Fabric SDKs, Corda Token SDK and Cosmos Ethereum Virtual Machine SDK.

SegWit (Segregated Witness)

SegWit refers to process changes made in Bitcoin regarding storage of transaction data by increasing the Block size, it was accomplished by removing signature data from bitcoin transactions. When certain parts of a transaction are removed, it frees up space or capacity to add more transactions to the chain.

It went live in August 2017 after being released in 2015. It also helped to fix tampering in Bitcoin transaction ids, that was possible earlier. SegWit2X was a proposal to increase Bitcoin's block size from 1 MB to 2MB. SegWit2X developers wanted to hard fork the Bitcoin to carry out these changes but abandoned it, owing to lack of consensus.

Self-Destruct

It is a function provided on Ethereum network where in self-destruct smart contract when triggered, destroys the contract. It is useful in cases of attacks, where self-destruct function removes smart contract from Ethereum and transfers Ether to the owner's address. Majority of developers use self-destruct function to deploy an updated contract after destroying the old contract.

Self-Executing

Smart contracts are self-executing contracts. They contain terms and conditions of an agreement which are embedded into the software code and are replicated amongst peers in the Blockchain network.

Serenity

Ethereum 2.0 version is referred as Serenity. It is an upgrade of existing Ethereum on the main net. New features include implementation of sharding to facilitate replacement of Proof of Work (PoW) consensus with Proof of Stake (PoS), leading to an increase in transaction speeds. Serenity will be launched in three phases with third phase implementation to be completed by mid of the year 2022. Topaz, Rinkeby, Medella, Zinken are some of the test networks of Serenity.

Serpent

In encryption standards, Serpent refers to block cipher application that came second to Rijndael in Advanced Encryption Standard (AES) Contest. It was developed by Lars Knudsen, Ross Anderson and Eli Biham. Serpent has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. In Blockchain world, Serpent, developed by Vitalik Buterin, refers to programming language that is used to write smart contracts in Ethereum. It is very similar to Python. It was deprecated as Vitalik believed that its technology has become outdated, hence has security concerns.

SGX (Software Guard Extension)

Intel introduced SGX in 2015 and it represents security set instructions baked into Intel's x86 based Central Processing Units (CPUs). SGX facilitates better protection of user's sensitive information by splitting computer's memory into enclaves. Enclaves are private and predefined areas in memory. For Blockchain, SGX delivers enhanced privacy and security to protect the transactions and also helps in increasing consensus efficiency and throughput.

SHA (Secure Hash Algorithm)

Created by National Security Agency in 2001for use in digital signatures. It is well adopted by Public Key Infrastructure market for digital signatures. It is widely used in security applications and protocols including TLS, SSL, PGP, SSH, IPsec, and S/MIME. SHA – 256 algorithms are used in blockchain to get a constant hash of 256 bits every time. This algorithm is also a part of encryption technology.

Sharding

Sharding is a database architecture technique that results in horizontal partitioning of data contained in a database. It is the practice of separating one table's rows into multiple different tables, known as partitions. In Blockchain, sharding is used to increase transaction speed by splitting Blockchain into small sections called as Shards. Each Shard will have its own set of account balances and smart contracts. Each node will have only a part of data on the Blockchain and not entire information. Zilliqa is the first public blockchain to implement sharding.

Shill

A shill is a person who publicly helps or provides credibility to a person or an organization without disclosing that they have a close relationship with them. Shill in cryptocurrency refers to a person holding some cryptocurrency and trying to promote that particular coin or token brand to increase its price and sell their holdings to book profits. John McAfee is considered to be a well-known Shill in the cryptocurrency world.

Side Chains

A sidechain is a secondary blockchain connected to the main blockchain with a two-way peg for exchange of transactions from main chain to side chain and vice versa. They provide efficiency and scalability to mainchain. Sidechains may have their own consensus protocols, which may be completely different from the mainchain's protocol. The two-way peg also enables interchangeability of assets from one blockchain to another securely at a predetermined rate.

Single Point of Failure

It is a malconfiguration, weakness or a flaw in a system that causes it to come to a grinding halt and stop working. It can also be due to malicious attacks such as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. Centralized systems are often prone to single point of failure. Distributed and decentralized systems like Blockchain are insulated from such failures.

Single Source of Truth

A single source of truth is the practice of aggregating data, information from many operating or business systems within an organization into a single location, ledger or system. In blockchain, a single source of truth means every node that is in the network contains same data. This results in a situation where information cannot be altered without the knowledge of others on the network, leading to immutability. Basically error proof and tamper proof system of records.

Slashing Condition

Slashing is a mechanism built into proof of stake blockchain protocol to discourage validators' misbehavior such as persistent downtime, double signing and delegation. Punishments include reduction in stakes and suppression of future rewards and ejection. Slashing is thus designed to incentivize node security, availability, and network participation. Ethereum 2.0, Celo, Cosmos, ICON and Polkadot have various slashing penalties for downtime, delegation and double signing.

Smart Contracts

Smart contracts, first proposed by Nick Szabo in 1994, are simply programs stored on a blockchain that run when predetermined conditions are met. They are used to automate execution of agreements so that all participants are aware of outcomes and abide by them; without any time loss or intermediaries' involvement to enforce outcomes. Ethereum is world's most popular smart contracts platform that uses Solidity for writing smart contracts that run on Ethereum Virtual Machine.

Soft Fork

Soft fork occurs when changes to Blockchain protocols are backward compatible and users only need to upgrade their software. Its pretty much like upgrading operating system of a smart phone, tablet or a smart watch to fix bugs and update security features. Post the soft fork, there will be only one Blockchain unlike Hard fork where Blockchain splits into two. Metropolis in Ethereum is a good example of soft fork

Solidity

It was proposed by Gavin Wood and developed by Christian Reitwiessner, Alex Beregszaszi and several former Ethereum core contributors. Solidity was shaped by C++, Javascript and Python, designed to interact with Ethereum Virtual Machine. In essence, it is the base of the Ethereum Network and enables developers to create their own decentralized applications (dApps). dApps can run smart contracts to accomplish activities like transmitting money, exchanging shares or moving anything of value based on predefined conditions.

Sovrin

Sovrin Foundation, established in the year 2016, is a private-sector, international non-profit that was established to govern the Sovrin Identity Network. The Sovrin Network is a public, permissioned distributed ledger purpose built for protecting identities on internet wherein individuals should own and control their identities without the intervention of administrative authorities, hence known as Self Sovereign Identity (SSI). Sovrin Foundation provides lightweight governance that is needed to operate SSI network in a trustworthy manner.

SPV Client (Simple Payment Verification)

It is a technique that has been first described in Satoshi Nakamoto's paper. It allows a lightweight client to verify that a transaction is included in the Bitcoin blockchain, without downloading entire blockchain. It is often used in Bitcoin wallet apps running on smart phones, by using special SPV nodes that act as an intermediary between the app and a mining node.

SQL (Structured Query Language)

First developed by IBM researchers in 1970s, SQL is a standard language used for storing, querying and retrieving data in databases. It is used for database creation, deletion, fetching and modifying rows.

SSI (Self Sovereign Identity)

SSI is an identity verification and authentication model that is based on the premise that individuals should own and control their identities. It provides security and flexibility to users, empowering them to share their information only when they intend to do so. It is free from interventions exercised by administrative authorities or centralized- or federated-identity providers and acts on the concept that no one owns but everyone has access. It eliminates the need for collecting documents that have already been collected somewhere else. Validators get only that information that users have authorized to share and such information is cryptographically shared on distributed ledger which prevents modification. Evernym and Sovrin are well known companies working on SSI.

Stable Coins

Stable coins are cryptocurrencies whose value is pegged to market value of assets or currencies that reference them. Stable coins may be pegged to a currency like the U.S. dollar or to a commodity's price such as gold. Most popular stable coins are Tether, Diem, USD coin, Dai, PAX. They generally provide pricing stability unlike other cryptocurrencies, hence they are very popular with investors and users who don't like excessive volatility in prices.

Stale Block

These blocks are also known as Orphan blocks which are successfully mined but are not included on the current best block chain. This occurs when blocks are added to the chain that is not the longest one. In Bitcoin blockchain, only the longest chain wins and takes the blockchain network forward.

State

State reflects all committed transactions on the blockchain. This is basically a key-value store which is updated as a result of transactions and chaincode execution. For this purpose, either LevelDB or CouchDB is used.

State Channel

A channel is a private blockchain overlay which allows for data isolation and confidentiality. Using state channels, users transact with each other directly outside the Blockchain network as they go off the chain. They help in increasing the throughput of Public blockchains as they reduce the load for nodes while processing and storing transactions. They are also expected to reduce the cost of using Ethereum network as users pay transaction fees (also known as gas) only while opening and closing channels and not for the entire transaction.

Static Nodes

They represent set of trusted nodes that are pre-configured. In Hyperledger Besu, static nodes are exempt from certain limitations like maximum peer and remote connection limits. Static nodes are also used as an alternate method to find peers.

Stellar

Stellar is Distributed Ledger Technology (DLT) powered Payments protocol. Stellar makes it possible to create, send and trade digital representations of all forms of money—dollars, pesos, bitcoin and other currencies It's designed in a way that all of world's financial systems can work together on a single network. Lumen is the native currency of Stellar, 100 billion Lumens were created during inception of Stellar Network.

Steward

Used in Sovrin Network that promotes usage of Self Sovereign Identity (SSI) on internet. Sovrin Stewards are organizations that operate the network by running validator nodes which write to and read the Sovrin ledger. These trusted volunteers donate time, resources, and computing power to operate and maintain the network while agreeing to abide by the requirements of the Sovrin Governance Framework. There are currently 50 Stewards from 13 countries over 6 continents.

Suicide contract

Suicidal contract is a contract with a security fallback option of getting killed by its owner or through a trusted address. This is generally used in emergency situations such as when funds are being siphoned either due to attacks on wallet or account or due to incorrect functioning.

Swarm

Swarm is a distributed storage platform and content distribution service, built on Ethereum Blockchain with native token called as BZZ. Swarm users upload data to the network and such data is split into small chunks. Incentives make sure that node operators will be rewarded for discovery, storage and propagation of chunks. Swarm Accounting Protocol (SWAP) ensures that node operators collaborate in routing messages. ZetaSeek (user specific search engine), Upala (unique identity for dApps), Waggle (spam free, decentralized email service) and Swarmify (decentralized music streaming) are projects that are being built on Swarm.

Syncing

Syncing in blockchain represents synchronizing with the mainnet. When a new node is launched, it needs to sync with the current blockchain right from the genesis block. New nodes need to catch up and come to speed with the network before contributing to the network or validating transactions. Syncing may take lot of time depending on the protocol and node type. To speed up syncing of node with Blockchain, imaging technologies are being used.

Synthetic Derivatives

These represent securities that are reverse engineered to obtain cash flows from a single security. They are engineered to simulate derivatives while changing important attributes like cash flow and duration. There is a Blockchain protocol called Synthetix that enables synthetic assets issuance on Ethereum Blockchain. They are usually in the form of ERC 20 smart contracts called Synths that provide returns on assets without owning assets. Synths can be traded based on cryptocurrencies, indexes or real-world assets like precious metals.

Security Tokens

They represent ownership in assets or company and provide token holders a share of returns on the asset or profits in the company. In essence, they are tradable financial assets. They are different from utility tokens; utility tokens are used in the ecosystem like Bitcoin, Litecoin and Ethereum. Security tokens on other hand, provide ownership of the ecosystem. Offerings which involve sales of security tokens to raise funds are known as Security Token Offerings (STOs). Sapien Equity Token, Robinhood Casino and Solarstake are examples of STOs

Slippage

Slippage is the price difference between the expected price of a crypto trade and the actual price at which the crypto is traded. This occurs on account of price movement between the time trade order enters the market and the time it is actually executed. The best way to prevent slippage is through the use of price limit orders instead of placing market orders. Limit orders set maximum buy limit or minimum sell limits for the orders and will not be executed till the conditions are met.

CHAPTER 20

T

Terra

Terra is a Blockchain platform containing many stable coins that are pegged to different fiat currencies. Collateral for stable coins is provided by Luna coin. It supports Oracle system and smart contracts with a plan for mass user adoption. Luna and Terra are traded on Binance, Huobi and other exchanges.

Test Net

A second blockchain network other than live network, used by developers for testing new versions of client software without putting a real value at risk. Bitcoin has testnets like Bitcoin Testnet, Ethereum has Ropsten, Kovan, Rinkeby and Hyperledger has Umbra.

Testnet Kovan

Kovan refers to an Ethereum Testnet that supports parity clients and uses Proof of Authority (PoA) consensus. It is the first PoA testnet issued by Ethcore after Ropsten attacks.

Testnet Rinkeby

It refers to an Ethereum Testnet that supports Geth clients and uses Proof of Authority consensus.

Testnet Ropsten

It refers to an Ethereum Testnet that supports both tGeth and Parity clients and uses Proof of Authority consensus. It is mostly similar to mainnet. Refer Ropsten in Section R for additional details.

Tether

Tether is a controversial stablecoin cryptocurrency with tokens issued by Tether Limited. It formerly falsely claimed that each token was backed by one United States dollar, but on 14 March 2019 changed the backing to include loans to affiliate companies.

Theta

The Theta blockchain is the only end-to-end infrastructure for decentralized video streaming and delivery that provides both technical and economic solutions. It is based on Multi BFT Consensus, Signature Gossip scheme and supports Micropayments. Investors include Sony, Samsung and others.

Timothy May

Timothy C. May, better known as Tim May was an American technical, political writer, electronic engineer and senior scientist at Intel. He coined the term Cryptoanarchy where government is not only redundant but also irrelevant. His cryptoanarchy movement has led to the emergence of Cypherpunks such as David Chaum, Wei Dai and others who programmed cryptocurrencies and eventually laid foundation for birth of decentralized cryptocurrencies like Bitcoin and Blockchain.

To the Moon

"To the Moon" is an exclamation used when cryptocurrency prices are rising off the charts. By the same token, when a coin's price is "mooning," that means that the price has hit a peak. Related information: Bitmex a crypto exchange has partnered with Astrobotic a space robotic company to place Bitcoin on the moon through a lunar mission.

Token

A token is the digital representation of an asset built over existing blockchain. They are designed for uniqueness, instant transferability, liquidity, digital scarcity, and security. There are over 10,000 different types of tokens traded in over 380 exchanges globally.

TPS (Transaction per second)

An input or addition into a blockchain network that can make some changes in the existing blockchain data is known as a transaction. Number of such transactions that can be accommodated per second is TPS which determines the speed of Blockchain. Bitcoin has TPS of 7, Ethereum has 25, Litecoin has 56, Cardano has 250, ICON has 9000.

Transaction Block

Transaction block refers to a collection of transactions on the blockchain that can be hashed and submitted to the blockchain. They are like digital files to store and record transactions.

Transaction Fees

The work of validating transactions and adding them to the Blockchain is performed by miners or validators. Miners use powerful computers to confirm the transactions as well as maintain Blockchain network. For doing this, they are rewarded with fees called as transaction fees for every transaction that is confirmed and included in the block. These transactions fees are over and above the block reward they get for adding every block to the Blockchain network. Usually miners, prioritize validation of transactions that carry higher fees.

Trilemma

Refers to scalability dilemma that crypto projects must address while designing underlying architecture and optimizing it. They pertain to scalability aspects like speed and volume of transactions, distribution of network nodes & preventing integrity of network from compromise.

Troll Box

It is a Social Application created for cryptocurrency enthusiasts to easily communicate. Exists on exchanges like BTC-E and Poloniex. Trolls on Troll Box help in providing censor free, relevant, accurate and timely news to help members make better trading decisions.

Trustless

The Internet created a global infrastructure for cheap and flexible communication and depends on a recognized authority or intermediary to promote trust. A global information system that has the properties of Internet and also the functionality to provide authentic statements without a trusted intermediary is required and such a system is called trustless. Blockchain enables trustless computing.

Turing Test

Devised by Alan Turing in 1950, originally referred to as an imitation game, evaluates a machine's ability to exhibit intelligence and behavior equal to humans. A machine will be involved in conversation with humans and evaluator and if evaluator is not able to differentiate machine from humans, machine is said to have passed the test. Test results are based on how close the machine will provide answers compared to that of humans and not necessarily correct answers.

Turing Completeness

A machine is considered to be Turing complete if it can perform any calculation that any other programmable computer is capable of. All modern computers are Turing-complete in this sense. The Ethereum Virtual Machine (EVM) which runs on the Ethereum blockchain is Turing complete. Thus, it can process any "computable function". It is, in short, able to do what you could do with any conventional computer and programming language.

Tokenization

Tokenization is a process that allows the translation of business goods, strategies, or services into discrete units that are tradable and can be recorded on a blockchain. They help in increasing the liquidity of underlying assets and promotes unlocking of value.

Tokenomics

Supply and demand characteristics of cryptocurrencies represent Tokenomics. It is based on the idea of token economy proposed first by Harvard psychologist BF Skinner in 1972. He believed it could control behavior and incentivize positive actions by giving some unit of recognizable value. It also studies how cryptocurrencies work in the broader ecosystem covering token distribution and how incentives foster positive behavior in the network.

Tendermint

A Blockchain application and leading Byzantine Fault Tolerance (BFT) engine for building blockchains, particularly the Cosmos Ecosystem. Supports Tendermint Core and Gaia. Tendermint core provides web server, database and supporting libraries for all blockchain applications regardless of their programming language.

Tezos

Tezos is an open source Blockchain network based on Proof of Stake, that facilitates peer-to-peer transactions and smart contracts with TEZ as native currency. Tezos smart contracts use formal verification, allowing them to be mathematically verifiable.

Truffle

TVL (Total value locked)

TVL in the DeFi world means the amount of money that a single Decentralized Exchange (DEX), Decentralized App (dApp) or the entire ecosystem is holding inside it. Curve Finance, Uniswap, Sushiswap, Bancor and Balancer are some of the leading DEXs based on their respective TVL.

CHAPTER 21

U

Ubuntu

Ubuntu is a Linux distribution created on October, 2004 by Mark Shuttleworth. It is based on Debian and composed mostly of free and open-source software to address fragmentations that existed in Linux with various unsupported community editions. It is compatible with many of Ethereum's development tools. Ubuntu is a complete Linux operating system, freely available with both community and professional support. In fact, it is known as world's first free software and also the first operating system that had scheduled releases in predictable intervals and cadence. Ubuntu Desktop is also the world's most widely used Linux workstation platform. Ubuntu Server is the reference operating system for the Openstack project and popular OS on AWS, Google and Azure.

Uncle Blocks

Uncle blocks are similar to Bitcoin Orphan blocks; they are created in Ethereum blockchains when two blocks are mined and submitted to the ledger at roughly the same time. Only one can enter the ledger as a block, and the other cannot as it has relatively lower share of proof of work. Miners are rewarded for uncle blocks in the Ethereum system unlike for orphan blocks in Bitcoin.

Uniswap

Uniswap is the most popular Ethereum based DEX and a decentralized finance protocol that is used to exchange cryptocurrencies. The protocol facilitates automated transactions between cryptocurrency tokens on the Ethereum blockchain through the use of smart contracts and Automated Market Maker (AMM) model. Developed by Hayden Adams in 201using Solidity.

Unlinkability

It helps in providing anonymity in Public Blockchains. In Bitcoin, unlikability occurs when it becomes difficult to link multiple addresses and transactions belonging to the same user.

USD Coin

USD Coin (USDC) is a digital stable coin that is pegged to the United States dollar and runs on Ethereum, Stellar and Algorand blockchains. Each USDC is backed by a dollar held in reserve. USD Coin is managed by a consortium called Centre. It is founded by Circle, a company that helps internet businesses accept payments and make payments in one unified platform

UTXO (Unspent Transaction Output)

A UTXO defines an output of a blockchain transaction that has not been spent, i.e. can be used as an input in a new transaction. In other words, it can be defined as the amount of digital currency remaining after a cryptocurrency transaction is executed. It helps in preventing double spending in a simple manner without the need for scanning entire Blockchain. Bitcoin uses the UTXO model to prevent double counting and spending. UTXO is based on Hal Finney's reusable Proofs of Work proposal, that in turn was based on Adam Back's Hashcash proposal.

UBIN (Project UBIN)

Project Ubin is a collaborative project with the industry to explore the use of Blockchain and Distributed Ledger Technology (DLT) for clearing and settlement of payments and securities. This project aims to help MAS (Monetary Authority of Singapore) and the industry to better understand DLT and potential benefits it may bring through practical experimentation and broad ecosystem collaboration in Tokenised Singapore Dollar, Rewiring Real Time Gross Settlement (RTGS) based money transfers, Delivery vs Payment (DvP) and Cross Border Payments.

Ursa

Hyperledger Ursa is a shared cryptographic library that prevents the replication of cryptographic work, thereby increasing the overall security of the Blockchain network. The two primary components of Ursa are the Base-Crypto library and Z-Mix. Its library serves as a repository for both Hyperledger and Non Hyperledger projects to use crypto.

CHAPTER 22

V

Validator

A Validator is the one who verifies all incoming transactions on a Blockchain and signs such verified transactions with their Private keys.

Vaporware

It is a product, typically computer hardware or software, that is announced early to general public but its launch is either delayed or never manufactured or officially cancelled. In Blockchain, it refers to a cryptocurrency project that has never become a reality or launched on account of no proper use case or technology to support promises or claims of the project. Tron and Verge, during their initial days, were considered as Vaporware in crypto world.

VeChainThor

The VeChainThor is a Public Blockchain, conceptualized in 2015 by Sunny Lu and launched in 2016. It is designed for mass adoption of blockchain technology by enterprise users for enhancing Supply Chain visibility, carbon credits and anti-counterfeiting services. It offers digitally verifiable provenance to Supply Chains. It hosts VeChain ecosystem that uses physical tracking devices to track every stage in Supply chain. Powered by VeChain (VET) token and VeThor tokens (VTHO), VET is used for storage and transfer of value and VTHO is used as an energy token (gas) to pay for transactions on the network.

VIPER (Viper Protocol)

Viper Protocol is a cross-chain and multi-product DeFi (Decentralized Finance) protocol based on Harmony Blockchain. VIPER is the native governance and revenue generating token that is used for Governance of Viper Exchange/DEX and all DeFi products operating on Harmony blockchain. It is also compatible with Binance Smart Chain, Fantom and others.

VMAC (vMessage Authentication Code)

VMAC is a block cipher-based message authentication code (MAC) algorithm that uses a universal hash proposed by Ted Krovetz and Wei Dai in April 2007. The algorithm was designed for high performance on 64 bit systems, backed by a formal analysis.

Vyper

Vyper is a contract-oriented, pythonic programming language used to write smart contracts. It was created by Vitalik Buterin and Gavin Wood. It has less features than Solidity but makes contracts more secure and easier to audit. It succeeded Serpent that was originally developed for Ethereum.

Vitalik Buterin

Vitalik Buterin is the Co-founder and creator of Ethereum. He was initiated into the world of Cryptocurrencies as Co-Founder of Bitcoin Magazine in 2011. He launched Ethereum with Gavin Wood in 2014. He is also known for his philanthropy and donated over USD 1.5 billion worth of cryptos to various institutions and foundations.

CHAPTER 23

W

W3C (World Wide Web Consortium)

Founded in 1994 and led by Tim Berners Lee, who invented World Wide Web, W3C is working on developing standards for World Wide Web. These Open Standards are accessible to all so that Web can function as One Web and drive innovation for Humanity. W3C works on design principles that promote 1. Web for All (benefits available to all regardless of hardware, software, native language, physical or mental ability) and 2. Web on Everything (Web being accessed by mobile phones, smart phones, kiosks, interactive voice response systems and others).

Wallet

A wallet is an app that allows cryptocurrency users to store and retrieve their digital assets. The five main types of cryptocurrency wallets include mobile, desktop, paper, hardware, online and mobile wallets.

Web3.js

It refers to collection of libraries that allow users to interact with local or remote Ethereum node using HTTP, WebSocket protocols or JSON Remote Procedure Call (RPC). Created by Ethereum Foundation, it facilitates retrieving user accounts, sending transactions and interacting with smart contracts.

Web of Trust

A web of trust is a concept used in PGP (Pretty Good Privacy). Initially a concept created by Phil Zimmerman, GnuPG (GNU Privacy Guard), and other OpenPGP-compatible systems to establish the authenticity of binding between a public key and its owner. It uses trust model in a decentralized way and is positioned as good alternative to centralized trust model of Public Key Infrastructure (PKI) that is dependent on Central Authority.

Web3

Web3 can be mentioned as a revolution of Internet Backend while Web2 was a front-end revolution. It is a set of protocols led by blockchain, that intends to reinvent how Internet is wired in the backend, combining the logic of Internet with the logic of the computer. It empowers users to control their data and also create a native settlement layer. It brings in a right to forget and delete on the Internet.

Wei Dai

Wei Dai is a computer engineer and famous cypherpunk known for contributions to cryptography and cryptocurrencies. He was a programmer at Terra Sciences and part of Cryptocurrency Research Group at Microsoft. He developed the Crypto++ cryptographic library, created the b-money cryptocurrency system, and co-proposed the VMAC message authentication algorithm. He also contributed to SSH2 vulnerability discovery by identifying loopholes in Encryption Block Chaining.

Wei

Wei is the smallest denomination of ether, the cryptocurrency coin used on the Ethereum network. One wei is one quintillionth of an ether. Wei is named after the Computer Engineer Wei Dai who is known for his contributions to the world of Cryptography and Cryptocurrencies.

Whale

Whale refers to individuals or entities that hold large amounts of bitcoin. With their large cryptocurrency holdings, they have the potential to manipulate currency prices and valuations. Barry Silbert, Tim Draper, Michael Novogratz, Tyler & Cameron Winklevoss are some well-known Bitcoin whales

When Lambo

It's a slang that is used to represent a crytpocurrency's success. When a new crypto-coin or token is launched, this question 'When Lambo' is asked to denote the time at which the coin's price will be worthy enough to buy the car Lamborghini.

Whisper

Whisper is a part of the Ethereum P2P protocol suite that allows for messaging between users via the same network that the blockchain runs on. It is a pure identity-based messaging system which provides a simple low-level API without being based upon or influenced by the low-level hardware attributes and characteristics.

World State

World State is a key-value store which is updated as a result of transactions and chaincode execution. It is a component of Hyperledger Fabric Ledger. It represents the latest values for all keys included in the chain transaction log. The world state will change every time the value of a key changes.

Wrapped Bitcoin

Wrapped Bitcoin (WBTC) is an ERC-20 token that represents Bitcoin (BTC) on Ethereum blockchain. Integration into the world of Ethereum wallets, dapps, and smart contracts is facilitated by WBTC. In essence, Wrapped Bitcoin allows Bitcoin holders to tokenize their coins on Ethereum and they are matched by equal number of WBTC tokens.

Wrapped Coins

They represent tokenized version of other cryptocurrencies and address limitations pertaining to interoperability between two different Blockchains. Wrapped coins exist on Blockchains that were not used to issue them initially. Eg: Wrapped Bitcoin and Wrapped Ether. Wrapped coins help in increasing liquidity of centralized and decentralized exchanges.

WASM (Web Assembly)

Web Assembly is a binary instruction format for a stack-based virtual machine. Wasm is designed as a portable compilation target for programming languages, enabling deployment on the web for client and server applications.

CHAPTER 24

X

XRP

XRP is a digital asset built for payments by Jed McCaleb, Arthur Britto and David Schwartz. It is the native digital asset on the XRP (Ripple) Ledger. Ripple began selling XRP in 2012. Its intent was to allow financial institutions to transfer money with negligible fees and wait time. Always positioned as a replacement for SWIFT by removing the settlement layer between major financial institutions.

CHAPTER 25

Y

YAC (Yet Another Consensus)

It's a novel and viable Practical Byzantine Fault Tolerant consensus algorithm based on modular architecture and simple implementation basis called Yet Another Consensus. It has been implemented in Hyperledger Iroha Blockchain platform and has helped in achieving low latency and a very high transaction throughput for transactions.

YAML (Yet Another Markup Language)

YAML, first proposed by Clark Evans in 2001, is a Markup and Data serialization language that came into existence in 2001. YAML is an alternative to JSON that formats data in a natural, easy to read and concise manner. Its not a programming language in the true sense. YAML files store information anddoesn't include actions and decisions. It was released in an era that had proliferation of various mark-up languages like HTML, XML and SGML. Later, YAML was recoined as YAML Aint Markup Language.

Yield Farming

Any effort to deploy crypto assets to generate maximum returns through them is called Yield Farming. It opens up new price arbitrages and also involves lending crypto assets or holdings through DeFi protocols to earn fixed or variable returns.

YFI (Yearn Finance)

It is a gateway to a range of yield generating products in the Ethereum ecosystem. It interfaces with all of DeFi investment avenues like lending aggregation, yield generation and insurance. Ithas a native coin called as YFI coin.

CHAPTER 26

Z

ZCash

Zcash is the first crypto currency in the world to use Zero Knowledge Proof (ZKP) through zk SNARKS and provide enhanced privacy to its users. It doesn't make every transaction detail public, which is the case with most of other cryptocurrencies. Zcash is based on Bitcoin's codebase. In 2013, Matthew Green, Ian Miers and Christina Garman from Johns Hopkins University came up with Zerocoin, a proposed privacy extension to Bitcoin. Alessandro Chiesa, Eli Ben Sasson, Eram Tromer & Madars Virza joined the founding team later. The Zero Coin Electronic Company was formed in 2015 to work on and deliver proposed privacy extensions. Zcash Foundation was launched in 2017. ZCash shares many similarities with Bitcoin such as a fixed total supply of 21 million units.

Zeppelin

Founded in 2015 by Demian Brener and Manuel Aaroz, Zeppelin is a new smart contract development framework through Open Zeppelin for the Ethereum Virtual Machine (EVM) that is focused on security, modularity, and code reusability.

Zero Confirmation Transaction

Zero confirmation transaction is a transaction which occurs but is not yet confirmed by the miners. This means the transaction that has not yet been recorded and verified on the blockchain. The first confirmation comes when a block records the data.

ZK Snark (Zero-knowledge succinct non-interactive argument of

A zk-SNARK is a cryptographic proof that allows one party to prove it possesses certain information without revealing that information. It was introduced by Bitansky et al. This proof is made possible using a secret key created before the transaction takes place. “Succinct” zero-knowledge proofs can be verified within a few milliseconds, with a proof length of only a few hundred bytes even for programs that are very large. Zcash is the first cryptocurrency in the world to use ZK Snark to encrypt the transactions. Till 2021, 82 cryptocurrencies have adopted Zero Knowledge Proof or other private technology to encrypt transactions.

ZK-STARK (Zero-knowledge Scalable Transparent Argument of Knowledge)

Created by Eli Ben Sasson, these are quantum proof unlike ZK-SNARK. They are more scalable in terms of compute speed and

size and do not need an initial trusted set up as they use collision resistant hash functions.

ZKP (Zero knowledge proof in cryptography)

Zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information. In simple terms, it helps in maintaining privacy in a data-based world.

A zero-knowledge proof must satisfy three properties:

Completeness: A honest prover will always be able to prove correctness of a true statement.

Soundness: A cheater can never prove a false statement to be correct to an honest verifier.

Zero-knowledge: If the statement is true, no verifier learns anything other than the fact that the statement is true. For example, a citizen above the age of 18 and wanting to prove this fact to a verifier, will be able to prove the truth about his/her age without revealing his actual date of birth or the actual age.

Fundamentals of ZKP are explained through the well-known tale – The Ali Baba Cave and ZKP written by Jean Jacques Quisquater in his paper titled - “How to Explain Zero-Knowledge Protocols to Your Children”

CHAPTER 27

Others

51% attacks

A 51% attack refers to an attack on a Proof-of-Work (PoW) blockchain where an attacker or a group of attackers gain control of 51% or more of the computing power or hash rate. Attackers use 51% attacks to reverse transactions that have already taken place in a blockchain, in what has come to be known as double spend. Krypton and Shift Blockchains that are based on Ethereum, have suffered 51% attacks.

$Whale

$WHALE is a social currency launched in May, 2020 as ERC 20 token. It is backed by tangible and rare NFT assets, while promoting scarcity through limited issuance and driving values thereby. It has a maximum supply of 10 million coins. It value proposition is based on 1. The Vault, 2. Strong Brand, 3. Community, 4. Tokenomics, 5. Leadership and 6. Vault storing digital art and collectibles

Index

SYMBOLS

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z