**Block Chain**

1. Blockchain works on the many principles such as **proof of work, proof of stake** etc.
2. Working of Bitcoin
   1. You open your preferred wallet app.
   2. You create a new message specifying the amount of bitcoin you want to send, as well as the recipient’s address.
   3. You use your private key to “sign” the message.
   4. After double-checking the message contents, you broadcast the message to the network of computers running the full bitcoin blockchain.
   5. The network verifies that your message represents a valid transaction (specifically, that you have the amount of bitcoin you want to spend, and that it was actually you who authorized the transaction).
   6. Miners race to record new transactions into a block and solve the associated proof of work problem (specifically, to find a nonce that produces a block hash with the correct number of leading zeros).
   7. A miner who finds a solution shares its proof of work with the other miners in the network. The other miners accept the block by beginning to work on the next block (which has to include the hash of the newly made block).
   8. The winning miner receives a set quantity of new bitcoins as a reward.
   9. After ~10 minutes, you and the seller each receive confirmation that the transaction went through. You receive your goods/services from the seller. Done deal!
3. 7 underlying design principles of blockchain and the problem they solve currently prevalent in the society.
   1. Networked Integrity: Erosion of trust in institutions by using **consensus mechanism**. This mechanism works using **proof of stake** & **proof of activity**.
   2. Distributed Power: Centralization of power is present. Blockchain using **peer to peer** technology could help restore equality.
   3. Value as incentive: Block Chin aligns the incentives of every participant using it.
   4. Security
   5. Privacy
   6. Rights Preserved: For any intellectual property, the artist is provided an immutable **time stamped**  proof of existence, authorship and copyright ownership. Using **Smart Contracts,** the payment to artist could take place without any intermediaries.
   7. Inclusion: Help all those who don’t have a bank account include in the economy. No proof of identity required , no min. A/C balance required, lowering barriers to investing
4. Businesses are free to use two types of blockchain
   1. Public: Un-Permissioned
   2. Private: Permissioned
5. However some privacy is required for a business to operate and carry out its functions so
6. A public blockchain is private in the sense that one’s address is pseudonymous.
7. It is also transparent because the holdings and transactions associated with each address are visible to anyone via a **distributed ledger**.
8. Properties of Distributed ledgers of blockchain
   1. Recording transaction and ensuring consensus is the key feature
   2. **Append Only** protocol i.e. allowing no changes to existing records
   3. No third part required as the process is transparent as a whole.
9. Features of distributed database
   1. There is no single point of failure
   2. All data are available locally
   3. System can be set up so different locations do not need to trust one another
10. However the drawback of this system is that participants of other network can see some of your data.
11. There are two types of distributed ledger: Public and Private
    1. Public ledger is permissionless: Anyone can become a network, node or a participant and anyone can enter record in ledgers E.g. Ethereum and Bitcoin
    2. Private ledger is built either by an individual enterprise or by a consortium of organizations. It requires permission to access info. useful for financial institutions. Don’t need a trustless protocol.
12. Blockchain as a strategic risk
    1. In trading markets, because transparency increases the risk of firms’ imitating each other’s trading strategies.
    2. Companies moving out of public equity markets, as a lot of information have to be disclosed.
    3. In voting, as a voter requires its privacy to take an unbiased decision.
13. Blockchain as a strategic asset helps business entities both directly and indirectly.
    1. Creating true value under scrutiny
    2. Understanding customer and building relationship capital.
    3. Protecting consumers privacy
    4. Acting with integrity
    5. Being candid with shortcoming.
    6. It can deal with government corruption
    7. Land Ownership contracts
    8. Corporate income statements which are manipulated
    9. Options grants which are backdated
14. To ensure privacy, users can use either procedural like **Multiple ID’s** or technological solutions.
15. For multiple ID’s one can use HD Wallet. **HD Wallets (Hierarchical Deterministic Wallet)** conceals one’s identity by algorithmically generating a new public/private key pair for each transaction, derived from a single master seed phrase.
16. For privacy conscious users the main challenge they face is of providing cryptographic proof of ownership but without revealing too much info. to the network.
17. To tackle this challenge **zero knowledge proofs** are used. E.g. different colours snooker balls shown to a colour blind person. Z-cash is an example of these zero knowledge proofs.
18. Linkable ring signature is also a tool for guaranteeing privacy. **Monero** is an e.g. of crypto currency using this alternate.
19. Blockchain stakeholders
    1. Industry Pioneers
    2. Venture Capitalist
    3. Banks and Financial Services
    4. Developers
    5. Academia
    6. Leadership
    7. Users
    8. Government
    9. NGO’s
20. Blockchain Governance(Stewardship) is done at 3 levels
    1. Platform Level: Self Governance
    2. Application level: Various Blockchain consortium come together
    3. Ecosystem Level: Advocacies, Chambers or even academic institutes like Blockchain Research Institute.
21. Global Solutions Network. Stakeholders can take the following actions in order
    1. Use standard networks
    2. Use networked institutions.
    3. Use advocacy network
    4. Watchdogs networks
    5. Use policy networks
    6. Knowledge Network
    7. Use Delivery Network
22. Showstoppers in this area , are referred to the obstacles Blockchain faces in its implementation. The 10 major showstoppers in today’s times are
    1. The technology is not ready for prime time:
       1. The infrastructure is unevenly distributed
       2. System lacks the transactional capacity for mass usage
       3. Inaccessible to avg. person
       4. Lack of liquidity- miners hoard coins
       5. High latency- takes 10min for transaction
       6. Behavioral changes
       7. Societal change
       8. Lack of legal choices in a world of transaction finality
    2. Energy used to show proof of work is significant and can turn to unsustainable.
       1. The maximum energy consumption is used by miners in hashing
       2. Huge electricity cost processing bitcoin transaction or processing any blockchain.
       3. Research being undertaken to develop consensus mechanisms other than proof of work which requires less electricity
       4. Computer architecture is also a problem
       5. Miners need to upgrade their systems regularly
    3. Government can stifle it or turn it
       1. New legislation can actually harm its development
       2. Chinese Govt. has banned all mining operations
    4. Powerful Incumbents of the old paradigm will usurp it
       1. Corporations have not been good stewardship of public trust
       2. To **fork** a blockchain means to change the protocol or consensus rules of the blockchain. This was done in 2014 when a theft of 8M VeriCoin was carried out on the Mintpal Exchange
       3. A 51% attack is also known as Double Spend attack. A type of this attack by someone will reverse one of their previous transactions and double spend the same amount.
    5. Incentives are inadequate for mass collaboration.
       1. Since the new bitcoins to be mined will be halved after every 4 years 6.25 in 2020, it gives less incentives to the miners to spend their time & CPU’s processing power on bitcoin.
       2. If the price of BTC keeps increasing, then there is some incentive to mine BTC lower in value.
       3. However if price drops, miners step out which will greatly affect Blockchain, as the trust protocol will be compromised and essentially the whole chain will fall.
    6. Blockchain is a job killer
       1. Blockchain could become an amazing platform for radical automation.
    7. Governing Protocols
    8. Distributed Autonomous Agents
       1. Bad actors threaten public safety and compromise network security
    9. Criminals Will Use it
       1. Silk Road- Dark web mkt place for illegal drug
       2. When this mkt place was shut down, BTC price plummeted, crypto currencies became synonymous with crime.
       3. Technology doesn’t have agency
23. A cryptoasset is a digital asset that uses cryptography, peer to peer network, and a public ledger to do 3 things
    1. TO regulate creation of new units
    2. To verify transactions
    3. To secure transactions without any middleman
24. There are 7 cryptoassets available today
    1. Cryptocurrency:
       * 1. Bitcoin is a reserve currency i.e. final settlement can be carried out using Bitcoin.
         2. Newer currencies like ZCash build up on Bitcoin’s principle, but add privacy to the mix.
         3. Metronome, another cryptocurrency, also builds on Bitcoins and Ethereum’s principles but it also allows its users to import and export it across chains
         4. Dash, Monero are also types of cryptocurrency.
25. Examples of Cryptocurrencies

* **Bitcoin** is the big daddy of cryptos and the one that most people are aware of. It was created in 2009 by the still mysterious and pseudonymous Satoshi Nakamoto. There are actually now two types of Bitcoin, the original and Bitcoin Cash which came about as a way of solving the high transaction times on the Bitcoin network.
* **Ethereum**, also known by the name of its token, Ether, is similar in that it uses a blockchain, but was created more with an eye to what are known as “smart contracts,” rather than use by everyday consumers. Smart contracts replace the need for paper contracts between parties to an agreement and remove the need for signing and amending contracts written on paper.
* **Ripple** is aimed at payments made between financial institutions. These payments have until now typically taken days to process and have been expensive, particularly when they involve low-value, high volume payments. The blockchain makes those transactions faster and cheaper.
* **Litecoin** is probably the closest to Bitcoin in that it is designed as a general use currency. Adherents will tell you that it is an improved version, as it allows for a greater volume of transactions and performs them faster.

1. Protocol Tokens
   * 1. Like Ether are connected to a platform like Ethereum
     2. Blockchain platform designed to run DApp (Decentralized Apps)
     3. DApps are powered by smart contract software
     4. Ethereum is the leading platform for ICO’s
     5. Ethereum has work in progress including Caspers’ Proof of Stake consensus mechanism
     6. Platforms like Polkadot and Cosmos aimed to integrate all blockchain into a giant seamless web.

1. Utility Tokens
   * 1. Are a programmable blockchain asset that provides consumers with access to services or resources within a DApp.
     2. Augur is a prediction market designed to harness the wisdom of crowds in order to make markets virtually anything
     3. Auger’s utility token is used to interact with the network or the application
     4. Golem is a decentralized alternative to the centralized clouds like Apple and Amazon. One can think of Golem as providing Amazon services without Amazon
     5. Golem allows its users to pay or get paid on the platform thereby disrupting the cloud platform
     6. Sweetbridge is also a platform which allows its users to claim discounts on goods and services until they have a utility token in their Sweetbridge wallets

1. Security Tokens
   * 1. They are not cryptocurrencies, protocols, or utility tokens, they are digital bearer assets.
     2. Equity tokens, an e.g. of security tokens, is a native digital asset borne on the blockchain and can be traded P2P without any middleman( Custodians, Clearing Houses, Brokers, etc)
     3. Security tokens can help restore trust in cryptoassets.
     4. Security Tokens Offerings (STO)
2. Natural Asset and Commodity token
   * 1. To tokenize physical assets
     2. We can use token backed by gold as a less volatile and a more liquid medium of exchange
     3. Royal Mint partnered with the Chicago Mercantile Exchange to create a digital gold token backed by actual gold in Royal Mint’s vault.
     4. Natural Asset tokens can be an incentive for people to cut their consumption of resources.
     5. Natural Assets are hard mkt. because of lack of standards and because it’s a fragmented audience.
     6. Blockchain could change that by aligning incentives with a common goal, like reducing Carbon emmissions.
     7. CarbonX or Veridium
     8. Not as big mkt. as other tokens. Mostly theoretical. Has potential to become one of the largest cryptoasssts.
     9. One Gram Coin/token (OGC) aslo tokens gold, backed by actual gold in their vaults.
3. Crypto- Collectibles/ Non- Fungible Tokens
   * 1. Cryptokitties are an e.g. of this
     2. Cryptokitties are unique tradable virtual pets
     3. It has processed $52 M in transactions running on Ethereum Network.
     4. There are two types of cryptocollectibles: Virtual and Real Life
     5. Cryptokitties and virtual trading cards are native digital assets without a real life equivalent.
     6. Blockchain connects the creative work to unique and scarce token. Artists using this tech. to share their intellectual assets without diminishing the value is the next big thing
     7. A company called Artley came up with CLIO, an art backed cryptocurrency to register real world works of art.
     8. Dada.nyc is also associated with it
     9. Artwork can get a digital fingerprint through a cryptoasset allowing us to trace, track and verify it.
4. Crypto Fiat Currency and Stable Coins
   * 1. Venezuela announced that its launching its own cryptocurrency called Petro backed by its oil reserves.
     2. However Petro already has 3 strikes against it
        1. There is no evidence that it is backed by oil
        2. There is little tech. info about how it works or the blockchain on which it runs
        3. Its controlled by the same people who tanked its actual govt. backed fiat currency Bolivar
     3. Iran and Russia also announced launch of their own fiat cryptocurrency. These countries have a few similarities
        1. They are authoritarian or deeply undemocratic
        2. They have a lot of oil
        3. They are under economic sanctions
     4. This matters because rogue govt. could use cryptocurrencies to undermine int. laws, treaties, and sanctions. This could further destabilize their already weak economies
     5. But if crypto-fiat currencies are implemented the right way, they can
        1. Make markets more efficient
        2. Improve inclusion, by breaking barriers
        3. Increase transparency
        4. Make central bank’s policy more effective
     6. Bitt , company in Caribbean, is working with region’s financial heads to create digital dollar standard
     7. Stablecoins are emerging as hybrid cryptocurrency.
     8. They try to maintain the same value over time, almost always by pegging themselves to underlying assets, like fiat currency, or gold, or by managing supply through changing supply.
     9. Tether or USDT is the largest stablecoin at present. Other stablecoins include: MakerDao(Dai)

1. In 2015, when the markets were on the verge of a global economic crisis. Augur launched one of the most successful crowd funding campaigns ever.
2. This was the first ever Initial Coin Offering (ICO)
3. The role of ICO is to match investors with entrepreneurs.
4. New crowdfunding platforms are helping new businesses to grow
   1. Oculus Rift
   2. Pebble Watch
5. US JOBS(Jumpstart our Business Startups) allows investors to make direct investments through crowdfunding
6. ICO’s help companies raise funds on the blockchain by issuing tokens and cryptosecurities.
7. Cryptosecurities can represent equity in companies or even bonds.
8. In Oculus, tokens grant market- makers seats on the platform, which allows the token owners get to decide which prediction markets the company will open .
9. ICO’s are paving the way for a new type of Distributed Virtual Exchange.
10. A token sale is like a crowdfunding campaign, except it uses the technology behind Bitcoin to verify transactions.
11. Ethereum funded the way of a whole new blockchain through a crowd sale of its own named ether
12. Many have argued that the term "ICO" is a bit of a misnomer.
13. Kind of assets an "ICO" can represent
    1. Ownership in a company: New companies can raise funds on the blockchain by issuing tokens or crypto-securities. "Security Token Offerings" (STOs) are the offspring of ICOs.
    2. Access to a network: Augur's ICO, for example, granted investors seats on the platform, enabling them to decide which prediction markets the company would open.
    3. Carbon credits: ICOs can represent many different things beyond "coins," including carbon credits.
    4. Art:ICOs can represent many different things beyond "coins," including art.
14. Smart Contracts are one of the most important parts of blockchain revolution. Nick Szabo is the father of smart contracts.
    1. Reduce transaction costs by eliminating the need for intermediaries
    2. Improve security and privacy of the parties involved
    3. Help to enforce terms of agreement.
15. Smart contracts’ software is coded to mimic the logic of an agreement. The point of smart contract is to reduce reliance on litigation.
16. A smart contract, when set in motion on a blockchain, cannot be seized or stopped or redirected to a different blockchain address.
17. No central authority, or third party can revoke it and no one can override the consensus of the blockchain network.
18. We just have to transmit the signed transaction to any of the blockchain network nodes
19. Benefits of smart contracts
    1. Reducing mental transaction costs: Like Uber uses its algorithm to calculate the fare of journey.
    2. Increased Predictability: Everything is mathematical so can be proved
    3. Broad Security:
20. The big example is DAO, an organization set in smart contracts on Ethereum Blockchain. It was supposed to be an autonomous venture capitalist investing in other tokens. It raised $150 Million Dollars in 2016.
21. However, a hacker figured out a weakness or a hole in DAO and drained $50 Million.
22. Effect of smart contracts is quite substantial on 4 phases of deal cycle: Search, Negotiation, Performance, Post performance incentives.
23. Difference between Smart and Traditional Contracts
    1. Traditional contracts take form if human language, interpreted mainly by lawyers. Nick szabo calls them wet code
    2. While smart contracts rules and conditions analyzed by software code.
    3. Performance in S.C are verified by impartial technology. This contract language is called as dry code.
    4. In dry code, each condition increases the complexity and attack surface of the code.
    5. Attack surface refers to the number of points in a software program where an attacker could break in.
24. Smart and traditional contracts are complimentary to one another and both of them are required for strong business relationships.
25. It is very hard and requires a multiple signature authority or multisig for 2 happy parties to reverse the outcome, without traditional legal intervention.
26. Traditional contracts tend to be biased towards their jurisdiction of origin.
27. A smart contracts generally makes no attempt to be legally binding. It just mimics or improves upon the traditional contract
28. Though smart and traditional contracts work best in tandem, there are others available to deal with contract breaches.
29. One is Performance verification Code which detects a failure in execution and will seize the on-chain collateral of whoever breached the contract as payment for damages.
30. If the outcome is unsatisfactory for both parties, they can rewind some of their transactions through multisig.
31. Regtech deals in whether humans are complying with laws and regulations in certain areas. Regtech is only a simulation to how a wet code may be enforced in court.
32. Applications for Smart Contracts:
    1. Retail Payments:
    2. Worry-minimized commerce
    3. Insurance using Parametric Contract: A parametric contractpays out based on measurable data, not on some estimate loss.
    4. Logistics
    5. Algorithmic Management
33. Smart contracts strategies suggested by Nick Szabo
    1. Audit your organization’s business processes for measurable changes
    2. For coordinating activities across borders, consider using public blockchain rather than private one.
    3. Use smart contracts to reduce the need for intermediaries
    4. Hire lawyers who know computer science, and software engineers who know law
    5. Consider converting some or all your employment contracts into independent contractor or business outsourcing contracts.
34. Five problems with identifiers
    1. The need for some overarching identifier
    2. Government identifiers are system-centric, system controlled , and vulnerable to cancellation, forgery, and theft.
    3. All the personal data we create with each identifier is stored in somebody else’s central databases
    4. The identifier – centric system is extremely user unfriendly
    5. Whenever a central database is hacked, we’re left to clean up the mess
35. Identity commons is a model which allows all users to have the right to manage their own identities.
36. This identity commons require 4 qualities
    1. Must be free of any corporate or government or any third party’s control.
    2. Must outlive us users, so we can transfer our assets to heirs
    3. Must enforce their right to be forgotten
    4. Must be inclusive
37. The path to self-sovereign identity has been a long one.
38. Veteran developer Christopher Allen traced its history
    1. Centralized Authority such as ICANN or Internet Corporation for Assigned Names and Numbers
    2. Liberty Alliance Project
    3. Open ID
39. Blockchain users can obtain digital identifiers through a variety of startups like Civic, ShoCard, uPort, Shyft Network
40. Proxy Contract lets us verify a transaction, an action, or a claim. They also help us manage cryptocurrencies and other tokenized assets.
41. Proxy contracts can interact with other smart contracts on the blockchain. They can also link to our off-chain data, and grant others temporary permission to read or write one of our data files.
42. uPort system works for systems such as driverless carsor 3D Printers. It also interacts with virtual entities like IBM’s Watson, and institutions like banks.uPort also has a mobile app for our cryptographic keys, jjust for convenience and security.
43. Controller contract is another type of smart contract. A controller contract separates our cryptographic keys from the proxy contract. It contains a logic for identity recovery
44. Shyft system is a bit different. Shyft is a blockchain based network compliant with know your customer and anti-money laundering regulation in the financial world.
45. Shyft reduces the costs of compliance and it increases data security
46. Many of the startups are collaborating in the Decentralized Identity Fondation, a consortium consisting Hyperledger,R3 , and Sovrin, as well as more established companieslike Accenture Microsoft and IBM.
47. The consortium focuses on three big areas
    1. Identifiers and discovery
    2. Storage and computation of data
    3. Attestation and reputation
48. Fabian Vogelstellaer is the father of the distributed application for ICO
49. In 2017, he issued Ethereum Request for Comment 725 or ERC 725, a standard which secifies an interface for self-sovereign identity.
50. Blockchain Startups like YouBase,-founded by Leonard Kisch, Josh Robinson, and Dr. Eric Topol- can improve medical research.
51. AI + IoT+Blockchain could have a profound impact on healthcare
    1. Improve quality of treatment
    2. Accuracy of diagnosis
    3. Efficiency if Clinical processes
    4. Integrity of data
    5. Help cut medical research costs
    6. Make the system less vulnerable to hackers
52. With these innovations, patients could agree to share their data at a byte level and they can track their behavior at a granular level
53. Whith these two capabilities, patients could generate an unprecedented amount of phonemic data.
54. Phonemic data is the data on our physical and biochemical traits as they change because of our behavior, our work, our food, our choices, and our exercise habits.
55. With this, patients will be able to donate or license their phonemic data to medical science and they can also donate or license their genetic information.
56. Six inefficiencies in financial system today which can be cured using blockchain
    1. Attestation
    2. Cost
    3. Speed
    4. Risk Management
    5. Value Innovation
    6. Open Source/Adaptability
57. The 8 Functions of the financial industry which can be disrupted by Blockchain
    1. Authenticating identity and A/C balances
    2. Moving Value
    3. Storing Value
    4. Lending Value
    5. Exchanging Value
    6. Funding and Investing
    7. Insuring Value and Managing Risk
    8. Accounting and Auditing
58. The four fundamental problems with modern accounting
    1. Greed
    2. Human Error
    3. Fraud
    4. Inability to support new Business Models
59. World wide Ledger is the solution to the problem we’ve identified with double entry book keeping
60. In 2005, Financial Cryptographer Ian Grigg, argued that cryptographically sealed transactions, essentially a shared receipt, was the same as a third entry. Thus Triple Entry System.
61. This world wide ledger have several implications for accounting
    1. It could streamline compliance and reduce risks for banks: Less accounting work and lower costs for banks
    2. Regulator would have real time access
    3. It bakes integrity into the financial system
    4. The audit business is overdue for disruption
62. THe first era of internet brought us several different organizational forms.
    1. Networked Enteprise
    2. Flat Organization
    3. Open Innovation Movement
    4. Business Ecosystem
63. Ronald Coase identified three types of transaction costs.
    1. Cost of Search
    2. Cost of coordination
    3. Contracting Cost
64. Blockchain is used to reduce costs particularly in 4 areas: Search, Contract, Co-ordinate and estb.Trust.
65. A lot of work has been carried out in the field of search on Blockchain
66. Three differences between internet search and blockchain search
    1. User Privacy: Parties will be able to search for information that users have made open
    2. Multidimensionality
    3. Value
67. ConsenSys is developing identity systems where job prospects or contractors will program their personal avatar to disclose relevant information to employers.
68. Oliver Williamson went on to explain that there are two significant coordinating system
    1. Market: A price system for decentralized allocation of resources
    2. Hierarchy: Organizational Principle of traditional firm where some centralized authority allocates resources
69. The internet still has not dropped the agency costs, the cost of making sure everybody inside the firm is acting in the owners interest.
70. Blockchain’s smart contracts and transparency should reduce agency cost at all level if management to a dramatic degree. These changes will make it to get harder to game the system
71. Trust in business means that the party acts with integrity(honesty, consideration, accountability, and transparency)
72. Corporate Boundary Decisions for businesses in the right sense should be to understand your industry, your competitors, and your opportunities for profitable growth.
73. Then use this knowledge as a basis for your business, and competitive strategy.
74. From there blockchain opens all kinds of new opportunities for networking
75. 9 questions to ask before you set your boundary of your business
    1. Are their partners who could do certain activities better?
    2. What are the new economics of corporate boundaries
    3. How much of your business relies on technological interdependence? How much is modular?
    4. How good is your firm at managing outsourced work or networks?
    5. Is there a risk a partner might invade fundamental parts of your business.
    6. Are there legal, regulatory, or political obstacles to change and to networking more?
    7. Will working with partners help you improve your overall competitive advantage?
    8. Is there a danger of losing control of something fundamental?
    9. Can you rapidly expand your market or value proposition while at the same time shutting out a competitor by vertically integrating?
76. Smart contracts can differ from each other on the basis of their complexity.
77. Simple Contracts involve few or no people and only 1 exchange of value
78. Complex Contracts call on more people and involve many exchanges making firms resemble network. These are called Open Network enterprise(ONE)
79. On taking one step further, smart contracts can be regarded as autonomous agents. These could have Machine Learning, AI built into them to pursue our goals and make decisions on our behalf
80. Autonomous agents can modify how they do their work over time.
81. A computer virus is an example of a bad autonomous agent
82. More complex agents could make more complex transactions. They could acquire resources or produce value for their owners
83. In the future autonomous agents will collaborate forming all kinds of new business models i.e. a distributed autonomous agents
84. Distributed Autonomous Agents: A set of autonomous agents corporating in a complex, blockchain based ecosystem
85. Entrepreneurs are writing code in languages like Scrypt and Solidity.
86. Innovators are using code to give multisignature control over funds.
87. A software startup called Slock.it developed a smart contract DAO(Decentralized Autonomous Agent ) on Ethereum
88. In essence, DAO was a decentralized investment fund
89. In essence, the platform would allow anyone with a project to pitch their idea to the community and potentially receive funding from The DAO.
90. Anyone with DAO tokens could vote on plans, and would then receive rewards if the projects turned a profit.
91. An attacker figured out a loop hole in the voting process and essentially stole 3.6M Ether
92. In his exploit, the attacker was able to ask DAO to give Ether back a multiple times before the smart contract could update the balance
93. Two issues which resulted in such an attack was a result of flaws in the code written for DAO
    1. Possibility of a recursive call
    2. The fact that the smart contracts first sent the ETH funds and then updated the internal balance
94. THe Ethereum network had two options to save shareholders funds from being looted
    1. Employ a Soft Fork: Blacklist the DAO network and call it illegal
    2. Hard Fork: To place the funds into a separate account subject to a 28 day holding period so the hacker couldn’t complete his getaway.
95. This hack resulted in de listing of DAO and ultimately it collapsed
96. The story of DAO taught us effective blockchain governance requires both on-chain and off-chain governance mechanisms
97. Blockchain based business models. Distributed models will distrupt centralized ones because they innovate better, provide value at lower cost, and producers can share in the wealth.
98. Examples of Open Networked Enterprises Business Models
    1. Blockchain corporative: Disrupting sharing economy companies like Uber,Lyft,Airbnb
    2. Creators of Intellectual Property: Art industry, Verisart
    3. Peer-Peer Production: Linux, Wikimedia, Reddit
    4. Metering Asset usage: E.g. your wifi renting itself in your absence in exchange for money
    5. Platform Builders
    6. Animating the Physical World
    7. Enterprise Collaborators
99. This Internet of Things depends on a Ledger of Things to track everything, ensure its reliability, and pay for its contribution. There are potential applications across virtually every sector.
    1. Transportation: Autonomous vehicles will get us safely wherever we need to go. They will intuitively take the fastest route, avoid construction, handle tolls, park all on its own, negotiate passing rates with other vehicles on the road, and communicate with traffic lights.
    2. Infrastructure:  We will use smart devices to monitor the integrity and other critical factors of road, rail lines, power and pipelines, bridges, runways, ports, and other public and private infrastructure to detect problems and initiate a response both rapidly and cost-effectively.
    3. Energy, waste, and water management: Traditional utilities can use blockchain-enabled things for tracking production, distribution, consumption, and collection. New entrants without infrastructure are planning to create new markets such as the neighborhood energy microgrid.
    4. Resource extraction and farming: This technology can help make expensive, highly specialized equipment available for just-in-time usage and cost recovery, improve worker safety, and compile “infinite data” analytics to identify new resources or advise on best practices. Sensors could help environmental protection agencies to regulate land usage.
    5. Environmental monitoring:  Weather sensors will make money collecting and selling air, water, and tremor data, giving people advance warnings of natural disasters, rising levels of pollutants, and monitoring lightning strikes and forest fires—all to increase emergency response time, save lives, and improve our predictive capability.
    6. Health care:  Blockchain-enabled hospitals could link the devices that manage medical records, inventory, equipment and pharmaceuticals to monitor and manage disease and improve quality control. Smart drugs could track themselves in clinical trials and present untampered evidence of their effectiveness.
    7. Financial services and insurance: Financial institutions could use smart devices and the IoT to tag, track, and trace their claims on physical assets—like an air traffic control for priceless objects, antiquities, jewelry, the stuff of museums, anything ever handled by Sotheby’s and insured by Lloyd’s.
    8. Smart documents: Like smart contracts, the coding of all documentation related to a particular thing—a patent, deed, warranty, provenance, registration, insurance, and inspection certification—could control the operation of that thing. If a vehicle has failed a safety inspection or its liability insurance has expired, the vehicle will not start.
    9. Real estate management: Digital sensors can create marketplaces for vacant assets by enabling real-time discovery, usability, and payment. In the evenings, a conference room could moonlight as a classroom for neighbourhood youth.
    10. Industrial operations: The global factory of things needs a global ledger of things. Factory managers will use smart devices and offer software services for monitoring customer demand, production lines, warehouse inventory, distribution, quality, maintenance, and performance data.
    11. Household management: Numerous products and services are entering the market to allow automated and remote home monitoring beyond the “nanny cam” to include access controls, temperature adjustments, lighting, and restocking the pantry, the bathroom, and the garage. The smart home will optimize energy and the in-house experience.
    12. Retail: Retailers will be able to personalize products and services to identifiable customers as they walk in or drive by, based on demographics, known interests, purchasing history, and whether those customers gave retailers permission.
100. Using Decentralized Apps or DApps, anyone can upload a program onto the blockchain and leave it to self-execute with a strong guarantee that the program will continue to perform indefinitely.
101. How C-Suite officers can lead Blockchain Revolution in their businesses
102. CEO can lead the transformation using three steps
     1. Acknowledging the market readiness and good financial results
     2. Effective marketing and communication
     3. Avoid setting unrealistic expectation
103. COO will oversee the supply chain revolution. The industries where disruption can happen are:
     1. Manufacturing: Foxconn Group uses blockchain to disrupt businesses that don’t do
     2. Mining: Everledger is working in diamond industry
     3. Agriculture:
     4. Retail: Walmart partnered with IBM and used blockchain
     5. Border Controls and customs: Delays due to movement of goods across borders
     6. Aerospace: Moog
104. Chief Legal Officer(CLO). Lawyers who are implementing smart contracts should keep in mind two things
     1. Stick with Well tested methods
     2. Make sure you have someone on the staff who can audit software code
105. Blockchain is surely on its way of disrupting the financial services with its P2P network, immutability, and distributed ledger.
106. The CFO of the company is definitely going to need to upgrade the way finances are being taken care of in their businesses
107. Traditionally, CFOs have three key roles: execution, enablement and development. EY’s The DNA of the CFO series further explains the CFO perspective. These roles comprise six segments: trusting the numbers, providing insight, getting your house in order, funding organizational strategy, developing business strategy and communicating to the external marketplace.
108. The following practices should be employed.
     1. The Accountants would need to understand Triple Entry Bookkeeping
     2. Real time status of all transaction relevant to us
109. The views regarding the regulation of the internet were similar to current views regarding the regulation of blockchain technology
     1. Pioneers of technology insisted that it couldn’t be regulated because of its openness and its international/global reach.
     2. More mainstream users agreed that the technology should be free from state-based regulation, but there was value in self-regulation.
     3. Those working in the industry have more expertise than most regulators do.
110. The Global blockchain rights should encompass
     1. Unrestricted access to blockchain applications, unless those apps violate the social contract
     2. Balance between your right to distribute and to access information
     3. Balance between your right to privacy and to protect your data
     4. Legitimate need for governments to restrict the flow of information, provided it’s infrequent and the reasons are transparent
     5. Enforcement of contractual rights
111. The Finance Action Task force defined virtual currency as a “Digital representation of value. It can be digitally traded and functions as a medium of exchange and/or a unit of account and/or a store of value
112. The Howey test defines an investment or a security as
     1. An investment of money
     2. In a common enterprise
     3. With an exception of profits
     4. To be derived solely from the efforts of others
113. Firms use regulatory sandbox to test run its deployment across sectors
114. Regulatory sandboxes aren’t always appropriate and should be used carefully. However, when conducted responsibly, they can be a helpful tool for observing how innovators might use highly disruptive and unpredictable technologies
115. Blockchain applications ultimately work on internet applications and protocols
116. Each new layer of the stack inherits the protocols and rules of the layer below, including the lower layers and governance
117. The three main layers are (from top to bottom)
     1. Application Layer
     2. Blockchain Layer
     3. Internet Layer
118. Blockchains like Bitcoins and Ethereum rely on Transmission Control and Internet Protocols (TCP-IP)
119. Net neutrality is the foundation principle of the internet
120. It’s the idea that all traffic on the network should receive equal priority. Information should be transmitted as it is received
121. The application layer is also made up of its own multiple layers. It includes two specific components
     1. DApp Framework: Built on top of blockchain network and provide the basic building blocks for DApps
     2. DApps:
122. Ways to alter the alteration of a DApp
     1. Change the state of the blockchain to overwrite the code of the DApp e.g. Hard fork done on the Ethereum Network after DAO was hacked. These hard forks can change the balance or code of a particular DApp or even delete the DApp entirely
     2. Change a small piece of code upon which the DApp relies (e.g. a smart contract library, or a proxy contact). A proxy contract is a smart contract that delegates calls to other smart contracts.
123. Two distinct governance structures on blockchain are
     1. Governance by infrastructure(On chain governance): Governance rules encoded directly in the blockchain itself
     2. Governance of the infrastructure(Off-chain): All influence forces outside the technological platform
124. These structures can be endogenous or exogenous depending upon the rules and regulations of the community/legislation
125. Endogenous rules: All the rules, social norms, customs and other governance structures developed or endorsed from within that community.
126. Exogenous rules are all other rules influencing the activities of a community but originating from outside the community.
127. Bitcoin Improvement Proposals (BIP’s) is an informal mechanism through which people can propose new features and improve to Bitcoin protocol.
128. Similar to BIP’s , the Ethereum blockchain has Ethereum Improvement protocols, EIPS
129. Once a suggestion is made, developers of the blockchain system will put forward a proposal. Then the voting system determines, whether the community adopts it or not
130. Off-chain governance is difficult is difficult to impose because of its social component
131. Both Off-chain and On-chain governance should coexist to provide stewardship to Blockchain
132. Networks which consist of private networks, civil societies and governments at various levels are called Global Solutions Network(GSN)
133. These networks have two defining characteristics
     1. Composition: Are multi stakeholder
     2. Control: Not controlled by states
134. There are 10 types of these networks out of which the top three are the most important ones.
     1. Knowledge Networks: Develops new theories, ideas and research. In world. In blockchain, the leading knowledge network in academic space are MIT Digital Currency Initiative,Blockchain Research Institute, and Reddit
     2. Policy Networks: Coin Centre, Chamber of Digital Commerce
     3. Standard Networks: Are non- state based organizations.
     4. Delivery Network: ICANN
     5. Advocacy Networks: Electronic Frontier Foundation
     6. Watchdog Networks: Human Rights Watch
     7. Platforms: Ethereum
     8. Networked Institutions: World Economic Forum
     9. Diasporas:
     10. Governance Networks: Combine all the 9 types
135. The seven elements a hub/a blockchain hotbed must have for a blockchain based innovation to thrive
     1. An environment supportive of incubators and entrepreneurship
     2. Community of corporate leadership
     3. Proximity to educational institutions
     4. A strong investment climate
     5. Government Support
     6. Fair Regulatory environment
     7. Diverse community of talent
136. A social contract is a shared idea that our best interest(morality, fair politics, and physical safety) depends on keeping a civil society
137. A new social contract is needed for a digital economy.
138. Drivers for Change
     1. Fourth Industrial Revolution: First use steam power for mechanized production. Second use electricity for mass production. Third use technology for automated production.
     2. Globalization:
     3. Demographic Upheaval
     4. Climate Change
139. Four Pillars of society
     1. State
     2. Private Sector
     3. Civil Society
     4. Individual
140. The private sector has a major role in developing a new social contract for the digital economy
141. This sector is the foundation of wealth creation, and also contributes to wealth distribution
142. Rethinking Work
     1. A guaranteed job backed by a Universal Basic Income(UBI)
     2. A portable net
143. There is a dire need of shift form Wealth redistribution and wealth pre-distribution
144. The Pre-Distribution of Wealth
     1. Providing high speed, broadband, Internet access
     2. Providing ownership of personal information
145. Traditional prosperity model is wealth redistribution through taxing rich and giving it to the poor
146. The new model is Pre-distribution of wealth in the conditions under which everyone can contribute
147. Pre-Distribution f wealth can be achieved by providing
     1. Universal, high speed, broadband Internet access
     2. Personal ownership of personal information
148. Blockchain technology can be used to distribute power
     1. By aligning incentives for participation of all stakeholders
     2. By tracking costs with transparency
     3. By managing stakeholders rights
149. Shared contract is a shared understanding of the roles and relationships of the individuals and institutions in the society
150. Problems Blockchain can solve in its current development
     1. Lack of resilience
     2. Durability
     3. Trust
     4. Privacy
151. Problems, blockchain in its current stage, it cannot solve
     1. Scalability
     2. Latency
     3. Transaction Rates
     4. Regulatory Uncertainty
     5. Interoperability
     6. Energy Consumption
     7. Pace of Change
152. Answer these questions to determine whether blockchain could help solve your use case:
     1. Is there a predictable, repeatable process that lends itself well to automation?
     2. Is there an ongoing or long-running transaction or process, rather than a process that occurs only once?
     3. Are there multiple stakeholders in this process or value chain?
     4. Is the role of reconciling disparate data usually played by one party or a limited number of parties?
     5. Remembering that value is not only monetary, is there an element of value transfer?
     6. Is there value in an immutable record? Or is an immutable record a requirement?
153. If answered yes to these questions, think how you will implement blockchain in the three layers of the blockchain network
154. PROTOCOL LAYER
     1. Is it possible to use public blockchains? Or is there a defined need for a private implementation?
     2. What are the design expectations regarding speed, programmability, or payment functionality?
     3. Do you have developer resources available?
     4. Or is the protocol you’re using supported by a robust, sustainable open-source developer community with access to resources?
155. NETWORK LAYER
     1. Who needs to run a node? Who has read access? Who has write access?
     2. What are the technology integration requirements?
     3. What are the data storage requirements regarding archiving and regulation?
156. APPLICATION LAYER
     1. Who is going to use the application? What are the implications for user experience and design?
     2. What is the existing organisational structure? And what behavioural patterns do users have today? How does this product or service fit into their existing workflow?
     3. Are there any behavioral or organizational changes necessary to implement this use case?