FEEDBACK

- Idea
- Response
- Opinion
- Survey
- Advice
- Comment
- Result
- Rating
Genesis block, coinbase transaction, and block confirmations
Genesis block, coinbase transaction, block confirmations

- **Genesis block**
  - Genesis block is the first block of a blockchain

- **Coinbase transaction**
  - First transaction in new block
  - Create by miner
    - Rewards miner
  - Has no inputs
  - When block successful mined/created then coinbase transaction also created

- **Block confirmations**
  - The blocks mined (or added) after the block where your transactions is included
Blockchain oracles and role within Blockchain-based Applications
Blockchain oracles and role within Blockchain-based Applications

Provide a link between blockchain and off-chain world.

- Blockchain itself does not access data from external source
- Oracles support the access, validation, and transmission of data from external sources to blockchain systems

“Blockchain oracle is an external data agent that observes the real-world events and reports them back to the blockchain to be used by smart contracts” by Al-Breiki et.al.
Blockchain in healthcare domain
Interoperability is a huge problem in the healthcare industry.

- The trouble of identifying patients
- Information blocking

Permissioned healthcare blockchain

- Healthcare institutes don’t own a patient’s personal data
  - The patient can have some control over their medical data
- Patients are identified via their hash ID
- Information sharing between the different institutes to prevent any kind of info blocking
- Anti-tampering
- Single global healthcare database
- Protection against insurance fraud
  - Medicare fraud in the U.S. alone costs about $68 billion a year.
Solidity
Solidity

- Object-oriented programming
  - To write smart contracts
    - Ethereum platform
- Solidity was initially proposed in August 2014 by Gavin Wood
  - Later developed by the Ethereum project Solidity team
- Solidity is compiled to bytecode that is executable on the EVM
- Enable self-enforcing business logic that incorporates in smart contracts
- Remix Ethereum IDE
  - [https://remix.ethereum.org/](https://remix.ethereum.org/)
ABI in solidity smart contracts
ABI in solidity smart contracts

- ABI stands for application binary interface
- JSON format
- Interact with contracts
  - Off-chain
  - On-chain contract-to-contract interaction
- Defines methods and structures used to interact with the binary contract
  - Data is encoded according to its type, as described in this specification
Memory vs calldata in solidity
smart contracts
Memory vs calldata in solidity

- Both keywords that define the data area where a variable is stored
  - Using to declare function parameters
- Memory should be used when declaring variables that you want stored in memory
  - It is mutable
- Calldata must be used when declaring an external function dynamic parameters
  - It is immutable
  - Non-modifiable, non-persistent
Ethereum virtual machine and ByteCode
Ethereum virtual machine and ByteCode

- Computation engine
- Run execution and smart contract deployment
- Ethereum node runs on the EVM to maintain consensus across the blockchain
- Smart contracts written in high-level programming languages
  - EVM can't execute smart contracts directly
  - Smart contracts compiled down to bytecode

For more details:
https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e
Corda and CorDapp
Corda and CorDapp

- Open source blockchain platform
  - Developed by R3 Blockchain company
    - https://www.r3.com/corda-platform/
- An example of permissioned blockchain
- Corda main objective is to manage and synchronises financial agreements
- CorDapp is distributed application that run on the Corda platform
  - https://docs.corda.net/docs/corda-os/4.5/cordapp-overview.html
Silk Road
Silk Road

- Founded in 2011 by Ross William Ulbricht
  - Dread Pirate Roberts
  - Shut down in 2013 by FBI
- Black market
- Darknet market
  - Criminal activities
  - Drugs sales
- Estimated $15 million in transactions were made annually on Silk Road
  - Net worth was $28.5 million
Guardtime blockchain project
Guardtime Blockchain project

- Digital signature system
- Keyless Signatures Infrastructure (KSI)
  - Distributed system for providing time-stamping and server-supported digital signature services
- KSI blockchain based products and services offer
  - Real-time immutable data integrity for electronic data, systems and networks
- Keyless signatures are an alternative solution to traditional PKI signatures
Cryptocurrency and Bitcoin scams
Cryptocurrency/Bitcoin scams

- Fake Bitcoin exchanges
- Ponzi schemes
- Fake cryptocurrencies
- Tax frauds
- Money laundering
- ICO scam
- Bitcoin gold scam
- Pump and dump scam
- Silk road dark web
EstCoin

- Estonian government proposed a cryptocurrency
  - Estonian e-Residency
- Initial coin offerings
- Criticism from banking authorities

“We’re working to make e-Residency the best option globally for entrepreneurs launching a trusted ICO, while proceeding with three variants of our own ‘estcoin’ under consideration.” by Kaspar Korjus
Craig Wright

- Australian computer scientist
- Self-proclaimed Satoshi Nakamoto
- Fraud Satoshi
  - He didn’t prove he is Satoshi
Defi coins and ICOs
Defi coins and ICOs

● Decentralized finance tokens
  ○ Open financial network. If you want to send, lend or borrow money you don't need to join a private network like PayPal or Fedwire or a bank
  ○ Bitcoin, Ethereum and other already existing cryptocurrencies are working in same mechanism
    ■ The word Defi is catchy and created the hype in cryptocurrency world
  ○ Chainlink and Maker are more trading Defi coins

● Initial coin offerings (ICOs)
  ○ Raise funds
    ■ To provide some service, app or as an investment opportunity
  ○ Ethereum based ERC20 tokens
Blockchain in supply chain
Blockchain in supply chain

Organizations can digitize physical assets

- Decentralized immutable record of all transactions
- Track assets from production to delivery
  - Transparency
  - Auditability and quality control
- Increase traceability
  - Ensure corporate standards are met
- Lower losses from counterfeit
- Reduce paperwork and administrative costs
- Strengthen corporate reputation through providing transparency of materials used in products
- Improve credibility and public trust of data shared