Decentralized Applications

Batch - 10

Abhishek Shrestha – 14221A0563

Pramesh Bajracharya – 14221A0566

Saurav Bajracharya – 14221A0567

Sundar Ghimire – 14221A0576

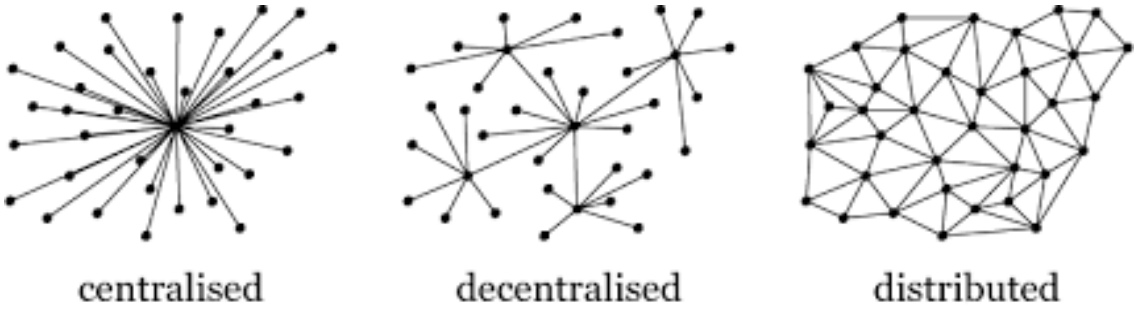
Decentralized applications (dApps) are applications that run on a P2P network of computers rather than a single computer. A new model for building successful and massively scalable applications is emerging. Bitcoin led the way with its open-source, peer-to-peer nature, cryptographically-stored records (block chain), and limited number of tokens that power the use of its features. It also revealed a sneak peek of the future: **a world running on decentralized applications (Dapps)**. Before we can even fathom what Dapps do, we need to be familiar with its underlying technology - the **Blockchain**. A blockchain is a ledger of records organized in 'blocks' that are linked together by cryptographic hash validation. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. It is a digital storage of consensus truth. The key is to understand that this ledger is neither stored in a centralized location nor managed by any single entity, hence its distributed-ness. The block validation system results in new transactions being added irreversibly and old transactions preserved forever for all to see, hence its transparency and resilience.

For an application to be considered a Dapp (pronounced Dee-app) it must meet the following criteria:

1. The application must be completely **open-source,** it must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by consensus of its users.
2. The application's data and records of operation must be cryptographically **stored in a public, decentralized blockchain** in order to avoid any central points of failure.
3. The application must **use a cryptographic token** (ethereum or a token native to its system) which is necessary for access to the application and any contribution of value from (miners / farmers) should be rewarded in the application's tokens.
4. The application must **generate tokens according to a standard cryptographic algorithm acting as a proof** of the value nodes are contributing to the application (Bitcoin uses the Proof of Work Algorithm).

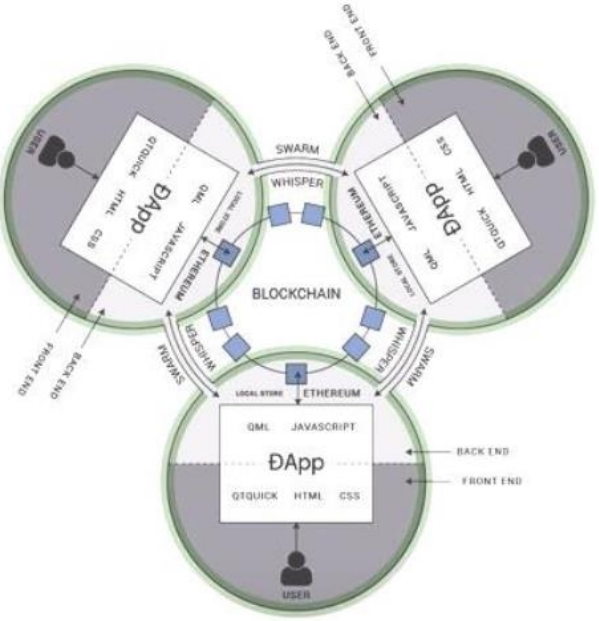
In Ethereum's white paper, it was stated that the intention of Ethereum is to create an alternative protocol for building decentralized applications with emphasis on development time, security, and scaling. The concept of a Dapp is so powerful and elegant, because it does not include these traditional corporate techniques. The ownership of the Dapp's tokens is all that is required for the holder to use the system. It's that simple. The value of the tokens is determined by how much people value the application. All the incentives, all the monetization, all the ways to raise support are built into this beautifully simple structure.

A typical web application consists of server side code and centralized database that clients can access remotely making it a single point of failure and single authority that controls your data. This is an outdated and has many shortcomings. To overcome this problem we can use Decentralization. **In a decentralized network there is no central server** to which the clients connect, and the data is distributed across nodes in the network. By storing data across its network, the blockchain eliminates the risks that comes with data being held centrally. This is where blockchain has its advantage. While centralized data is more controllable, information and data manipulation are common. By decentralizing it, **blockchain makes data transparent** to everyone involved. Its network lacks centralized points of vulnerability likewise, it **has no single point of failure**.



Blockchain security methods include the use of **public-key cryptography**. Every node or miner in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust.

One of the platform that helps us realize Decentralization Applications is **Ethereum**. **Ethereum** is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality. **Ethereum** is considered to be one of the pioneer platforms in distributed ledger and blockchain technology. Contracts in Ethereum are written in a high level programming language called – **Solidity**. A contract in the sense of Solidity is a collection of code (its *functions*) and data (its *state*) that resides at a specific address on the **Ethereum blockchain.**



Decentralized autonomous organizations are one particularly ambitious breed of dapp. The DAO had an objective to provide a new decentralized business model for organizing both commercial and non-profit enterprises. It was instantiated on the Ethereum blockchain, and had no conventional management structure or board of directors. The code of the DAO is open-source. The DAO is stateless, and not tied to any particular nation state.

Dependencies:

- NPM, NodeJS 5.0+ recommended: https://nodejs.org
- Windows, Linux or Mac OS X
- Chrome/Firefox Browser with MetaMask extension: https://metamask.io
- Truffle: https://github.com/trufflesuite/truffle
- ReactJS: https://reactjs.org
- Ganache: http://truffleframework.com/ganache
- TestRPC: https://www.npmjs.com/package/ethereumjs-testrpc

Many uses have been proposed for Ethereum platform, including ones that are impossible or unfeasible. Use case proposals have included finance, the internet-of-things, farm-to-table produce, electricity sourcing and pricing, and sports betting.

Possible applications of dApps are listed below:

- Digital signatures that ensure authenticity and proof of existence of documents.
- Slock.It is developing smart locks.
- Digital tokens pegged to fiat currencies.
- Digital tokens pegged to gold.
- Improved digital rights management for music.
- Platforms for prediction markets.
- Platforms for crowdfunding.
- Social media platforms with economic incentives.
- Decentralized marketplaces.
- Remittance.
- Online gambling.
- Electric car charging management.
- Secure identity systems for the Internet.
- Labour economics.
- Video Games.