Report

In the era of censorship, multiple industries as well as a vast variety of applications are shifting towards peer-to peer network or decentralization unlike the traditional client-server model. Apart from censorship client-server architecture are also expensive requiring frequent maintenance. Also the problem of single-point of failure in the client-server architecture causes delay and sometimes total break down of the system blocking hundreds of clients from accessing and working with data on their applications. Decentralization can overcome all the drawbacks of client-server architecture providing favorable conditions for businesses as well as application development. Decentralization provides increased system reliability, scalability as well as privacy. Eliminating the consequences of single point of failure it also provides greater privacy as the information passes from multiple points[1].

Decentralized applications or dApps refer to applications that run on peer-to-peer network rather than being controlled by single entity. dApps require a distributed platform to run on. The most common platform on which dApps run today is the Blockchain. Blockchain as the name suggests, basically refers to a block of chains linked to each other using cryptography. Each block in a block chain consists of transaction information, timestamp and the hash of the previous block. The main advantage behind using Blockchain is that it is immutable and cannot be tampered maintaining the integrity of the data. The working of Blockchain is as given in the figure below.

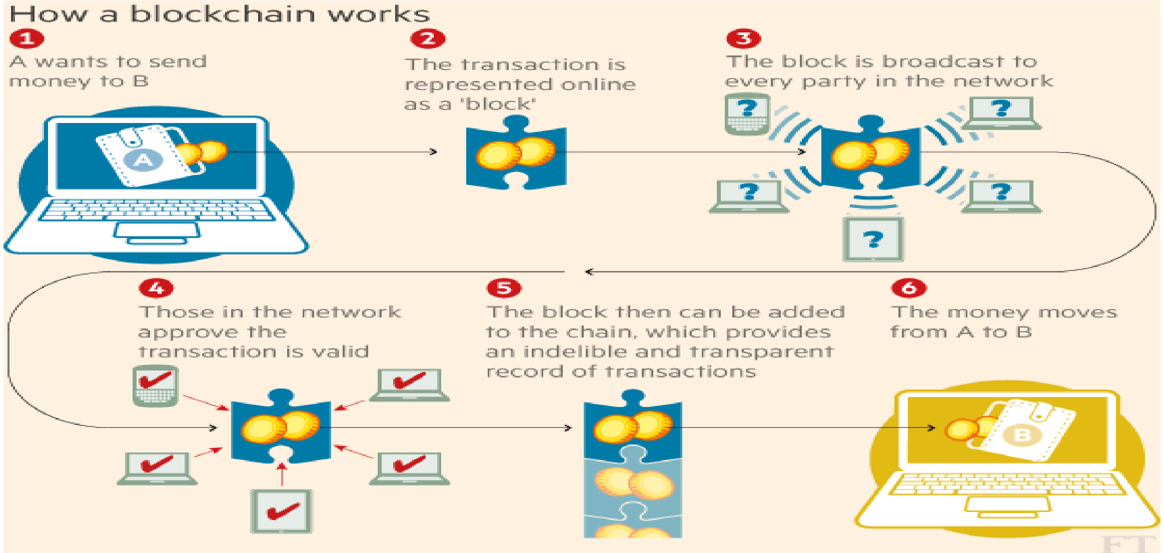
How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Fig 1[2] **Working of Blockchain**

Smart Contracts allows dApps to connect with the Blockchain. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. They render transactions traceable, transparent, and irreversible[3]. dApps to a certain extent are similar to conventional web application. The front end uses the Web technology to render the page while instead of an API connecting to a Database, we have a Smart Contract connecting to a Blockchain[4]. Unlike the traditional application where the backend code used to run on centralized servers, in case of dApps the backend code runs on decentralized Peer-to-Peer network. The frontend code as well as the user interface in case of dApps are independent of the language in which they are written. To host the frontend we would need to have decentralized storage systems such as Swarm or IPFS.Fr an application to be considered dApp, it needs to meet certain criteria as listed below[5]:

1. Application needs to be completely open source.
2. The data and records of the application must be stored cryptographically.
3. A cryptographic token is a must to be used.
4. The application must be able to generate tokens.

In our case we will be using IPFS as a decentralized source. IPFS stands for InterPlanetary file system. InterPlanetary File System (IPFS) is a protocol and network designed to create a content addressable, P2P method of storing and sharing hypermedia in a distributed file system. Similar to a torrent, IPFS allows users to not only receive but host content. 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. IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.

Using IPFS, NuCypher and Keepass we will be developing a decentralized password manager known as “Keepassxc-IPFS” . A password manager is used to store multiple passwords in a single database locked by a password manager eliminating the need to remember multiple passwords. IPFS as discussed above is used to store data on a decentralized network. NuCypher is based on proxy re-encryption network used to empower privacy on decentralized systems. The NuCypher network facilitates end-to-end encrypted data sharing for distributed apps and protocols. Access permissions are baked into the underlying encryption, and access can only be explicitly granted by the data owner via sharing policies. Consequently, the data owner has ultimate control over access to their data. At no point is the data decrypted nor can the underlying private keys be determined by the NuCypher network[7].

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key file. So you only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish)[8].

References

1. https://www.solarwindsmsp.com/blog/centralized-vs-decentralized-network
2. https://images.app.goo.gl/Jj4DtzMVcK3NWTNt5
3. https://www.investopedia.com/terms/s/smart-contracts.asp
4. https://blockchainhub.net/decentralized-applications-dapps/
5. https://nirolution.com/decentralized-applications-explained/
6. https://en.wikipedia.org/wiki/InterPlanetary_File_System
7. https://github.com/nucypher/nucypher
8. https://keepass.info/