DRAFT II (Report)

Decentralized Applications

Introduction

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].

Technological Background

Blockchain

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.

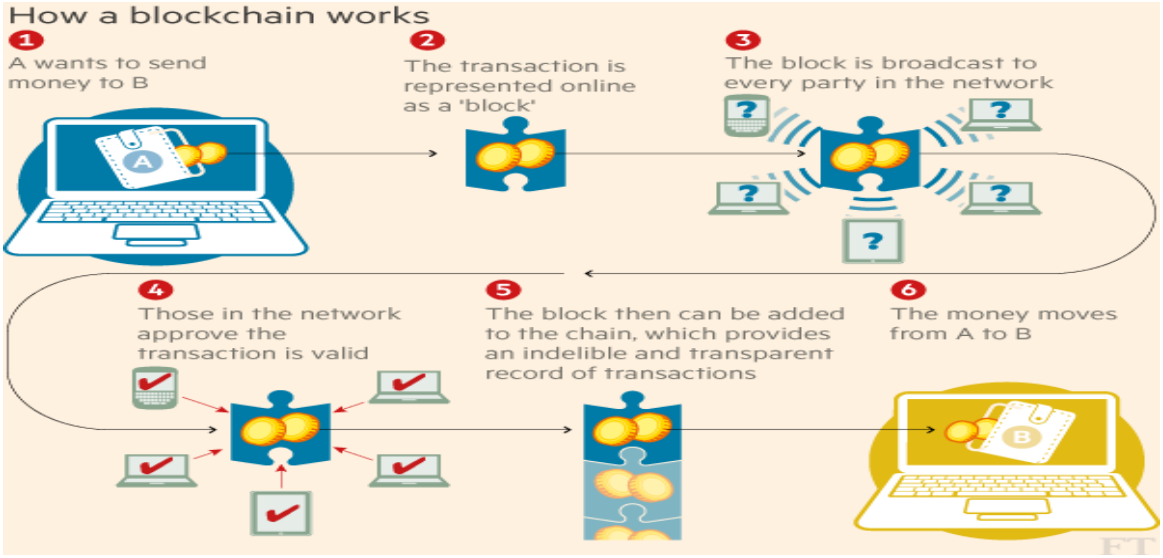

Fig 1[2] **Working of Blockchain**

Smart Contracts

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. For 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 which can work as an incentive for the dApp.
4. The application must be able to generate tokens and should have an inbuilt consensus mechanism.

Classification Of Decentralized Applications

1. dApps can be further classsified into 3 categories based on the type of block chain model they use which are as follows :-

TYPE I	**TYPE II**	**TYPE III**
dApps consists of their own blockchain	dApps make use of the Blockchain of Type I dApps, The dApps in this category are basically protocols having tokens necessary for their functioning.	dApps in this category use protocol of type II dApps.
An example of Type I dApp is Ethereum, which is currently the most popular dApp platform, and a great example of a Type 1 dApp. Other popular platforms include NEO, EOS and Bitcoin.	Example of Type II dApps can be dApps built upon existing blockchains such as etherum and bitcoin. One example is the 0x protocol, which uses Ethereum blockchain to power decentralized exchanges.	ype 3 dApps are built upon existing Type 2 Protocols. An example of a Type 3 dApp is the DDEX decentralized exchange, which operates on the 0x protocol.

2. dApps can be further classified into different categories based on their applications as follows:

Financial Applications - dApps of such kind provide users with different ways for managing their money and finances. For example, Bitcoin provides its users with a distributed and decentralized system of monetization. Central authority is eliminated leaving the power and regulation with the people of the network. Users are the sole owner of their money in these applications.

Semi-Financial Applications – dApps in this category consists of monalong with information that resides outside the blockchain. For example, insurance applications that allow a refund for flights in case of delay in arrival. Another example of Semi-Financial application is a fundraising mechanism known as Initial Coin Offerings(ICOs), which involves cryptocurrencies. ICOs send fund to smart contract in the form of virtual currency and in return the smart contract stores the fund and shares an equivalent value in the form of a new token at a later point in time.

Fully-Functioning Decentralized Applications - 3rd category of the dAppsuses all the features of both decentralized and distributed systems. They are the most popular type of dApps and are not financial at any level. For example, applications for online voting or decentralized governance.

Advantages

Fault tolerant[9]
As there is no single node controlling the data transaction and data records in the P2P decentralized network, there is no single point of failures in dApps. Its distributed nature supports this very strongly.

No-Internet-Censorship
It Controls and prevents Internet Censorship violation as there is no central controlling authority owning this dApps network. So if someone tries to manipulate with data sets in their favor it is

practically not possible. Any government authority if tries to block any dApps, it will be not be possible as app doesn’t lie on any particular I.P address being decentralized in nature.

Enhanced trust on the system

As no single entity own the apps it helps user to have confidence and trust on the dApps system against the data theft and manipulation.

Security

dApps uses Blockchain technology which was itself borne out of the intent to solve the limitations of centralized models, the vulnerability to security attacks and the chances of collusion and thus enhancing the security of the dApp. Since the code is stored on the blockchain and the information is distributed to all the nodes in the network, there is no single point of failure and thus makes it virtually impossible—and hugely expensive—to attack the whole network. In addition, transactions that occur on the blockchain are immutable, meaning that all verified transactions are stored permanently and cannot be tampered with, resulting in more secure data protection.

Transparency

All the records stored on the blockchain in spite of being open to the public is tightly secured through cryptography making each and every transaction is easily verifiable.In the context of dApps, this means that all executed amendments to the code, as well as all data stored on the blockchain, can be easily and precisely verified. Users of dApps can thus have confidence in its strong sense of data security and permanence of its records.

Speed, efficiency, and reliability

Decentralization essentially takes out the necessity for a middleman, resulting in faster and cheaper transactions. This also applies to the processing and storing of data on the blockchain, as well as those running on a dApp. With the pace of data coming from new and modern sources such as the Internet of Things (IoT), dApps offer a fast, efficient, and affordable way to handle big data. Moreover, as there is no central data center to harbor the entirety of the data stored, dApps are immune to downtimes and physical outages.

Community involvement

In a decentralized software model, any changes to the underlying code can only be executed after reaching a consensus. This fosters a stronger sense of community involvement, as everyone in the network can actively participate and contribute to the decision-making process. Additionally, the inclusivity of dApps also extends to its synergistic capacity. As anyone can interact with and use a decentralized app once it’s hosted on a blockchain, many dApps can be compatible with one another. This makes for a whole ecosystem of apps that seamlessly work together to create an innovative solution.

Payment processing: No user needs to integrate with centralized digital wallets to accept funds from users. All users can send/receive Cryptocurrencies as a common payment means.

User Credentials: Users don't need to sign up; they already have an account, which is a public/private key to bind with their user session and metadata.

Logging: Smart contracts can create their own logs, which a dApp can query to know what's happened in the past, rather than needing to create separate logs.

Drawbacks

Any Updation And Bug Fixes Are Difficult:

It is nor easy to fix any issues in dApps as every peer in the network has to update the fixes across all the copies in the network making it time consuming.

2. KYC Is Diffcult:

A lot of modern day centralized apps rely on user verification, which is quote easy given the single authority is controlling and verifying it. But with dApps as there is no one single entity responsible to do KYC verification, it is quite a challenge to build this type of apps in dApps.

3. Complex To Develop Scale

As there are complex networks and protocols to be implemented in dApps in- order to achieve consensus for data validation , the entire Apps needs to be planned and build considering the scale from the very beginning. It is not the case with Centralized Apps where you can build MVP and later on scale the system based on need.

4. Not Enough Evolved Third Party dApps:

As we rely many times on third party API to fetch certain their party information in the current Centralized App mechanism, you don’t have this leverage with dApps as currently there is no such large third party dApps ecosystem in place. As **dApps** are supposed to interact with another dApps for their API needs it is quite a lag which will improve over the period of time. dApps are not supposed to access API through any centralized Applications which is not the reality in current market dynamics.

Steps for Developing a dApp

Whitepaper and Prototype

First of all, a whitepaper is published, which describes the dApp and its features. This whitepaper outlines the idea for dApp development but also entails a working prototype.

Token Sale

The sale of initial tokens is set up.

ICO – Initial Coin Offering

The ownership stake of the dApp is spread.

Implementation and Launch

The final step is investing the funds in the development of the dApp and deploying it.

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].

Future Of dApps

dApps have the power to revolutionize the digital world providing better security and flexibility being a perfect match for technologies such as Blockchain, Cryptocurrencies , Smart Contracts ,AI as well as Computer vision. dApps will be a perfect match for such technologies since they are much more powerful than a traditional internet application. The potential uses for these blockchain dApps are endless. They can solve many real-world issues in areas such as identity authentication, supply management, food delivery, music services, and a variety of other functions which will become more evident as the technology develops. All these industries can benefit from dApps by enhancing application security, integrating with cryptocurrency and being free of external intervention.
Blockchain 4.0, the next upgraded generation of Blockchain stated to begin when almost all the industries's applications will be transformed into dApps[10].

This developing technology is slowly taking over the world as it attracts more and more users. As the concept of blockchain and decentralization grows, web applications will be less preferred. dApps enable value generation, and the fact that they eliminate the need for third parties makes them very enticing. Not only do they offer reduced costs for users, but also security.Apart from cryptocurrency, adopting blockchain in financial and other industries is a growing interest. This allows decentralized apps to develop even further away from the banking industry. Eventually, dApps will be customized by any individuals or businesses' requirements, just like web apps are today.For now, web applications are still more accessible and user-friendly, and they have a wider range of functionalities. However, once dApps become popular with non-professionals, they may give web apps a run for their money[11].

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/
9. https://blog.xsolus.com/advantages-of-decentralized-applications-dapps

10. https://www.netsolutions.com/insights/why-blockchain-based-dapps-are-the-future-of-decentralization/

11. (https://medium.com/hbus-official/what-is-a-dapp-eec896a4bbbf)