

Table of Contents

Introduction 3

The 9 logical components of a decentralized network 3

Contents 4

Blockchain and its fundamental components..... 4

Smart Contracts 6

Smart Contracts 4

Smart Contracts 6

Conclusion 4

 Type chapter title (level 2)..... 5

Type chapter title (level 3)..... 6

Citations 4

 Type chapter title (level 2)..... 5

 Type chapter title (level 3)..... 6

References..... 4

 Type chapter title (level 2)..... 5

 Type chapter title (level 3) 6

Abstract: True internet freedom accords the public in control of their data, a ***Decentralised Internet***, but at what cost?

1 Introduction

The terms decentralised, and internet have been dichotomous throughout its existence, owners of data farms gathering public information from its services has been the primary contribution to the existence of a decentralised network to begin with. Furthermore, organisations could listen and read data transmitted from devices to gather marketing strategies or worse, governments use them to censor public data.

But this power has to be managed efficiently, since corporations are currently providing a reliable service to the public, we have to understand the problem in its original creation: servicing data stored on servers on the cloud which provide the content displayed on the interface. Therefore, every online transaction made by the public today has been through a ‘middle-man’ server. The choice as to how long the data is kept, and to how the data is treated might be contractually binding, however many companies are being caught using data in unlawful ways to convene their markets at the publics expense.

The question is revealed: How do we receive data from anything else, since we originally have been receiving and sending to servers?

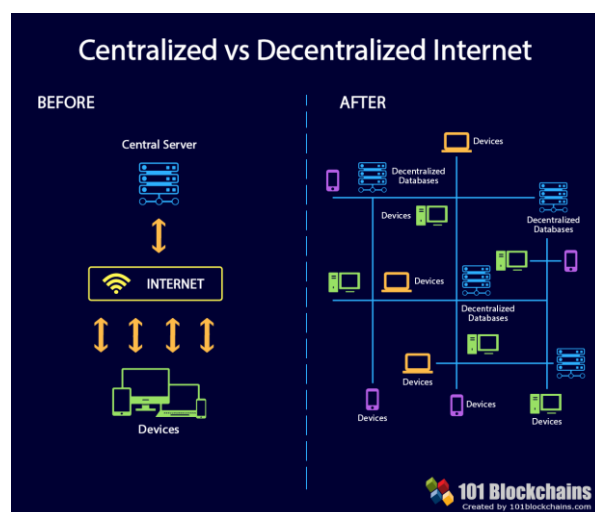
Well.. true decentralisation compliments individual privacy and for our data to be unmonitored by any single entity within its network, but how would this be possible?

The following are fundamental components of a decentralised internet, however components 6 (Money transactions) and 7 (Wallets) respectfully, are focused for the duration of this research to directly target the main challenges faced and that being the blockchain and the evolution of smart contract sections discussed further on the paper:

1.1 The 9 logical components of a decentralised network:

- | | |
|--------------------------|-------------------------|
| 1. Infrastructure layer | 2. Consensus mechanisms |
| 3. Distributed computing | 4. Distributed storage |
| 5. Privacy and identity | 6. Money transactions |
| 7. Wallets | 8. Exchanges |
| 9. Industry applications | |

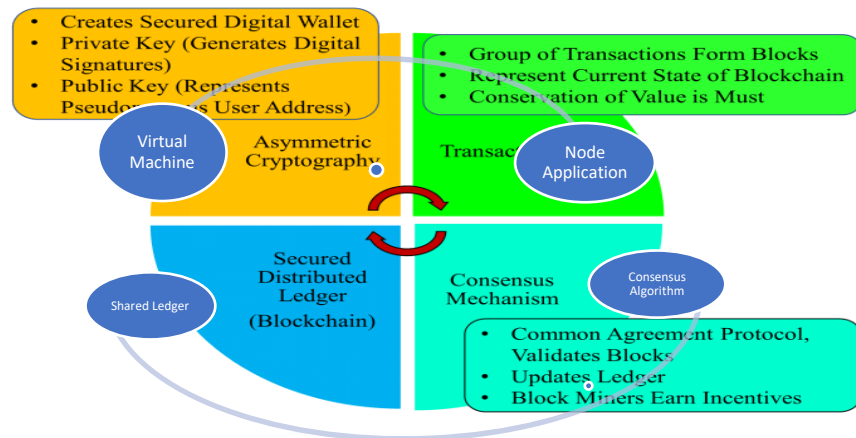
All these components contribute to the decentralised network eco-system, however the monetary transactions for this topic will be indirectly targeted by the logic that encompasses successful transfers. So, in order to get the correct credentials to start dealing with monetary stocks we must perfect the upcoming technologies in their higher demanded components to ensure the concept of a decentralised internet is possible.



2 Content

2.1 Blockchain

To allow a perspective of blockchain, think of it as a technology that allows peer-to-peer sharing of resources between devices and manages the life cycle of the data. To put the blockchain ecosystem to its logical [components](#) we factor the following components:



- **Node application**
this is the device that has the application that allows the functionality of the communication and storing of the data, without a node the blockchain wouldn't be able to estimate the unique key for that device to make use of content shared from the blocks containing data, it also has the rights of the shared ledger discussed as follows
- **Shared ledger**
every node application has a set of rules to follow made up by a smart contract for operation of the application, these rules enforce the procedures of data received and sent as determined in the following consensus algorithm, if the algorithm cannot satisfy that the node is using the blockchain correctly the ledger will not allow the node to interact with the network.
- **Consensus algorithm**
the gatekeeper as to how data is distributed in a network and implements the rules set by the ledger to control incoming and outbound data that should not disrupt the blockchain flow, meaning that you could send and receive as much data to your node however the content being sent cannot distribute amongst nodes that don't access that content.
- **Virtual machine**
allows the emulation of such node application to run. It's the founding logic that contains libraries for functionality to behave correspondingly to the information in/outbound. For a node to exist it requires a service that will provide data for functionality of the application, this service is in built to the virtual system installed and the node application calls the libraries whenever intended use is required for example, decrypting data incoming and encrypt outgoing.

With the logical components in place we can conceptualise an entire eco system that blockchain has built and in order to use this technology correctly we have to strategize the idea of decentralisation and the internet as simultaneous importance to find an optimal solution, so we have to consider fundamental component 8 (Exchange):

2.1.1 **Communicating between nodes on a blockchain**

Communication between nodes have been researched since the beginning of ARPAnet and some effective solutions have come up since, with the power of the following collaboration solutions we can use those communication protocols established:

- **Peer-to-peer technologies**

This resembles the architecture that the blockchain will follow to share content amongst nodes, the connection established will ensure a trust protocol from the consensus algorithm to each node where content is now shareable. The connection type is negligible however here are some considered communication protocols considered:

- **Bluetooth**
- **HTTP/TCP, email and many other internet protocols**

Basically, existing protocols will enable the peer to peer to communicate between nodes and transfer content accordingly. However nodes in the network will not always require all the information shared, that's where blockchain comes helpful as the ledgers holding the rights to the data will allow the content to be passed onto the next node requiring access to that data and that's when it will update the blockchain network.

We allow internet protocols to provide a chance for communication in a P-2-P network, furthermore we realise that internet protocols are maintenance intensive and would require an organisation to handle the requests, albeit this raises concern in the decentralised network however the functional requirement of communication will require signal routers to link nodes in a network across the world, therefore we introduce:

- **Internet Service Providers**

The eradication of a centralised network is the ability to provide content directly to nodes using peer to peer, however the usage of internet protocols requires a server to provide the service of each call made between nodes, therefore ineffective for decentralisation. However, HTTP requests can be redirected to its corresponding node instead of allowing the server that contains that data to send the requested data. Therefore, a complete infrastructure change would be required from ISPs as the local connections form a greater challenge to the overall connectivity reliance. Thus, ISPs are pushing to get 5G operational within high population areas.

We observe that ISPs provide a key role in the making of a decentralised network. Furthermore, the content shared on the decentralised network will never be intercepted as it will get passed along the nodes containing that very content using key cryptography, therefore only nodes with this key are able to view the content shared. ISPs therefore will be unable to control the content of the requests made; we don't want to allow ISPs to be able to mismanage the maintenance of the signal routers as that would compromise the definition of the decentralised network.

We allow our blockchain to communicate between nodes using the methods discovered in 1.1.1, however communication will be ineffective if the data stored isn't there or inaccessible, we now consider the logical component listed 3 (Distributed computing). and 4 (Distributed storage). This stage of decentralisation requires nodes in the blockchain to have a copy of the content to be accessed:

2.1.2 **Distribution of content in a blockchain**

Data needs to be allocated somewhere in a blockchain, which will be placed on each node, using cryptography we decide which node would require storage of that data which itself depends on the nodes that share a unique key on that individual block, this will decide how many copies of the block exist on the chain of nodes, to put it simply, if you share a picture on Facebook, all your friends on the decentralised network who have a shared ledger to exist in the blockchain will receive a copy of your picture stored on their personal devices. This may cause storage overloading on many devices, so we investigate the consistency of the replication of data. Only points at which data is created we must further rationalise the approach to ensure a reliable feed of data; we introduce:

- **RAID technologies “Redundant Array of Inexpensive Disks”**

This will allow a copy of the origin content to be replicated on another drive located on the network, this strategy sounds like it will just create twice as much data to store than originally, that is true with the following levels of RAID

- **RAID 0** – striping.
- **RAID 1** – mirroring.
- **RAID 5** – striping with parity.
- **RAID 6** – striping with double parity.
- **RAID 10** – combining mirroring and striping.

Moreover, a node will have to notify the user on which type of redundancy will the device require, and this will have cooperated with the same numbers of users that share that data. Therefore, any level higher than RAID 1 will cause complications and inefficiency within the sharing of content. RAID 1 allow 2 drives on the network to be synchronised and the content that is synchronised between these two nodes serve as a primary source of the data that is exposed to the entire blockchain if they shared that block effectively.

The synchronisation of drives online will provide the key to blockchains success, removing the need of a server being there for any needs, however a device will become inactive if the entire drive that stores its operating system and personal data also is synchronised with another devices drive, causing havoc in the functionality of the nodes using RAID 1, in this section we discuss how to alleviate the stress of available drives:

- **Drive Partitioning**

A user whom is part of the blockchain would require the main drive of their device to be partitioned or an entire virtual drive will need to be available so that the entire contents of that virtual drive can be synchronised with another drive online, these synchronised drives will provide the resources required when another node in the blockchain requests to view, based on the shared ledger agreement of that block, the content is now available to the requesting node

So, we introduce the implementation of smart contract to further analyse the rights at which devices are granted to have the necessary permissions to read or modify the contents of that block

2.2 Smart Contracts

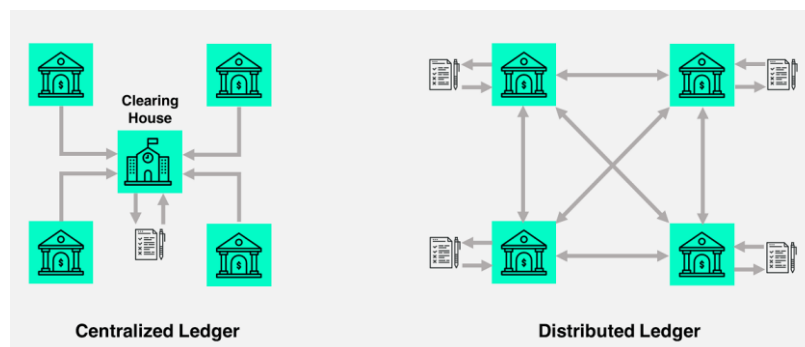
The whole idea of smart contract enforcement is to ensure the integrity and authentication of that data. We need to ensure that the data shared on the blockchain is still secure received from the authentic origin and arriving at the correct destination with a node having a shared ledger of that copy of data by being linked to the application of another node that shares the privileges that both node applications have been granted, these privileges include:

- Having rights to read / modify content
- Having the correct key provided by the shared application that will allow the block to be updated between these nodes



To ensure that the keys between nodes are shared in a secure manner we cannot simply pass a hashed key that grants access to the content without conditioning the distribution of contents, the means of conditioning is set to standards which make a decentralised network exactly that, and this is produced by a:

1.2.1 Shared Ledger



Another decentralised technology is required to provide sufficient rollout of a decentralised network as the shared ledger itself has no administrative duties to bind any parties in a blockchain as the permissions deduced are stipulated in the ledger itself, these permissions are of a wide range as they are always application specific, in terms contributes to parties being liable for the data stored on their drives which is shared on any application it has been exposed to in the shared ledger you agreed to for the terms of use of that application.

The documentation produced from these ledgers from a legally binding document between every node in a blockchain but we don't understand the primary goal of the shared ledger, and that is the distribution of the smart contracts compiled by code that enforces the regulations between parties.

With a shared ledger we allow different nodes to form a mutual trust that when a certain block is updated within the blockchain, all nodes must be updated with the new founding information within the ledger to ensure the smooth operation of the smart contracts, this assist multiple organisations that rely upon each other to provide resources for the service it renders for example if a client transfer money from their account to another, the bank must first release that money from the total exchange its allowed to transfer and also balance the transferred money with international markets at the time the money is transacted to ensure that money at a certain time was correctly transferred.

1.2.2 Security issues concerning smart contracts

Data should be fully controlled by the origin, using appropriate legislation we need to ensure that every node has a confidential interaction to the blockchain. If by any chance the original owner of that data loses the majority consensus determined by the algorithm, that node loses the ability to change that data from the blockchain. That being said, replication of data is the something that a smart contract would have to address as the true origin of the content should have never been accessed to modify firstly, as discussed with the distribution of data, any data that is replicated should follow a backup strategy to provide the data whenever that node is unavailable, however that key will be unique to that specific block and any other block containing the same data as the mentioned block will have a separate key with its own ledgers as to how that data may be accessed

We discover that in a decentralised network that trust is given to a node and that node is expected to behave in a certain way that contributes to the entire network, the role of the smart contract is to enforce exactly that and to allow the procedures to continue if all parties have their mandates followed. The smart contract must also stipulate the consequences of misbehaving on such a network by ensuring that:

- A node that doesn't uphold the smart contract mandate by using the given data exactly how it was intended for use
- A node that attempts to damage the network by modifying properties of the content directly without permissions
- A node that tries to override the network by consuming all the keys

The smart ledger will interactively work with the blockchain to get consistent updates to ledgers to ensure each node has the latest ledgers in terms of the content it hosts. No policies can be added to a ledger once it's assigned to the nodes, unless 51% of the nodes with correct permissions to modify the content that the ledger protects agree to a policy update, the data shall remain untouched.

1.3.2 Conclusion

We have discussed majority of the 9 logical that ideally contribute to a decentralised network of content sharing where the main challenges are faced of implementing the concept as the primary function of decentralised data sharing, therefore any currency marketplace affiliations are to be negligible.

The core finding of decentralised networks was discovering the use of blockchain technologies to enable peer to peer communication, however we had to identify at what cost did the implementations of founded technologies:

- **Blockchain**

The initial implementation would have to perfect the rollout of data distribution effectively as any upgrades to the system afterwards would have to have a majority of 51% of nodes on the blockchain agreeing to the new feature release. Which could prove to be impossible if a majority of user would think that the update is unnecessary, therefore any implications on the initial release could be catastrophic due to the regulations that have not being protocolled accordingly.

- **Smart Contracts**

For every transaction on a blockchain the transaction would have to be processed in a smart ledger before that process can be confirmed to update the entire blockchain it affects, which provides the security layer of not allowing content to be misused and shared across unwanted places, however if the node has not completed a task correctly it could deteriorate the experience for every other user connected in the blockchain that pulls data from the origin, it will implicate the ability to verify the smart contract as the chain has been broken and cannot request the content from a drive that is linked in that blockchain

Ultimately we observe the implications that could be costly to the users in a blockchain, where reliability of the network to work effectively at an individual level depends on the number of users on the blockchain that make a decision that contributes to the 'fairness' of such a network, the ability to maintain a smart contract also impacts reliability as if a node is sharing data it has to be online to provide the block requested by other nodes, if the block cannot be sent, a breach of the smart contract is clear as data is requested from a non-existent location which in turn breaks the chain of content sharing and becomes the weakest link in the blockchain that affects every user requesting the same block.

In conclusion, blockchain technologies seem adequate to implementing an efficient strategy in the role of a decentralized internet, the entire eco-system addresses the primary needs of such a network and the concept of shared resources is a primary goal of blockchain, the integrity instilled into the blockchain will be entirely determined by the majority of people who believe a certain procedure requires arbitrary legal proceedings to validate that each party on a blockchain behaves in accordance.

The political debacle it now generates is a battle for the generation that manages to operate a decentralised network and as humans our cultural differences have been observed in the past, moreover the decisions of different cultural groups will greatly define what a new decentralised internet defines

Thank you for taking the time to read my research paper:

Tiago Pinto

(Definition/s):

Decentralization or **decentralisation** is the process by which the activities of an organization, particularly those regarding planning and decision making, are distributed or delegated away from a central, authoritative location or group.

Internet - a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols