HOWDOO
The Power of Sharing

howdoo

Abstract

Today's social media platforms are limited by the platform providers. Leading platforms steal user data for the platforms' benefit, failing to incentivize content creators. However, most blockchain-based platforms have limited scalability, leading to transaction bottlenecks. This makes launching new dApps on these networks non-viable.

Howdoo solves these issues by releasing a public, decentralized blockchain with an advanced social layer. This enables infinite scalability, providing an ideal platform upon which to build decentralized dApps. Howdoo's decentralized platform incorporates all the good that exists in modern-day social media and electronic currency exchanges, putting that power in the hands of people using it. With Howdoo's social layer, users gain more control over their data and are compensated for creating content. Developers gain a powerful decentralized platform upon which to build their dApps. All participants enjoy the ability to utilize the time spent by people on social media and community networks in the form of real assets, empowering users, society and the world at large.

This whitepaper examines the technical aspects of Howdo's distributed public network, showing how it enables everyone involved to become part of a financially rewarding community of users. This will also show how Howdoo allows all users to collectively benefit from the commercial viability of the network, translating individual contributions into real wealth.

Table of Contents

1 Introduction

While the concept of a decentralized digital network has existed for decades, realizing this concept has proven challenging, even to the current day. The incognito e-cash protocols of the late 90s, mostly reliant on a cryptographic primitive known as the Blind Signature proposed by David Chaum, provided currencies with a high extent of seclusion. But the protocols failed to gain acceptance, largely because of their dependency on a centralized intermediary. While some modern blockchain networks have achieved greater decentralization, they often suffer two critical problems.

First, achieving a truly decentralized infrastructure layer that meets its network's scalability needs is impossible on most blockchain networks. This is due to the inability of nearly all blockchain infrastructures to scale performance and speed once users hit critical mass; in fact, most major blockchains (such as those used by Bitcoin or Ethereum) received notoriety in the press when sudden public interest led to major transaction delays and high transaction costs.

The second challenge to executing a decentralized cryptographic network is developing an app layer. Decentralized applications (dApps) require a stable, reliable network to deliver user experiences that actually promote user growth. Yet due to the natural bottlenecks and scalability challenges described above, most dApps are doomed to fail even before they launch. Additionally, the lack of a unified ecosystem makes dApp development difficult, leading developers to turn to other platforms upon which to build.

Though these challenges are difficult, solving them is more important than ever. Social Media and commerce on the modern-day internet have come to rely almost exclusively on institutions serving as trusted third-parties for the system to function. While the system works well enough for most intents and purposes, it still suffers from the inherent weaknesses of the trust-based model. As the public becomes aware of the common practices of data mining and selling private information on the part of major social media networks, public trust in these key institutions is inherently declining.

In order for a truly decentralized digital network to exist, there needs to be a reliable alternative that enables users to maintain control over their data. This type of network needs to be truly decentralized, and it needs to be able to scale to support an infinite number of users. this type of network also needs to consistently deliver excellent user experiences in terms of performance and reliability as users scale. The mere existence of this network would incentivize developers to build attractive social media dApps. Additionally, users are increasingly interested in privacy, control over their data and receiving compensation for contributing content to these social networks. It is likely a social network offering these features would be immediately popular if it were built by developers who delivered exceptional user experiences.

The need of a social network based on cryptographic proof and an optimal level of trust, allowing any two disposed parties to interact and transact directly with each other without the need for a centralized authority still persists.

- **1.1 Purpose**

  The aim of this document is to provide a brief overview of the Howdoo system. It is a basis for a non-formal agreement between Howdoo Team and other stakeholders about the product to be developed.

- **1.2 Document Convention**

  For most part of the document, the IEEE conventions for Technical Specification Documents have been followed.

- **1.3 Intended Audience**
  This is a white paper, open to everyone who wish to know about the Howdoo system.

2 Problems and Roadblocks

There are several fundamental flaws with the present-day systems:

2.1 SOCIOECONOMIC

- Users are burdened with a constant stream of unsolicited advertising.
- Users have negligible control over their personal data which is sold to the advertisers.
- As the established and big players continue to dominate the social market, the content creators are not being fairly compensated for their work.
- There is no strict moderation and penalty in place for antisocial behavior, cyberbullying and trolling.
- Overseas movement of money is an expensive and cumbersome process owing to the numerous forex fees and service charges. If someone without a bank account wishes to transfer their money, they end up paying even more charges.
- Sellers and Advertisers are largely isolated from the consumers, as the majority of social media advertising constructs in place these days fail to link the individuals to the products directly.
- Advertisers are prone to frauds as they don't have any real and verifiable insight into the space on which their ads are displayed or if they are even displayed altogether as promised.
- There is a lack of audit trail in the current social media construct and it has negative impact on both the consumers and sellers.

2.2 TECHNICAL

- Existing blockchain platforms are burdened by large fees and limited computational capacity (i.e speed and latency) that prevents widespread blockchain technology adoption.
- In the current blockchain systems, failed or broken applications cannot be frozen, isolated and fixed. Instead it disrupts the whole network, forks happen, and investors can lose their money.
- The existing blockchain platforms are not robust enough to fix bugs when they inevitably occur. Furthermore, these blockchains lack a built-in functionality where this can be done without disrupting the whole network.
- Businesses building blockchain-based applications lack the flexibility to enhance their applications with new features owing to the limitations of the existing blockchain technologies.
- The current blockchain systems have limited scalability given their low transaction throughput. A lot of scalable blockchain solutions are being developed but none of them are scalable enough to support a full-fledged social network and currency exchange system.
- Crypto-based services still face difficulty in seeing mainstream adoption because the interaction using their cryptocurrencies via their wallets do not provide the same level of ease and familiarity as with existing online payments and money transfer systems such as PayPal, Skrill, Stripe, and WePay.

3 Approaching the solution

3.1 WHY BLOCKCHAIN SOLUTION?

Mainstream social media has existed for decades and will continue into the foreseeable future. But most of these networks rely on ad-based business models which share a major shortcoming: users and creators are unequally compensated for their participation on the platform. For example, on August 13, 2017, Barack Obama produced the most liked tweet in Twitter history; however, he received no direct reward for doing so despite advertising revenues this may have generated for Twitter. Through creating a public blockchain with an advanced social layer, users could be fairly compensated for their participation in this ecosystem. This could also solve monetization challenges through a new form of crowdfunding.

In centralized social networks, user data is often compromised by being used for purposes of advertising and analytics. However, a social network built on a Blockchain-based ecosystem could be designed to ensure there is no single entity that can enforce invasive monitoring and controls over user-generated content.

These, along with many other factors like forced advertisement, cyber-bullying, lack of data privacy, etc. can be resolved by building a transparent social media network on Blockchain.

3.2 REQUIREMENTS TO BE ADDRESSED

Howdoo would be a decentralized social networking platform with added support for advanced blockchain applications like wallets, exchanges and other dApps. In this section we will discuss the essential requirements for Howdoo system.

3.2.1 On chain transactions

There is a need to be able to perform operations such as multimedia content uploading and transfers along with µDoo and token transfers (tokens here refer to tokens built on top of Howdoo blockchain) inside Howdoo blockchain ecosystem.

3.2.2 Distributed storage

Content provided by users and advertisers along with the users' private information is to be safely stored on decentralized storage.

3.2.3 Data and Message Privacy

In order to ensure the security and privacy of data, encryption is needed in the Howdoo ecosystem. Moreover, end-to-end encryption needs to be implemented along with message reversing feature in Howdoo chat, so that the sent message data can be retracted if needed.

3.2.4 Faster load times

Howdoo is a social networking platform. Thus in order to achieve an enhanced user experience, it is imperative that content load times on the Howdoo platform are low and content should be delivered in real time.

3.2.5 Internal exchange for Tokens

Howdoo will support multiple dApps built on top of it and these dApps may have their own tokens built atop the Howdoo blockchain. Therefore, Howdoo needs to support token deployment on its platform, while providing services to exchange these tokens with each other as well as with µDoo, which is the cryptocurrency of the Howdoo ecosystem.

3.2.6 Governance mechanism

Howdoo needs a system in place which can ensure the maintenance and improvement of the Howdoo ecosystem in a decentralised manner.

3.2.7 Smart contract mechanism

Various aspects of Howdoo require functioning smart contracts deployed on a decentralised solution. These are essential to process agreements among various users of the Howdoo platform in a trustless manner, without a central authority.

3.2.8 dApp platform

Howdoo aims to support thousands of dApps functioning parallely on it, while interacting with each other and with the services exposed by the Howdoo platform.

3.2.9 Scalability
Howdoo ecosystem is to be designed to sustain widespread adoption, while maintaining its decentralised core.

3.2.10 Required request throughput
Howdoo ecosystem needs to process requests on par with existing social networks in a decentralised manner. Here are a few stats from Facebook's OLTP performance that serve as a benchmark for the Howdoo ecosystem:

- Query response times: 4 ms : reads, 5 ms : writes
- Rows read per second: 450,000,000 peak
- Network bytes per second: 38GB peak
- Queries per second: 13,000,000 peak
- Rows changed per second: 3,500,000 peak

4 Howdoo

Howdoo is a revolutionary blockchain solution which has its roots in one of the most promising blockchain technologies. It has been additionally improvised to support a full fledged distributed social media network. This makes it the most democratic yet scalable blockchain solution.

4.1 RESEARCH : END RESULT

In implementing Howdoo, quite a few existing solutions were considered and tested using a prototype. This subsection explores the blockchain technology selected to serve as the foundation of Howdoo. For full details on our testing and selection methodology, see section 6.

4.1.1 EOS blockchain

The EOS system introduces a new blockchain architecture designed to enable vertical and horizontal scaling of decentralized applications. This is achieved by creating an operating system-like construct upon which applications can be built. The system provides accounts, authentication, databases, asynchronous communication and the scheduling of applications across hundreds of CPU cores or clusters. The resulting technology is a blockchain architecture that is capable of scaling up to millions of transactions per second, eliminates user fees, and allows for quick and easy deployment of decentralized applications. (ref)

4.1.1.1 Key Properties

- As of May 5th 2018, excluding merges, 43 authors had pushed 818 commits to EOSIO's github. This put EOSIO in the top 8 most active c++ projects on github in the month of April.
- The cofounder of EOS is also the founder of Bitshares and Steemit both of which are quite successful dApps themselves and are able to handle upto 1000 TPS.
- EOS promises a good user experience without delays. It is achieved in EOS broadly via:

  Parallel Performance
  It allows large scale applications to divide the workload across multiple CPUs and computers.

  Sequential Performance
  EOS allows applications such as exchanges which just cannot be implemented with parallel algorithms due to sequentially dependent steps with enough sequential performance to handle high volumes.

- EOSIO based blockchains execute user-generated applications and code using WebAssembly (WASM). WASM is an emerging web standard with widespread support of Google, Microsoft, Apple, and others. At the moment the most mature toolchain for building applications that compile to WASM is clang/llvm with their C/C++ compiler.
- EOS uses BFT-DPOS consensus mechanism.

4.1.1.2 EOS Scalability Benchmarks

Since the inception of EOS, four developer versions have been released based on user feedbacks and test results which are classified as Dawn 1.0, Dawn 2.0, Dawn 3.0, Dawn 4.0 respectively. EOS Dawn 3.0 refers to the previous developer release designed to be "feature complete" with stable APIs.

Through a Parallel Chain Case, EOS Dawn 3.0 could possibly achieve an unlimited TPS. This would be done through implementing inter-blockchain communication to divide workloads across as many blockchains as needed. For example, 1000 parallel chains could produce millions of TPS.

Howdoo's unique implementation of blockchain technology effectively solves the technical limitations affecting other blockchains. Thus, Howdoo is uniquely positioned to provide a blockchain ecosystem upon which a true, high-performance competitor to Facebook and other social media platforms could be built.

Dawn 3.0 has already been succeeded by Dawn 4.0, bringing major changes and producing even better test results.

4.1.1.3 Smart Contract Engine

The decision to implement smart contracts in general purpose languages such as C++ and Javascript exemplifies a design focus that favors performance and features over security. This also highlights that EOS supports Turing complete languages, which should be able to suffice the requirements of Howdoo ecosystem.

Each account on EOS can send structured Actions to other accounts and may define scripts to handle Actions when they are received. The combination of Actions and automated action handlers defines smart contracts in EOS. Smart Contracts can communicate with each other, for instance, to have another contract perform some operations pertinent to the completion of the current transaction, or to trigger a future transaction outside the scope of the current transaction. Communication among contracts should be considered as occurring asynchronously. However, the asynchronous communication model can result in spams, though this can be resolved by the resource limiting algorithm provided by EOS.

4.2 DEVELOPMENT

Although EOS has all the features that a dApp needs, it was designed for a public use case and has its own economy model. Howdoo is intended to be a social platform and has its own set of technical requirements that are specific to the challenges that it is aiming to solve. This eliminates the use of any public chain.

4.2.1 Added features

This subsection details the shortcomings that Howdoo would have had if it were implemented as a dApp on EOS rather than a separate blockchain along with the features that were added/improvised on top of EOS to create Howdoo.

4.2.1.1 Isolated seperate network

→ **Problem Statement**
In EOS blockchains, the entire network is to be headed by 21 chosen block producers. As time passes, the user base of EOS is expected to grow tremendously, and with it will grow the strain on the resources. This is bound to create network congestion for Howdoo's system (if deployed as a dApp on top of EOS blockchain) as it will have to compete with other users and dApps on EOS for resources.

→ **Requirement**
Howdoo ecosystem requires an isolated network.

→ **Solution**
Howdoo will operate on a entirely separate fork of EOS running it's own blockchain governed by Howdoo users and ECO Company.

→ **Benefit**

- Howdoo and the dApps hosted on top of it will not end up fighting with other resource hungry dApps on EOS blockchain which will ensure smooth execution.
- Having its own set of delegates (master and spare nodes), Howdoo will be more efficient in handling the ecosystem and 3rd party dApps' installations, rather than if it were dependent on the global EOS block producers.

4.2.1.2 Restricted Smart Contract deployments

→ **Problem Statement**
Anyone can deploy smart contracts on a blockchain given it's public nature which will crowd the Howdoo ecosystem with unrelated and resource hungry dApps.

→ **Requirement**
We need full potential of Block Producers to be available for Howdoo Platform dApps.

→ **Solution**
Howdoo will provide a set of restricted APIs that can be used by other dApps developers to leverage the inbuilt functionalities of the platform and construct a solution for their own specific use cases.

→ **Benefit**
These APIs would be designed in a manner that they do not compromise with the security and scalability of the platform, but at the same time give enough functionalities to dApps developers to build rich and interactive applications on top of the platform.

4.2.1.3 Incorporation of Proof of Trust in election process

→ **Problem Statement**
Choosing election candidates based only on a prospective Block Producer's market value seems like a far fetched solution.

→ **Requirement**
Howdoo is in need of an internally maintained score which should be a true reflection of a master node's capacity and capability.

→ **Solution**
Howdoo's "Proof of Trust" will be included in the election process for the Block Producers. Proof of Trust will be calculated for each node in the network (detailed in section 5.3.1.1.5) which is an indicator of stability, offered space & resource. We are modifying the core logic of EOS to enforce the inclusion of this continuously calculated value in the election process at protocol level.

→ **Benefit**
Master nodes will be enforced/motivated to maintain node availability along with better infrastructure to be in the lead.

4.2.1.4 More Democratic Election Procedure

→ **Problem Statement**
A select few nodes may keep getting re-elected to be block producers (given their influence over the network accumulated over time).

→ **Requirement**
We need a way to give a fair chance to other contenders to get on top.

→ **Solution**
If a node has been working as a Block Producer for a cumulative time period of 10 days over a span of 15 days, that node is automatically removed as a Block Producer and cannot take part in the elections for the next 7 days.

Benefit
→ With this forced circulation of Block Producers, the spare nodes will get a chance to become Block Producers.

4.2.2 Utilizing Parallelism

EOS supports parallel execution. By leveraging this feature, the Howdoo platform has been designed as a set of multiple dApps which can be executed parallelly.

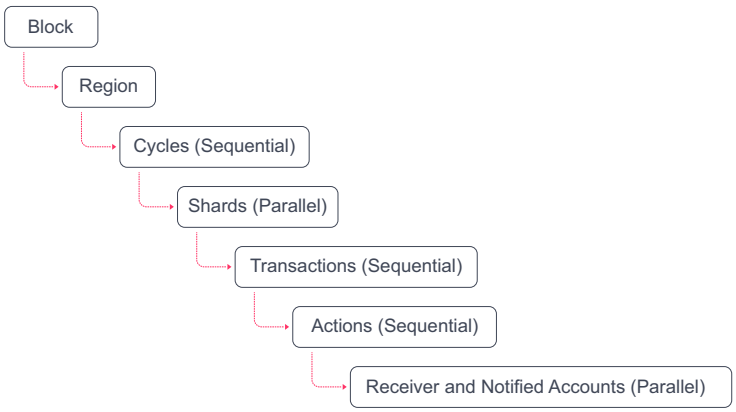
All the tokens that exists in the platform are supported by their own internal Smart Contracts that will execute parallely, making micropayments blazing fast. All these contracts can run in parallel and independently from one. Other functions that can be parallelized include: advert engine instances, fake view elimination engine, community management system, and exchange engine components, as smart contracts on these engines will be independent of each other.

It will be the job of the block producer to organize Action delivery into independent shards so that they can be evaluated in parallel. The schedule is the output of a block producer and will be deterministically executed, but the process for generating the schedule need not be deterministic. This means that block producers can utilize parallel algorithms to schedule transactions.

Part of parallel execution means that when a script generates a new Action it does not get delivered immediately. Instead it is scheduled to be delivered in the next cycle. The reason it cannot be delivered immediately is because the receiver may be actively modifying its own state in another shard.

4.2.2.1 Decreasing Latency

Howdoo's current blockchain is inspired from EOSIO, Dawn 3.0. With future releases, Howdoo may upgrade to new versions of Dawn while making improvements of its own if needed. Each block is divided into cycles. Each cycle is divided into shards and each shard contains a list of transactions. Each transaction contains a set of Actions to be delivered. This structure can be visualized as a tree where alternating layers are processed sequentially and in parallel.



Transactions generated in one cycle can be delivered in any subsequent cycle or block. Block producers will keep adding cycles to a block until the maximum wall clock time has passed or there are no new generated transactions to deliver.

It is possible to use static analysis of a block to verify that within a given cycle no two shards contain transactions that modify the same account. So long as that invariant is maintained a block can be processed by running all shards in parallel. This enables two accounts to exchange Actions back and forth within a single block without having to wait for a block period between each Action.

4.2.2.2 Processing read only actions and Context free actions

Read only actions do not modify the state of the Howdoo blockchain and therefore can be processed in parallel, so long as these are read only action requests for a particular account within a single cycle.

Context free actions involve computations that depend only on transaction data, but not upon the blockchain state. Signature verification, for example, is a computation that requires only the transaction data and a signature to determine the public key that signed the transaction. This is one of the most expensive individual computations a blockchain must perform, but because this computation is context free it can be performed in parallel.

4.2.2.3 Atomic Transactions with Multiple Accounts

Sometimes it is desirable to ensure that Actions are delivered to and accepted by multiple accounts atomically. In this case both Actions are placed in one transaction and both accounts will be assigned the same shard and the Actions applied sequentially.

4.2.2.4 Subjective Best Effort Scheduling

This subjective evaluation of computational cost frees the blockchain from having to precisely and deterministically measure how long something takes to run. With the undermentioned design there is no need to precisely count instructions which dramatically increases opportunities for optimization without breaking consensus.

In Howdoo, at a network level all transactions are billed a computational bandwidth cost based on the number of WASM instructions executed. However, each individual block producer using the software may calculate resource usage using their own algorithm and measurements. When a block producer concludes that a transaction or account has consumed a disproportionate amount of the computational capacity they may simply reject the transaction when producing their own block; however, they will still process the transaction if other block producers consider it valid.

In general, so long as even 1 block producer considers a transaction as valid and under the resource usage limits, then all other block producers will also accept it. However, it may take up to 1 minute for the transaction to find that producer.

In some cases, a producer may create a block that includes transactions that are an order of magnitude outside of acceptable ranges. In this case the next block producer may opt to reject the block and the tie will be broken by the third producer.

4.2.2.5 Deferred Transactions

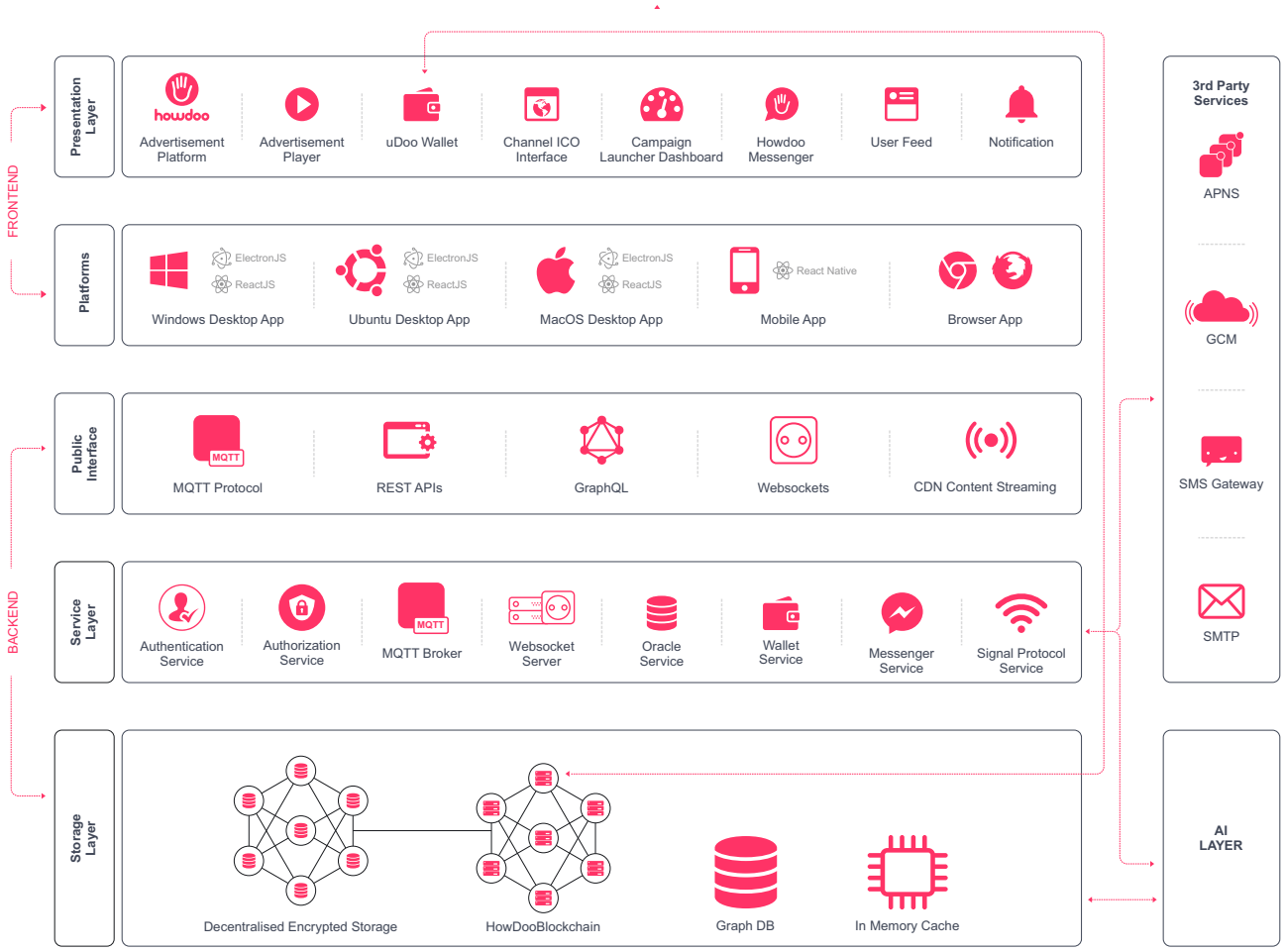
Howdoo has support for deferred transactions that are scheduled to execute in the future. This enables computation to move to different shards and/or the creation of long-running processes that continuously schedule a continuance transaction.

5 Howdoo Ecosystem

This section describes the entire Howdoo Ecosystem.

5.1 ARCHITECTURAL LAYERS

Below figure represents the layered architecture diagram of the Howdoo ecosystems. It's purpose is to define which systems/subsystems/modules have been implemented as a part of which layer.



→Front-End Layers

- **Presentation Layer**
  This layer represents the feature components which are available to end users
- **Platforms**
  This layer represents all the platforms where Howdoo application is available

→Back-End Layers

- **Public Interface**
  This is a virtual layer where all endpoints of the different microservices are exposed to be consumed by front-end components. All the front-end applications interact with this layer.
- **Service Layer**
  All different microservices that incorporate the business logic reside on this layer. This layer is responsible for serving the data to front-end applications via Public Interfaces. It also handles third-party components.

- **Storage Layer**
  This layer is used by components in the service layer to store the data and process it.

- **AI Layer**
  The AI layer will interact with the Storage layer and Service layer and will be used to deliver relevant advertisements to users/communities.

5.2 ARCHITECTURE DIAGRAM

The high level architecture diagram of the overall Howdoo Ecosystem is presented on the next page. The architecture has been broken into following subsystems:

→ **Governance:**
This subsystem comprises of election process to elect the leaders for smooth functioning of the system, issues' resolution etc. It has been elaborated in section 5.3.1.

→ **Finance:**
This subsystem comprises of the wallet functionality along with all the transactions done using the underlying cryptocurrency of Howdoo ecosystem or any of the numerous tokens built atop Howdoo system. This has been detailed in section 5.3.2.

→ **Content Delivery:**
This subsystem comprises of all the modules which aid in delivering the content stored in a decentralized manner to the Howdoo users.It has been described in section 5.3.3.

→ **Adverts:**
Adverts subsystem includes the advertisers, the audience and the delivery mechanism of the advertisements to appropriate audience based on their preferences and assent. This has been elaborated in section 5.3.4.

→ **Messaging:**
This subsystem consists of a messaging app and the end to end encrypted exchange of messages between Howdoo users. This subsystem has been detailed in section 5.3.5.

→ **3rd Party dApps:**
This subsystem deals with the deployment of the 3rd party dApps on top of Howdoo. This has been described in section 5.3.6.

→ **Server Operations:**
This subsystem comprises of functionalities which will be managed by a dedicated server, given the limitations of the blockchain technology. This subsystem has been presented in section 5.3.7.

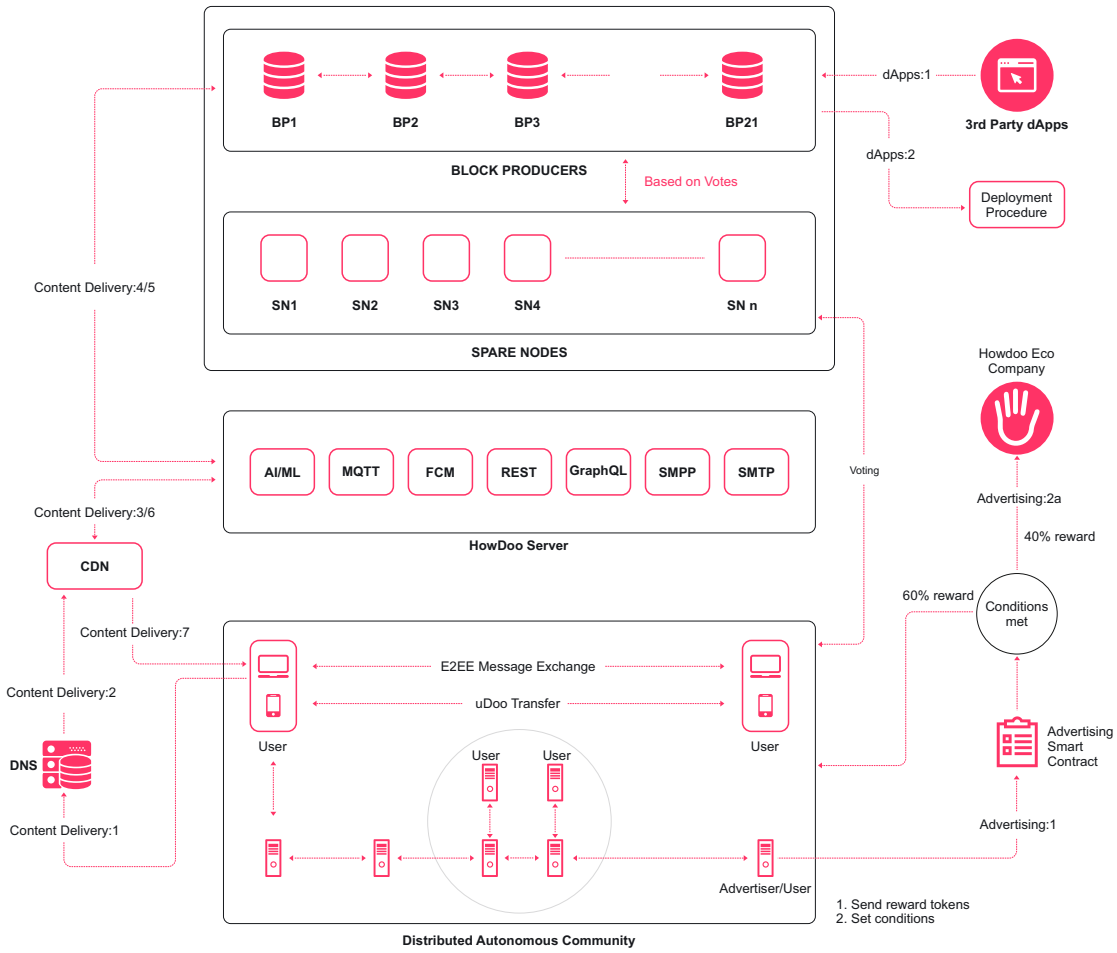
→ **Miscellaneous:**
This section covers a few other components which are an integral part of the Howdoo ecosystem. These have been detailed in section 5.3.8.

Howdoo aims to leverage the following modules/subsystems on the blockchain framework:

- Data Storage
- Adverts Delivery
- Content Delivery
- Financial Transactions
- Governance and Voting

The following will be implemented off the chain:

- MQTT
- GraphQL/ REST API endpoints
- Firebase Cloud Messaging
- SMS gateways
- Email gateways
- Web-socket Server
- ML/AI
- CDN



5.3 HOWDOO SUBSYSTEMS

5.3.1 Governance

This section details the concept of democratic leaders in Howdoo ecosystem, how they are elected, and how the decisions are made (consensus is reached). This subsystem can be visualized as an amalgamation of six sub-subsystems which have been itemized beginning from section 5.3.1.1 through 5.3.1.6.

5.3.1.1 Block Producer (Master Nodes)

Block Producers are the democratically elected leaders of the Howdoo ecosystem by a continuously ongoing election.

5.3.1.1.1 Minimum Requirements for being a Block Producer

Following are the minimum requirements for a candidate node to qualify for the Block Producer elections.

5.3.1.1.1.1 Public Presence

A public website URL and at least one social media account.

5.3.1.1.1.2 Public Information

Information to be made public includes:

- Official block producer candidate name.
- Location of company headquarters.
- Expected location of servers.
- Type of servers (cloud, bare metal, etc).
- Current employee list and pictures of at least 67% of staff (if managed by a team).
- Relevant background qualifications for at least 67% of staff (if managed by a team).

5.3.1.1.1.3 Technical Requirements
Minimum computational power required for the nodes to qualify as spare nodes.

- CPU with 24+ cores.
- 32+ GB RAM.
- 50+ TB Storage.

5.3.1.1.1.4 Minimum Stake
A node must hold 2,25,000 µDoo tokens to qualify as a block producer candidate, failing which it's candidature will be cancelled.

5.3.1.1.1.5 RoadMap
Values, community project timeline, finances, transparency, or any other topic the candidate deems important to be shared in a public post on any of the mainstream social media.

5.3.1.1.2 Proof of trust score
Proof of trust score for master nodes will be calculated as described below. A node will have to maintain a minimum network availability of 95 percent to be a part of the election process and also maintain this score throughout it's tenure as a block producer. The Proof of Trust rating is calculated periodically using the following equation:

$$\max(0, (N_t - 95)) * S + (G_t + O_t)$$

where,
t = Sampling period
N_t = Network availability for time period t (i.e. proportion of node uptime)
G_t = Storage coefficient (i.e. minimum gigabytes of storage made available to the network during time period t)
O_t = Processed operations coefficient (i.e. number of operations processed on behalf of the network during time period t)
S = Stake coefficient (i.e. the value of µDoo held in the node operator's wallet).

The proof of Trust score will also be visible to the user nodes in real time, so that they can decide to upvote or downvote a block producer.

5.3.1.2 Spare Nodes
The minimum requirements for block producers applies to spare nodes as well. A node can classify as a spare node (any number of contenders next in line for being block producers) only if they satisfy the minimum configuration requirements.

5.3.1.3 Infrastructure on Lease
It maybe difficult for everyone to manage a huge infrastructure with maintenance teams (as described in section 5.3.1.1). For making it easier for the interested parties to get involved in election process, Howdoo has teamed up with 3rd party vendors.
So people/organizations willing to enter the block producer elections, can pay the infrastructure providers to setup and manage the nodes for them.

5.3.1.4 Election Process
Continuously ongoing elections will begin when the Howdoo network goes live. The initial election period will end when 10% of the total Howdoo tokens in circulation have been staked (for voting purposes).

During the initial governance period, 21 Appointed Block Producers (ABP) will be chosen at random from the pool of candidates. Once the election period ends, the ABPs will be replaced with the elected Block Producers.

Each members' staked tokens will count as individual votes towards each of the Block Producers they have chosen. For voting purposes, tokens will need to be staked. Members can also delegate ("proxy") their voting power to others who can vote on their behalf. Proxied voters can outsource the decisions to trusted friends, exchanges, or community members.

Each Howdoo member can choose up to 10 Block Producer candidates per µDoo (1 µDoo is equal to 10 votes in the Howdoo elections). The candidates that receive the most votes will be those who will become the Block Producers. Votes can be changed immediately, but staked tokens will be locked for 3 days.

Elections will be ongoing and votes will be recalculated approximately every 2 minutes. It is possible that Block Producers will be changing as often as every few minutes.

5.3.1.5 Reward System

5.3.1.5 Reward System

Howdoo Block producer and Spare nodes are compensated accordingly for their continued efforts towards ensuring the smooth function of the Howdoo ecosystem. These nodes are incentivized as elaborated below.

Howdoo token economy will be subject to a 2.5% yearly inflation on a pro-rata basis. 2% of this 2.5% inflation amount comprises the reward system.

At any given time there are 21 active block producers and other spare nodes. The top 21 block producers will divide up the 1.50% per-block rewards proportional to the number of blocks each one produced on a daily basis. The top 21 block producers for the day will be the ones with the most number of Votes.

All block producers plus spare nodes will divide up the 0.50% per-vote rewards budget proportional to the total number of votes they receive, also to be divided on a daily basis. In order to claim this per-vote reward share, the nodes must qualify for at least 100 tokens/day. Nodes which do not qualify for at least 100 tokens/day on a per-vote basis are not entitled for any rewards for that particular day.

The idea behind this algorithm is to ensure all candidate producers have sufficient pay to provide full-node services to the community and to ensure no one is in the position of receiving money that is insufficient to cover their costs.

It is critical to have a minimum per-day payment so that wealthy individuals who have no intention of producing blocks don't attempt to earn interest on their producer candidate by voting on themselves.

5.3.1.6 Blockchain Upgrades

All upgrade decisions will be taken and processed by the 21 Block Producers, the process of which has been elaborated below.

A Block producers proposes a change to the constitution and obtains 15/21 approval.

B Block producers maintains 15/21 approval of the new constitution for 30 consecutive days.

C All users are required to indicate acceptance of the new constitution as a condition of future transactions being processed.

D Block producers adopt changes to the source code to reflect the changes in the constitution and propose it to the blockchain using the hash of the new constitution.

E Block producers maintain 15/21 approval of the new code for 30 consecutive days.

F Changes to the code take effect 7 days later, giving all non-producing full nodes 1 week to upgrade after ratification of the source code.

G All nodes that do not upgrade to the new code shut down automatically.

By default configuration of the Howdoo software, the process of updating the blockchain to add new features takes 2 to 3 months, while updates to fix non-critical bugs that do not require changes to the constitution can take 1 to 2 months.

5.3.2 Finance
This section details how the finances are managed in Howdoo ecosystem.

5.3.2.1 µDoo Wallet
The µDoo Wallet is a typical crypto wallet with some added functionalities. The private key of the Howdoo blockchain account for each user is stored on the client side itself to ensure that the complete control of µDoo remains in the hands of users. The user will also be able to provide their private keys in a mnemonic seed from (inspired from BIP39). A Hierarchical Deterministic wallet strategy is also put in place using the BIP32 protocol.

To initiate a transaction Howdoo web client will consume the private key from user's mobile/desktop storage and will create and sign a raw transaction which will include information about the transaction amount (in terms of µDoo), recipient of the transaction, sender of the transaction and nonce of the sender. Once a raw transaction is created, it will be broadcasted to the Howdoo chain.

The µDoo wallet will also provide options to join and create a multi signature wallet. Communities on Howdoo can create shared wallets and manage their µDoos by assigning owners among admins of the community.

Apart from these, the µDoo wallet will also help transact and maintain the tokens deployed on the Howdoo platform.

5.3.2.2 µDoo Token
The Howdoo network is fueled using its own cryptocurrency- µDoo. It functions as a vehicle for transferring value between users, advertisers, and operators of the Howdoo network.
Howdoo's own cryptocurrency will serve following functions:

- The µDoo tokens will reflect the participation of individual users.
- µDoo will reflect the share of all advertising rebates. It will be the medium for rewarding both users for engaging with featured content, and content creators for the traffic they generate.
- It will be the currency for advertising on Howdoo as the advertisers will be required to own µDoo for funding their campaign activities.
- The advertisers will use µDoo to bid for access to specific audiences and Communities.
- It will provide a form of value exchange to stimulate activity in the e-shops that will open on Howdoo.
- It will enable individuals with a high Proof of Contribution to set their engagement fee' in µDoos, which has to be met by anybody wanting to make contact with them– via the Howdrop messaging Function.
- The network operators will earn µDoo through the technical and financial services they provide to the network's users.

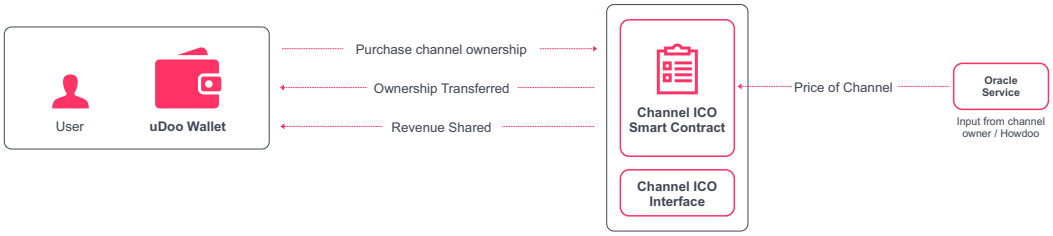
5.3.2.3 Multi token support
The Howdoo system will have a support for tokens built on top of it, similar to the way Ethereum hosts tokens. Howdoo has built on support for multiple ERC token standards. Some famous ERC standards which are already being considered for Howdoo token distribution are- ERC20, ERC223, ERC721 and ERC827. Some modifications might be made to these protocols to ensure a seamless integration with Howdoo blockchain. We currently do not have plans to support cryptos which are not part of Howdoo ecosystem.

5.3.2.4 Exchange
Howdoo has an internal exchange which would allow users to swap tokens or exchange them with µDoos. For each token pair a separate Howdoo dApp will be deployed so all the token pair exchanges could be executed parallelly and avoid order execution delays.
Token values on our exchange is pegged to the base currency µDoo, while swap rates between µDoo and other fiat currencies are available in the interface provided for the exchange. Exchanges will take place on a demand and supply basis, where Howdoo will increase/decrease the costs of the listed tokens based on these transactions. Therefore an increase in demand will result in a price hike and vice versa.

5.3.2.5 Howdo ICOs

Channel/community owners can raise funds by offering a share of revenue to other Howdoo users. The process is very analogues to how the ERC20 ICO tokens are bought, but the Howdoo wallet makes it simpler. These coins can only be bought using µDoo tokens. There is an internal exchange to trade channel tokens.

Dividends are automatically distributed to all channel coin holders automatically when the channel generates any profit.



5.3.2.6 Transactions

5.3.2.6.1 Fees

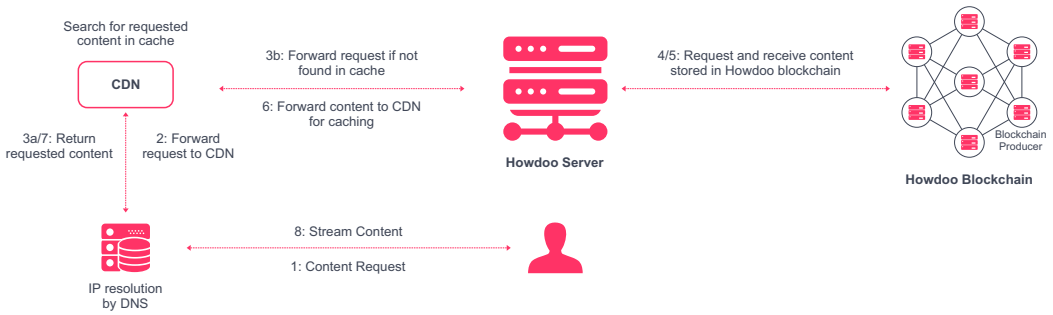
Unlike other blockchains like Ethereum & Bitcoin, Howdoo does not have any transaction fees. Spamming is controlled by the bandwidth available to every account on the network which is proportional to the µDoos in the account balance. If an account holder disobeys this limit set on their account's bandwidth, the Block Producers are within their legal rights to reject that transaction.

5.3.2.6.2 Micropayments

Howdoo platform opens doors for the content creators to be rewarded for their work. The content consumers can tip the content creators if they wish to (Similar to liking a post with few tokens as appreciation)
The µDoo token can also be used for multiple purposes like making payments, transfering money etc.

5.3.3 Content Delivery

Howdoo deploys its own Content Delivery system. To minimize the distance between the visitors and the main content hosting server, a CDN stores a cached version of its content in multiple geographical locations (a.k.a., points of presence, or PoPs). Each PoP contains a number of caching servers responsible for content delivery to visitors within its proximity.
In essence, CDN puts the content in many places at once, providing superior coverage to the users.
In Howdoo's platform, whenever client requests for a media, the CDN will look for it in its cache. If the content is stored in a cache, the content would be served directly from the CDN; otherwise, the CDN will request the content from the Howdoo server, which in turn will get it from the Block Producer nodes.



5.3.4 Adverts

Adverts are an integral part of the Howdoo ecosystem and this section elaborates on the same.

5.3.4.1 Adverts Overview

Howdoo is not a typical ad-based revenue system; rather, the Howdoo Adverts model is based on the principle of mutual benefits wherein both the advertiser as well as the viewer will be incentivized for their participation.

5.3.4.2 Howdoo Adverts' Features

- A user will be able to set their profile to either Full Stealth, Community, Open Borders or Professional Mode depending upon the type and extent of advertising that he/she is ready to consume which can be changed anytime.

- Communities can decide to welcome advertisements, in which case the advertisers will then compete to display their messages through either a Cost Per Click (CPC) or Cost Per Thousand Impressions (CPT) bidding process, much like the auction system of Google AdWords.

- Users and communities also have full control over the personal data they wish to expose to advertisers, and what information they make available for use in demographically targeted advertising campaigns that generate a share of available rebates.

- Advertisers are able to find demographics and communities to target by searching against community keyword tags. They also have the ability to see the full set of preferences of any given community before deciding whether to bid, as well as visibility of a community's KPIs in order to determine if it represents an attractive advertising opportunity. Wherein KPIs consist of

    - Membership metrics, e.g. number of members, average length of membership, growth rate, etc.

    - Proof of Contribution metrics, e.g. posts per day, percentage of active versus inactive members, average number of replies, etc.

    - Previous campaign metrics, e.g. impressions per day, click-through rate, etc.

5.3.4.3 Incentivization Model for users and communities

Using the Howdoo AdAuction application, advertisers will be able to purchase µDoo in their wallets and set bidding limits for acquiring personal and community advertising space which will be distributed to viewers and Howdoo company on fulfilment of the contract rules. The sharing ratio will be based on a 60/40 rule (60% to the community and 40% to the Howdoo ECO Company).
AdAuction will be distinct from the main client application to ensure the process does not interfere with the core experience of the community network.

5.3.4.4 AI Engine for Adverts

The AI layer will interact with the Storage layer and Service layer to deliver the relevant advertisements to users/communities based on the

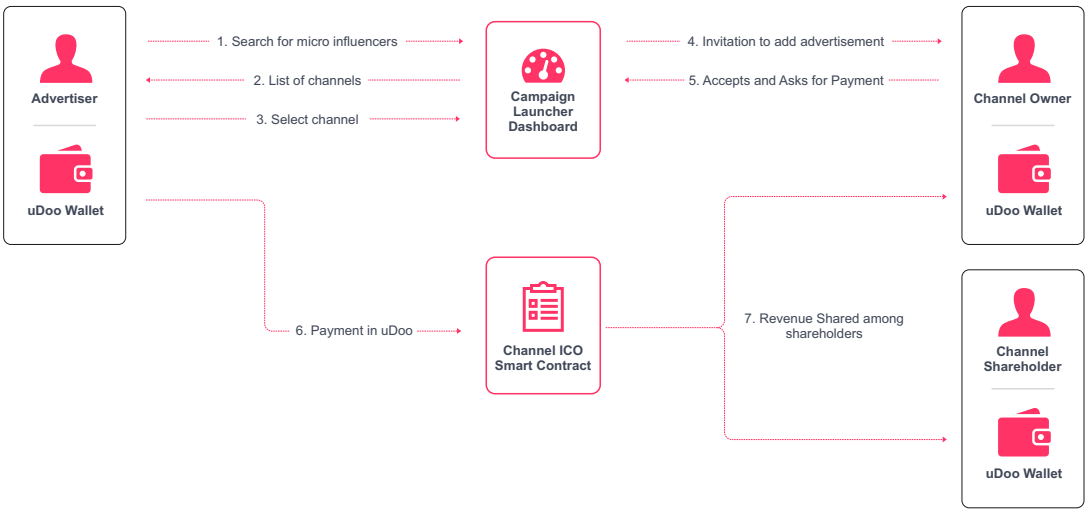
- Keywords selected / blocked by the users / communities in the ad preference forms filled out when they choose to consume adverts.

- The mode that a profile is set to (Full Stealth, Community, Open Borders or Professional Mode).

5.3.4.5 Advertisement Campaign Platform

It helps in searching for appropriate channels for their advertisement on Howdoo platform with the help of Campaign Launcher Dashboard. The figure below explains all the steps.

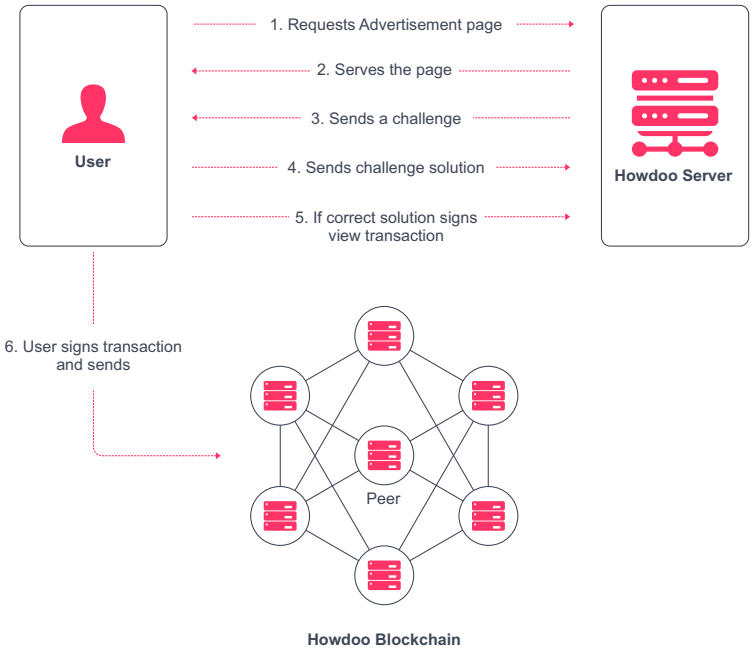
The dashboard will have the features needed to find the right audience. The below diagram describes how a campaign works with a channel of a micro-influencer where the channel has already sold its shares to raise funds.



5.3.4.6 Fake Views Prevention

To mitigate the possibility of Bots consuming the Adverts, the server sends a challenge to the Advert consumer which a Bot can not solve. If the challenge was resolved on the client side correctly, the server signs a confirmation message and sends it to the user. The user signs this message, and it is recorded on the Howdoo blockchain affirming the advert consumption. Via this mechanism, the advert providers can audit the advert consumption on blockchain by validating the Advert consumer and challenge resolution recorded by Howdoo server.

The advert challenges are made in a manner such that they do not interfere with the user experience on Howdoo platform.



5.3.5 Messaging

5.3.5.1 Messaging System

Howdoo supports P2P messaging platform which

- Is end to end encrypted
- Has a UI similar to existing IM services.
- Has support for emojis.
- Has encrypted group chats
- Has support for end to end encrypted voice and video calls

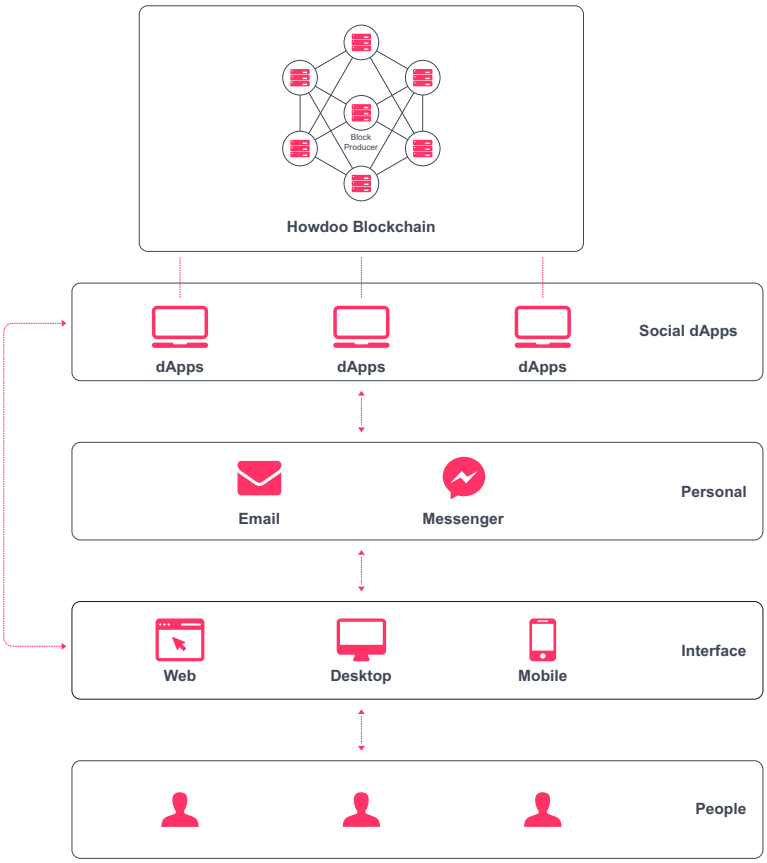
5.3.5.2 Message Privacy using Signal Protocol

The messages are end to end encrypted using the Signal protocol.
Implementing end-to-end encryption in a messaging service means that the contents of any given message are only available to the sender and the intended recipient.

Without E2EE, the message may be encrypted while it's being transmitted to the server, but the server might be able to read it. For example, some service providers might do this to generate ads that are more specific to a user.
With E2EE, the message is always in an encrypted state while it makes its way through any possible intermediaries. No one except the intended recipient has the key to decrypt it. With a good E2EE protocol, neither intermediaries (messaging app server, database), nor anyone with malicious intents would be able to read the messages.
Signal uses Curve25519, AES-256 and HMAC-SHA256 when handling messages. The security of these algorithms has already been battle tested.
The Axolotl ratchet in Signal is the most advanced cryptographic ratchet available. Axolotl ensures that new AES keys are used for every single message, and it provides Signal with both forward secrecy and future secrecy properties.
Signal's protocol suite also features enhanced deniability properties that improve on those provided by OTR, except unlike OTR all these features work well in an asynchronous mobile environment.
Howdoo will use the Axolotl and TextSecure protocols in Signal that represent the current state of the art in secure messaging.

5.3.6 3rd Party dApps

3rd party vendors will be allowed to host their dApps and tokens on Howdoo platform but in a restrictive and controlled manner.
As mentioned in section 4, Howdoo will provide a set of APIs that can be used by 3rd party dApp developers to leverage the inbuilt functionalities of the platform and construct a solution for their own specific use cases.
These APIs would be designed in a manner that they do not compromise with the security and scalability of the platform, but at the same time give enough functionalities to dApp developers to build rich and interactive applications on top of the platform.

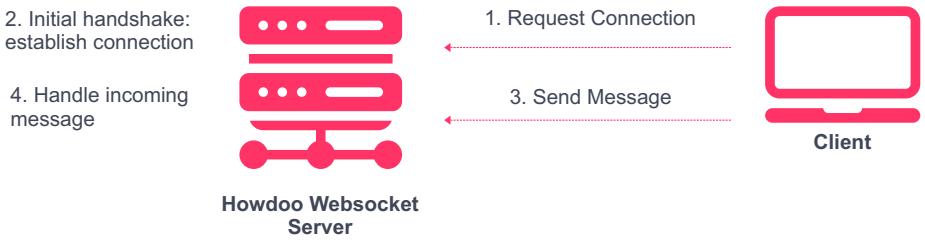


5.3.7 Server Operations

Features that do not require immutability, transparency or consensus are taken off chain in the Howdoo platform. Howdoo Server will be responsible for ML/AI, MQTT, GraphQL, REST, SMS Gateways, FCM and SMTP operations.

→ **MQTT**
Howdoo will utilize MQTT for real time communication between mobile device and the server, for operations like transmitting realtime encrypted chat messages or realtime feed update notifications. This isn't a replacement of push notifications but a functionality to be used alongside. The push notifications cannot be used to transmit large amount of data on mobile devices where MQTT comes into action.

→ **Websocket Server**
The following diagram illustrates the communication process between a Websocket server and a Websocket client, emphasizing the triggered events and actions. Websockets will handle real time communication between the browser and the server, for operations like realtime feed updates, just like MQTT on mobile device end. Also Websockets will be exposed to IPs of Howdoo platform consumers. This data is not exposed to the Block Producers of Howdoo ecosystem.



→ **ML/AI**
Machine Learning and Artificial Intelligence operations will be applied on the datasets of Howdoo users to organize users into proper target groups, so that advertisers can reach out to their intended audience easily and both users and advertisers can benefit from it, by getting a share of the reward µDoo set by the advertiser. Also data for these target groups will be fetched in a compliant way by accessing data for only those users who agree to provide it to Howdoo eco company. This data will not be shared with the advertisers, who will only be able to access strategic data, through which individual users cannot be identified. Howdoo uses a proprietary matching ML model for processing of user data and fake view elimination.

→ **FCM**
It will be used for PUSH notifications within the Howdoo ecosystem. FCM is necessary because device IDs of the Howdoo users and credentials of the Howdoo FCM account on google cannot be shared with the Block Producers.

→ **REST APIs and GraphQL endpoints**
Several API will be exposed to consume and interact with different services using REST and GraphQL within the Howdoo network. They're necessary because many services explained in this section are handling sensitive/private information about the user's device, location, credentials etc. Also, these services need to interact with each other, which requires a REST and GraphQL based framework to function in a faster and sustainable manner.

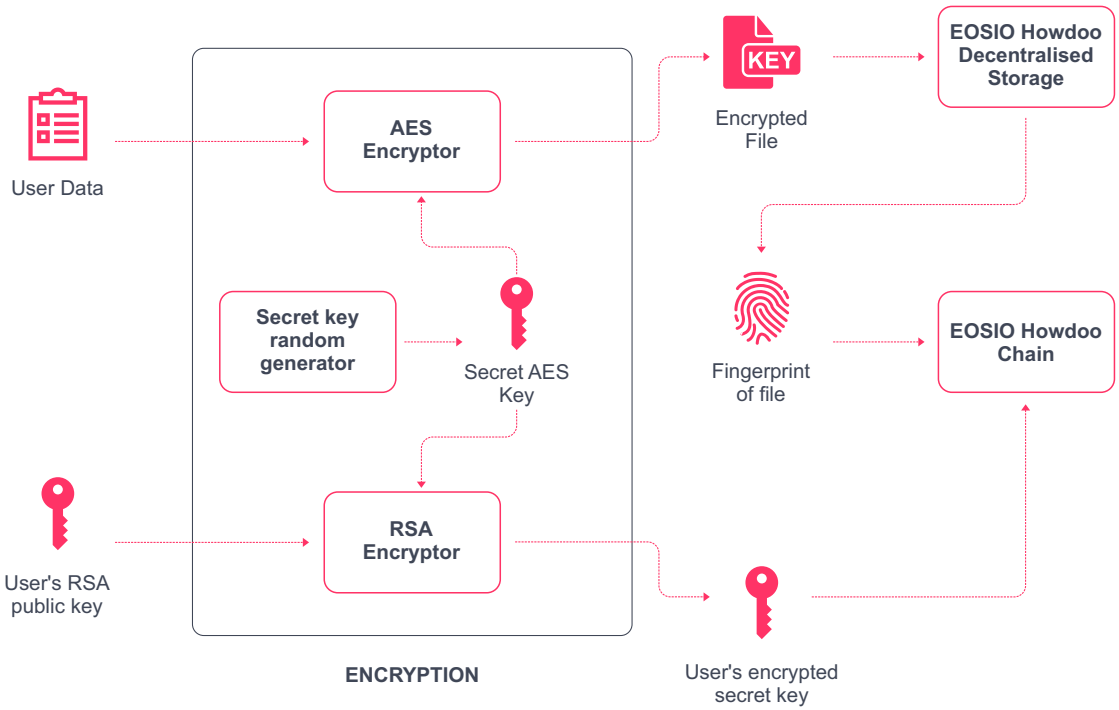
→ **SMTP**
Howdoo network will utilise SMTP for email notifications. This setup will contain email server credentials of the Howdoo network, which has to be kept off chain to safeguard this information from Block Producers.

→ **SMS gateway**
SMS gateways will be utilized for sending and receiving SMS alerts to Howdoo users' registered mobile numbers. The data in alerts can include credentials and personal unencrypted chat messages, which should not be shared with Block Producers.

5.3.8 Miscellaneous

5.3.8.1 Data Privacy
User data is encrypted in a manner that only he/she can access it using their private key. Data is encrypted with AES encryption and these encryption keys will be encrypted with users' public key. Encrypted AES keys are stored on the Howdoo blockchain.

To access the data, user has to fetch encrypted AES keys from blockchain, decrypt the keys, fetch the data and decrypt it with AES keys.



5.3.8.2 Inflation Economic model

Of the 2.5% inflation each year, the division will be as follows

5.3.8.2.1 Reward System

1.5% of the inflation funds will be distributed as detailed in section 5.3.1.5.

5.3.8.2.2 Future Worker Proposal Funds

The remaining 0.5% will be stacked for future development with the Howdoo ECO company, distributed or burnt based on user voting.

5.3.8.3 Ethereum ERC20 Tokens Migration to Howdoo Blockchain

Since data cannot be transferred from one chain to the other directly, Howdoo will be deploying a new Token Migration contract on Ethereum. This takes tokens from all the existing users and records this data (user address and corresponding tokens) in the TokenMigration contract. The TokenMigration contract will not have any token transfer function, ensuring that once the tokens are transferred to this contract they will be locked at their destination forever (which will be equivalent to burning these tokens). Before we launch our public Howdoo blockchain mainnet, we will invite ERC-20 token holders to exchange their tokens (migrated to the Howdoo blockchain) via a portal that will follow these steps:

A Howdoo will launch its own blockchain wallet by the time it launches its token exchange portal. User will first generate address of new Howdoo blockchain and keys on this wallet.

B Users will approve the TokenMigration contract to transfer the amount of tokens they want to migrate to the Howdoo blockchain mainnet.

C Users will register their new Howdoo blockchain address on existing Ethereum public blockchain by making a transaction on a Ethereum smart contract deployed by Howdoo. By this Howdoo gets a recorded consent from the existing ERC-20 Token holder about their new Howdoo address.

D Now the users' tokens get transferred to the TokenMigration contract and they are locked.

E The amount of tokens locked in the contract will be credited to the respective user's account on the Howdoo blockchain's mainnet.

6 Solving the technical Roadblocks

The section 4 specifically states the end result of an extensive research which is expounded in this section. Following are the options which were considered for implementing the Howdoo system.

6.1 CONSENSUS

All blockchains are fundamentally a deterministic state machine acted upon by transactions. Consensus is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. In simple words it is the process of agreeing on a deterministic order of transactions and filtering invalid transactions.
Below is a list of the most widely accepted consensus mechanisms along with their pros and cons.

6.1.1 Proof of Work

In PoW consensus mechanism hordes of miners compete with each other, trying to solve a cryptographic puzzle which requires (computational) work to be done before block submission. This means that, in order to mine a block, the block producer have to spend computational power/energy, along with the other contenders who were trying to produce a block.

As the time passes & the system grows, this computation becomes more and more complex. With this grows the requirement to keep on upgrading hardware to produce blocks faster. All the mining nodes compete to produce blocks and the node to come up with the block first wins and gets incentivized.

→ **Benefits of PoW Consensus**

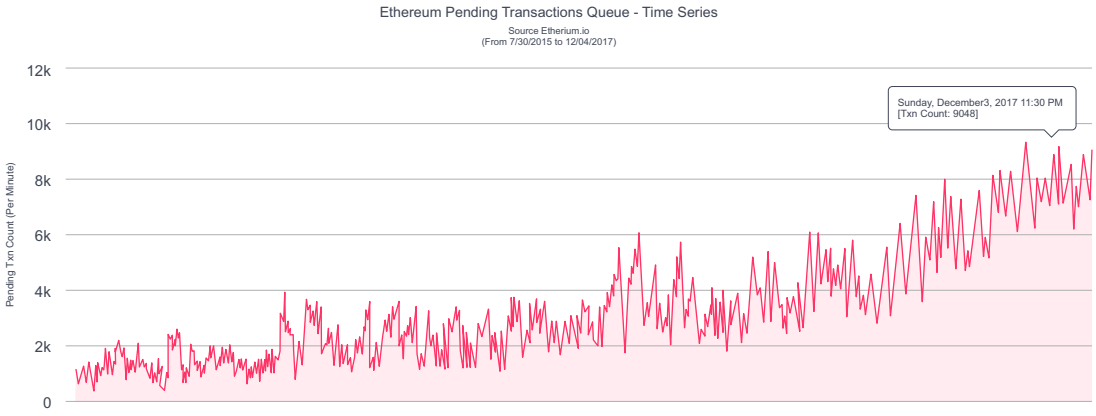
POW consensus mechanism has been widely adopted and is argued to be the most decentralised consensus mechanism by many. This consensus mechanism is utilized in the two major blockchain projects- Bitcoin and Ethereum.

→ **Drawbacks of POW consensus**

- POW based mining mechanism requires extensive power. Bitcoin mining, a once harmless practice that could be performed from any regular desktop computer is now a billion dollar industry with an estimated consumption of 288 megawatts, according to data from the Global Cryptocurrency Benchmarking Study by the Cambridge Judge Business School.
  The continued growth of cryptocurrency mining is not only affecting our environment, it is also harming cryptocurrencies themselves by promoting centralization and industrialization.

- It is quite a full-proof consensus mechanism for large distributed systems but the same use of computational power can prove fatal for the system if overloaded with transactions.
  For instance CryptoKitties- an online cat breeding game built atop Ethereum, which is currently the most used contract on the Ethereum network, making about 12 percent of the network's transactions. It's popularity is now clogging the network due to the sheer number of transactions produced by the game.The game is designed to encourage many small transactions, eventually making the blocks 100 percent full. The pool of pending transactions is already in the range of 16-17,000 and is rising.
  If this game is here to stay, then it can choke Ethereum completely by forcing users to set higher gas prices or miners to settle on another massive increase in the default gas limit. Below graph demonstrates the rise in the pending transactions.

  This wasn't the first time when the throughput of Ethereum's network was seriously tested. The Status ICO launch and several other events have pushed the network to its limit and caused transaction delays lasting hours and even days.



- Bitcoin validates transactions using a Proof of Work consensus algorithm. In the context of PoW blockchains, the hasrate is the speed at which a computer is completing an operation. A higher hash rate increases the opportunity of finding the next block and receiving the verification reward, thus, the mining pools with the highest hashrates are the ones verifying the most transactions. Following data was obtained during a period of 24 hours :

Pool	Hashrate	% of network hashrate	Location
BTC.com	8.53 EH/s	28.57%	China
AntPool	5.17 EH/s	17.29%	China
SlushPool	3.14 EH/s	10.53%	Czech Republic
BTC.TOP	2.47 EH/s	8.27%	China
F2Pool	2.25 EH/s	7.52%	China

The conclusion is quite straightforward for this case. Bitcoin mining is practically centralized. A group of mining pools control most of the network's hashrate, and they are mainly based in China. This raises immediate concerns. Miners secure the network and give validity to Bitcoin. A high percentage of hashrate, or a possible alliance between pools, could increase the risk of a 51% attack (ref).

6.1.2 Proof of Stake

Proof of Stake (PoS) is another consensus mechanism like PoW but instead of requiring work or computational power, it requires the miners to hold a certain amount of the cryptocurrency. Let's say cryptocurrency "stackcoin STC" relies on Proof of Stake, and that Bob owns 2% of all of the STC in existence. This implies that the probability of Bob mining a proof-of-stake block is 2%.

→ **Benefits of PoS consensus**

- Proof-of-stake based systems consume less computational power as opposed to POW based systems.
- These generally have increased throughput compared to PoW based systems.

→ **Drawbacks of PoS consensus**

POS mechanism is comparatively less resource hungry than POW mechanism but it suffers a few fundamental flaws in the design part itself.

- The consensus mechanism only takes in account the individual's stake for choosing Block Producers while their credibility and capability is unaccounted for.
- The individuals with stakes falling in the lower half of the token distribution spectrum have negligible chances of becoming block producers themselves and also have no say in deciding who gets to produce the blocks.
- Many PoS implementations have a minimum staking price, ultimately sacrificing their extent of decentralisation.

6.1.3 Delegated Proof of Stake

The DPOS algorithm is divided into two parts: electing a group of block producers and scheduling production. The election process makes sure that stakeholders are ultimately in control because stakeholders lose the most when the network does not operate smoothly. Although how people are elected has little impact on how consensus is achieved on a minute by minute basis.
A DPOS system can have N number of block producers (selected by the stakeholders, where the votes are weighed using the stakes) and the consensus requires ⅔+1 majority to resolve.

The block producers produce the block in their delegated time slot, in a pre decided order. This order though is randomized every N slots, so that a block producer say 'A' doesn't always ignore block producer 'B' and that anytime there are multiple forks of identical producer counts that ties are eventually broken.

Delegated Proof of Stake is robust under every conceivable natural network disruption and even secure in the face of corruption of a large minority of producers. Unlike some competing algorithms, DPOS can continue to function even when a majority of producers fail (ref). During this process the community can vote to replace the failed producers until it can resume 100% participation.

Ultimately DPOS gains significant security from the algorithms chosen to select the block producers and verify that the nodes are of high quality and unique individuals. Using the process of approval voting ensures that even someone with 50% of the active voting power is unable to select even a single producer on their own.

Just like a democracy, the system works better and becomes more decentralized/fair aa more people participate and are informed. Additionally, there is no minimum stake for users, thereby expanding the participation among blockchain users.

→ **Benefits of DPoS over other consensus mechanisms**

- Since the nodes are elected to produce Blocks and get paid for the services, they need to be consistent on stability and up to date with the hardwares to hold their position and be competitive to other candidates to be elected.
- Delegated Proof-of-Stake offers advantages over the most well-known consensus algorithm, Proof-of-Work (PoW). These advantages include savings on energy costs, being faster, efficient, and more democratized.
- Though theoretically POW/POS are more decentralized, practically DPoS is found to be more decentralized than other consensus systems because the threshold to enter the consensus is very low. Other alternatives theoretically "allow" anyone to enter, but most individuals are excluded from entering the consensus due to high costs/needs, and generally a few pools or large miners produce all blocks on those systems.

→ **Drawbacks of DPoS consensus**
Critics of DPoS argue that, by concentrating the role of validation in a smaller number of hands, it is less decentralized and less resilient.

BFT-DPOS
Byzantine Fault Tolerance can be added to traditional DPOS by allowing all producers to sign all blocks so long as no producer signs two blocks with the same timestamp or the same block height. Once a ⅔ majority is reached (i.e. they have signed a block), the block is deemed irreversible. Any byzantine producer would have to generate cryptographic evidence of their treason by signing two blocks with the same timestamp or blockheight, this proof can be used to punish him. Under this model a irreversible consensus should be reachable within a few seconds in ideal situation.

6.2 BLOCKCHAIN SCALABILITY TRILEMMA

The trilemma advocates that a blockchain can only have at most two of the below mentioned three features.

→ Decentralization

→ Scalability

→ Security

Every blockchain has compromised with one of these in their solution. We can compare Ethereum, EOS and Ripple here to understand this in a better way. Ethereum chooses theoretical decentralisation as well as security, but lacks in scalability. Ripple is one of the most scalable and secure blockchains, but is not decentralised. While EOS is quite scalable and secure but is argued to be theoretically less decentralised.

6.3 BLOCKCHAIN SOLUTIONS

Following blockchain solutions were considered for implementing the Howdoo ecosystem:

6.3.1 Ethereum based solution

Howdoo application was initially planned to be implemented on the public Ethereum blockchain along with it's ERC20 token.

6.3.1.1 Key Properties

- Mass adoption
- Extensive documentation and Developers' community.
- Smart Contract enabled.
- A high level language which would have made it appropriate for this use case. Also, other features related to economy were planned to be implemented using the Ethereum smart contract.

6.3.1.2 Drawbacks

- As of now ethereum is mainly based on Proof of work consensus mechanism which is quite resource hungry.
- Because of the roadmap, there are some major upgrades coming down the line for Ethereum, including moving the platform from Proof of Work to Proof of Stake. If this transition does not go smoothly, it could introduce some critical issues in the architecture and cause the system to crash.
- Given the traditional architecture of the EVM and the extensive computational power required because of POW consensus mechanism, the overall throughput of Ethereum network is extremely low and thus the applications running on it face similar issues.
- Ethereum consumes gas for producing transactions, meaning one needs to spend money for simple operations on Ethereum based dApps which result in a state change within the smart contracts.
- Resource hungry and populated blockchains like Ethereum won't be able to fulfil data storage requirements needed by a social media platform like Howdoo.

6.3.2 NEO based solution

NEO is a blockchain project that aims to utilize blockchain technology and digital identity to digitize assets, to automate the management of digital assets using smart contracts, and to realize a "smart economy" with a distributed network.

6.3.2.1 Key properties

- Smart contract capabilities.
- Throughput claim of upto 10,000 TPS.
- Consensus is dBFT (distributed Byzantine Fault Tolerant) - very similar to DPoS, except all transactions are final (no forks).
- NEO supports a wide variety of commonly used programming languages such as Javascript and C++ by using a customized version of Docker called neoVM that compiles the code into a secure executable environment.

6.3.2.2 Drawbacks

- Semi-decentralized asset exchange : Transaction settlement happens on the blockchain, but the process of matching orders occurs off-chain, by a central exchange that provides matching services.
- No decentralised storage facility provided which is an integral part of Howdoo.
- Neo has scalability issues as well, practical situation is far off from theoretical. This was highlighted when an ICO was hosted on NEO, it took 4 minutes instead of 30 seconds to add a block.(ref).
- NEO is mainly created to digitize assets, which is not the specific use case for Howdoo ecosystem.

6.3.3 State Channels (Raiden Network) based solution

A state channel is a two-way communication channel between participants which enable them to conduct interactions off the blockchain, which would normally occur on the blockchain. This decreases the transaction time exponentially since you are no longer dependent on a third party (like a miner) to validate your transactions.

6.3.3.1 Key Properties

- Microtransactions are completely off chain and final result is settled on main Ethereum chain. This reduces load on the main chain. 1000s of microtransactions can be settled through only 2 transactions on the main chain.
- Network of these channels will make Raiden even more scalable.
- Ethereum smart contracts support.

6.3.3.2 Drawbacks

- Raiden network is not implemented yet. Only MicroRaiden has been implemented which is a simpler version of Raiden network. MicroRaiden is not suitable for our aim as a user will not create a new channel each time they want to upvote and make a microtransaction. This problem will be solved only after Raiden Network is implemented.

6.3.4 DAG based solution (Byteball, IOTA)

Blockchains are single Linked Lists - common data structures where each new entry (block) includes a reference to a previous one. DAG is an implementation of Graph, and it allows the networks using it to circumvent some of the blockchain's most daunting limitations. In DAGs, all the nodes are pointed in the same direction.

6.3.4.1 Key Properties

- High transaction throughput. More the traffic on a network more it scales as it is not a blockchain, instead it is based on the concept of DAG (Directed Acyclic Graph).

6.3.4.2 Drawbacks

- No smart contract capabilities in IOTA till now. Byteball supports very primitive smart contracts which are not turing complete.
- Both of these are centralised right now and have never been tested in high traffic.

6.3.5 LISK based solution

Lisk aims to provide a blockchain solution where developers can build and deploy blockchain applications using JavaScript.

6.3.5.1 Key Properties

- Each blockchain application runs on a separate side chain to main LISK chain. This sidechain can be customized as per need. Can have any consensus algorithm it wants i.e. consensus algorithm can be customised.
- DPOS with 101 delegates is the consensus mechanism.
- Theoretical throughput of 1000Tx/sec.

6.3.5.2 Drawbacks

- In development phase right now. Current throughput is 3-5 tx/sec and only by the end of 2018 it hopes to achieve up to 1000 tx/sec.
- They claim that virtual machine for smart contracts can be implemented on one of the side chains but no one has implemented it successfully.
- No decentralised storage facility provided which is an integral requirement for Howdoo dApp.

7 Conclusion

We have proposed an architecture that incorporates a full-fledged social media platform along with an electronic payment transfer system without relying on a trusted third-party vendor.
We started with the usual framework of social network and electronic cash transfer system made from digital signatures, which provides strong control of ownership, but suffers from innumerable flaws.

To solve this, we proposed a peer-to-peer social media network built utilizing the EOS platform and extending it to support our custom feature set.

The network is robust in its unstructured simplicity. Nodes work all at once and can leave and rejoin the network at will. Any needed rules and incentives can be enforced with the mentioned delegated proof of stake consensus mechanism. With µDoo token ownership, users also gain the ability to operate SuperNodes and Virtual Nodes (requiring 1.5 million and 125 thousand µDoo tokens, respectively).

Howdoo has an anticipated launch of Summer 2018 and will roll out the various elements of its ecosystem in phases. Currently, µDoos are available for purchase as part of Howdoo's initial coin offering (ICO). Individuals interested in learning more are encouraged to visit www.howdoo.io and participate in the ICO.

Glossary

Howdoo ecosystem Philosophy
The fundamental principle behind the Howdoo ecosystem is that, all the participants should be financially motivated to behave responsibly and share value with each other.

µDoo Token
The Howdoo network is fueled using its own cryptocurrency- µDoo. It functions as a vehicle for transferring value between users, advertisers, and operators of the Howdoo network.

Distributed Autonomous Communities
Any user of Howdoo can set up a community. These naturally differ in scale and privacy levels depending on the intention of the creator – from private groups between close friends and family members to vast, borderless collection of people who share a common interest.

Howdoo ECO Company
At the highest level, the Howdoo ECO Company is the one that maintains responsibility for supporting the Howdoo ecosystem, and for ensuring that the platform's development stays aligned to the objectives as laid out in this whitepaper.

Democratic Moderation
The communities are self-moderating as there is minimal moderation from the Howdoo ECO Company or any other central party.

Proof of Contribution
Each individual user and community member have a Proof of Contribution rating – a continuously evaluated score that defines the permissions, access rights and entitlement to community earnings for that member.

All the user nodes are subject to a periodically calculated Proof of Contribution rating as mentioned in section 3 which is calculated as follows,

The Proof of Contribution rating is calculated using the following equation

$$\max(0, E_1(R_1 - D_1)) * S + \sum_{n=2}^{6} E_n(R_n - D_n)$$

where,
n= The week number from 1 (previous week) to 6 (six weeks ago)
E_n=Engagement coefficient for week n (e.g frequency of posts, community reach)
R_n=Reputation coefficient for week n (e.g. up/down votes, likes)
D_n=Disruption coefficient for week n (e.g. messages flagged as inappropriate, messages removed)
S= Stake coefficient (i.e. the value of µDoo held in the user's wallet)

Transactions
The Howdoo platform also enables individual users to transfer money to each other, either as a standalone payment or as a single leg of a purchase transaction. Providing this service and making it independent of traditional banking facilities enables Howdoo to cater both banked and unbanked users.

MQTT
MQTT stands for MQ Telemetry Transport. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The design principles are to minimise network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal of the emerging "machine-to-machine" (M2M) or "Internet of Things" world of connected devices, and for mobile applications where bandwidth and battery power are at a premium.

Websocket server
A Websocket server is a simple program, which has the ability to handle Websocket events and actions. It usually exposes similar methods to the Websocket client API and most programming languages provide an implementation.

FCM
FCM stands for Firebase Cloud Messaging, it is a cross-platform messaging solution that lets you reliably deliver messages at no cost. Using FCM, you can notify a client app that new email or other data is available to sync. You can send notification messages to drive user re-engagement and retention. For use cases such as instant messaging, a message can transfer a payload of up to 4KB to a client app.

REST
REST leverages less bandwidth, making it more suitable for internet usage. A RESTful API breaks down a transaction to create a series of small modules. Each module addresses a particular underlying part of the transaction. This modularity provides developers with a lot of flexibility.

GraphQL
GraphQL, is a query language for APIs and a runtime for fulfilling those queries with your existing data. GraphQL provides a complete and understandable description of the data in your API, gives clients the power to ask for exactly what they need and nothing more, makes it easier to evolve APIs over time, and enables powerful developer tools.

SMTP
SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port. After successfully establishing the TCP connection the client process sends the mail instantly.

SMS gateway
An SMS gateway allows a computer to send or receive Short Message Service (SMS) transmissions to or from a telecommunications network. Most messages are eventually routed into the mobile phone networks. Many SMS gateways support media conversion from email and other formats.

References

1. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#eosio-technical-white-paper-v2
2. https://medium.com/eosio/introducing-eosio-dawn-4-0-f738c552879
3. https://medium.com/eosio/eosio-dawn-3-0-now-available-49a3b99242d7
4. https://etherscan.io/chart/pendingtx
5. https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper
6. https://medium.com/@poolofstake/pow-vs-pos-showdown-which-is-more-centralized-aaa01c8052b3
7. http://storeofvalueblog.com/posts/neos-secret-scaling-issues/