RESPECTONOMY

A Decentralized Social Network

Third draft

tbolt256@respectonomy.com

Motivation

An opinion held about someone acts as proxy for our brain to judge the quality of the content they will produce. Reputation is thus, what social networks aim to simulate.

Problems with existing systems

Voting-based social networks, such as Hacker News and Reddit, allow pseudonymity and measure this reputation earned based on votes but the karma earned cannot be carried forward or used. Systems like Stack Overflow thus try to build an economy around the content and reputation information generated by its own users.

Contrary to these are systems like Facebook and Twitter that emphasize reputation by attaching it to the real world identity of the user. The partial system of measuring reputation, such as likes collected, are not usable either. Further these systems are proprietary in nature, locking in the data that users produce and selling off users attention.

Blockchain entrepreneurs have understood these problems and have made various attempts at trying to solve these problems by decentralizing various aspects of publishing.

Systems such as ChangeTip and ZapChain have tried to award bitcoins instead of votes. But users of such systems want to earn more than they want to spend. Economic activity dies down over time - both of these systems are now closed. A similar project, Yours, is yet to launch but it seems that it will face the same problem.

Others tried to decentralize the data-storage aspect of publishing by attempting to store data on the blockchain such as Alexandria, or using distributed databases such as Akasha that uses IPFS, whereas some like Steem use both. In such systems users bear the burden of storing data for using the system since fee analysis shows that blockchains are not free databases.

Furthermore, systems like LBRY, Decent, JoyStream use bittorrent protocols to distribute content to be hosted by the users and lets others charge for it. Although this is better than storing data on the blockchain, yet still run into storage issues over time. But an even bigger problem in such systems is determining the price that must be paid for a content.

Existing Solutions

The bitcoin protocol offers a solution to this issue by providing a valuable lesson that the price of a rare token can be determined automatically with the free market trade and provides a mechanism to create such tokens.

Most of the systems described above and others, all have their own blockchains with unique coins that does help determine the true value of these systems as percieved by the free market. The problem then, is with the distribution of coins created.

All proof-of-stake based blockchains face this problem while even some proof-of-work systems use tactics to mine unfairly. Some have even gone as far as to publicly admit accumulation of coins to be distributed to content creators effectively reducing these systems to a ponzi scheme for investors.

A transparent proof-of-work blockchain based content publishing platform that uses distributed data -storage can work out. But the distribution of coins still affects these systems because a fair mechanism for content-ranking and reputation measurement is required and distributed storage might still run into censorship problems with controversial data. Some systems try to build liquid- democracy based systems but a system with delegates runs into problems with minority representation. Others try to distribute reputation based on various aspects of the social graph but the edges on someone's social graph are binary someone is your friend or not which cannot represent the weight . Systems such as Synereo assume a centralized method for forming social graphs (while having other problems with identity and coin-distribution as discussed earlier.)

Respectonomy's solution

Respectonomy modifies the bittorrent protocol to only host content with users that endorse it; when users 'share' a content they become a seed in a sub-network of only those respectonomy users that have shared that content. Thus, only the supporters of a content bear the burden for hosting it.

While downloading from someone, a user can see descriptions to other files that the uploaders might be hosting and thus this sub-network also acts as recommendation engine by measuring the frequency and nearness of other data, and because content downloading is paid for, the seeds act as curators. The 'shared content then becomes a locally hosted curated list which the users earn from by hosting. To fairly determine the price for such exchange respectonomy deploys its own blockchain where the flow of the token 'respect dynamically determines the value of content exchange. This mechanism of tracking data in an isolated network helps fight censorship by replicating the data globally and data being available until anyone in the world is willing to host it.

Respectonomy server in itself is just a mining pool, which others can freely clone and run, and the system has no concept of a signup. The code is completely browser based that connects to other browsers without a central server and performs all actions based on user's addresses being tracked on a blockchain. All activities are observed via monitoring transactions which makes it expensive to spam and troll due to network fees and offloads the problem of controversial content to the discovery problem. Thus controversial content remains hosted on its isolated sub-network and someone has to discover it and willingly download it by paying for it. This is also necessary because what is controversial for a majority might be necessary for a minority. The site mines just enough ‘respect’ such that its expenditure introduces a built-in latency that does not affect humans but charges the bots to tap the firehose.

Respectonomy provides a layer for anyone to build bots on, that can crawl user’s data by paying them for it and bots can earn by providing services. Advertisers then effectively become special kinds of bots that instead pay users to modify their hosted data. This has an added benefit that ads always appear as recommendations rather than polluting the content stream.

When users like a content, they pay ‘respect’ to the oldest record of that content in the blockchain. Since pirated content will have a different record it becomes a problem. If we aim to solve it using some algorithm, even a bit of information changed in a file changes its records but it could either mean piracy or creation of new content for example changing a single character in a code could mean new code. Also what some people might consider curation, such as a collection of songs, could mean piracy for others. Labelling something as ‘pirated’ is thus a subjective opinion. Thus, an algorithm cannot determine whether a content is pirated but respectonomy provides tools if a community effort wants to recommend original content to others downloading the pirated copy. The original content creator can assign special benefits to community for this effort and since everything happens through transactions, it is an immutable record of people who bought your song for example. The transactions sending money to the address associated with that content’s fingerprint then can have special use-cases such as access to a concert. Money sent to pirated copies will not have this benefit whereas the downloader would also have spent equivalent amount for it. This mechanism drives the price based on rarity of content.

Contents

Abstract **1**

1 Introduction **1**

2 Background **1**

2.1 DHTs and BitTorrent 1

2.1.1 Ownership of data 1

2.1.2 Value of data 2

2.2 Blockchain 2

2.2.1 Data Storage 2

2.2.2 Transaction Ledger 3

2.3 Proof of Work 3

2.4 Bitcoin Protocol 4

3 Respectonomy Design **4**

3.1 Challenges 4

3.1.1 Quality of Content 5

3.1.2 Reliability of Factual Data 5

3.2 Censorship 6

3.2.1 Solution 6

3.3 Architecture Overview 7

3.4 Architecture 8

3.4.1 Social Networking Services 9

3.4.1.1 Interaction Services 9

3.4.1.2 Respectonomy Services 9

3.4.2 Substratal Management Services 9

3.4.2.1 Authentication Protocol 10

3.4.2.2 Discovery Protocol 10

3.4.2.3 Library Protocol 10

3.4.2.4 Blockchain Protocol 10

3.4.3 Micropayments-based Content Streaming Protocol 10

3.4.4 Peer-to-peer Networking Services 10

3.5 Respectonomy Layers 10

3.5.1 Peer-to-Peer Networking Layer 11

3.5.1.1 Blockchain Layer 11

3.5.1.2 Distribution Layer 11

3.5.2 User-Interaction Layer 12

4 Conclusion **12**

5 Notes **13**

5.1 Consensus Protocol 13

5.2 Hashing Algorithm 13

5.3 Genesis Block, Mining and Halving 13

6 References 14

Abstract

Cryptographically secured transaction-log when rendered reliable using the proof-of-work signature over the blockchain data structure has demonstrated its utility as a form of a medium of value exchange. This manifests itself in the form of a currency in case of bitcoin. However, this can be used to represent any form of rare token that represents a unit of value.

'Respect' is one such token that drives transfer of various kinds of value required to run an open decentralized social network system. However, being an independent token, unlike colored coins, the proof-of-work blockchain system that 'respect' flows on, represents a closed network with dynamic membership of parties, and this enables Respectonomy to determine its true value in a free-market. Also, unlike bitcoin sidechains, Respectonomy has coins originating at the coinbase of the blocks, like bitcoin, which is a useful property to maintain liquidity, fair distribution, and avoid starvation of the system by delaying consumable value production to units of timestamping.

1 Introduction

Decentralization rooted movements like BitTorrent and Bitcoin have demonstrated, through the power of cryptography to reach consensus and through an incentive/punishment structure, that is is possible to transfer data and value, trustlessly over a network without the need of a third-party.

Respectonomy is a project that aims to assign value to data by measuring the quality of inherent information, and to provide a mechanism for fairly compensating data bandwidth availability and its transfer as a means to find unwanted information (advertisements, spam and trolling) and a means to avoid censorship. This paper discusses how 'respect' can enable an open social network that rewards content fairly.

2 Background

This section reviews the properties of decentralized solutions, which Respectonomy combines.

2.1 DHTs and BitTorrent

2.1.1 Ownership of data

The current generation of social networks own the data produced by its users. Not only is this unfair to the rights of content creators but also takes away their revenue share. Furthermore, lack of ownership on social networks has lead to:

(a) Censorship of Data

(b) Proprietary Data Control

There have been attempts to distribute the ownership of data but decentralization has only been successful in terms of networks available to choose from. This only prevents the power from accumulating with a single platform while trading off the networking advantages due to users being distributed and not on a single platform.

Distributed hash tables (DHTs) have been used to maintain and coordinate metadata about information residing in a peer-to-peer system and BitTorrent protocol to co-ordinate untrusting peers to distribute pieces of files to each other. Thus, a decentralized social network, that uses BitTorrent-like protocol for distribution of its content is feasible. Key advantages are:

1. This system, that Respectonomy implements in the browser, enables open content and no ownership of the data by the social network, but by the users themselves.
2. The social graph, with its edges between parties representing the desire for content consumption and related behavior (share, retweet, etc.) represents the endorsement of content, effectively assuming the seeders in the role of a curator in such a network. Additionally, by seeding content, not only does a node affect the availability bandwidth of content but also disallows central takedown of information, by decentralizing it.

2.1.2 Value of data

Since the data is hosted by seeds, they can determine the custom price for it or the system sets a default pricing based on its rarity and demand. The 'respect' token then enables micropayments for exchange of such data and with an inbuilt mechanism for custom or dynamic pricing can provide value based on the data availability.

2.2 Blockchain

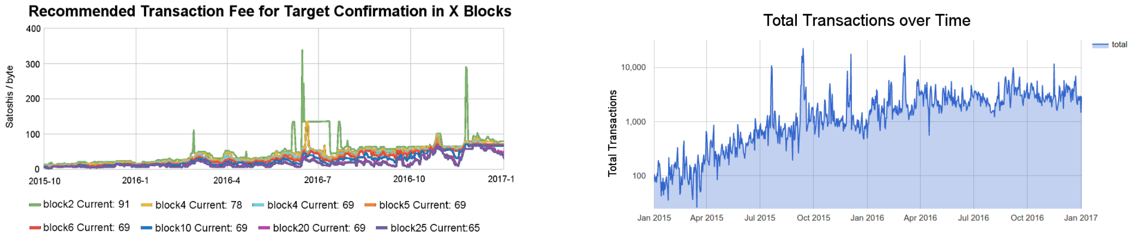
2.2.1 Data Storage

Blockchains are a poor store of data because the demand for a globally replicated free database is infinite. But due to physical limitations, there is a cap to how much information can be transferred, so the block space is rare and expensive. Various blockchain projects have or are bound to fail due to this reason.

Also, decentralized storage using a bittorrent-like protocol is a superior method for storage of data than a blockchain, based on reasons described above. There have been attempts to imagine social networks on a blockchain but have been infeasible practically.

However, the immutability of content is not compromised, since the hash of the document acts as a fingerprint, which being small and fixed in size can be readily stored on the blockchain.

Assume a scenario where data is stored on the blockchain and a user is trying to download that data. Putting that data on the blockchain constitutes a transaction. An attempt to upload a large amount of data in a single transaction would take up majority of the network bandwidth. Data, if stored on the blockchain, incurs an added cost for broadcasting in the network. This additional cost is taken as transaction fees. The transaction fees determines the number of blocks it takes before a transaction is confirmed 1. The data can be variable in size, content and type. An attempt to download such data would put a strain on the network bandwidth and would expend more time in the process. Thus storing data on the blockchain is expensive in terms of time taken, network bandwidth and transaction fees.



(a) Recommended bitcoin transcation fees for confirmation in different blocks.

(b) Total number of bitcoin transactions between 1st January 2015 and 31st December 2016.

Figure 1: Transaction fees and total transactions in bitcoin network

Thus Respectonomy does not burden its blockchain storage with everyone's data. Users only host whatever data they want to share with others and its correctness is guaranteed by the hash fingerprint of the content, verifiable on the blockchain.

2.2.2 Transaction Ledger

A blockchain stores the records of transactions that have happened in the system. Due to the way these transactions are implemented in cryptocurrencies, they can have multiple outputs of coins. Among various possible types, one type is used in bitcoin allows data to be stored in it (op_return). Using this information as a proof-of-existence users pay the original author for the content they like.

2.3 Proof of Work

Earlier platforms that attempted to use bitcoin for upvoting content let users tip money with each vote. Such platforms run primarily into these problems:

1. Since the reputation earned on such a platform is directly a form of money, people want to earn it. However, users do not want to spend all what they have earned; everyone wants to earn more than they spend. This leads to the system starving off bitcoin and the system only sees free activity despite having users.

2. Some platforms start giving sign-up money to solve the problem stated above. However, one account one vote is easily sybil attacked and the platform runs out of money.

3. Further, platforms tried to associate real-world identities to accounts to prevent sybil attack; a behavior that is disliked by the users. Some tried to tie the accounts to social media identity but those were gameable too eventually leading users to move to more easier-to-use and known social networks.

Proof-of-work, when enabling creation of new coins by securing blocks, can act as mechanism to provide the required signup money in installments over time in ratio of the computational resources invested. This prevents sybil attacks because the net total of computational resources invested by various identities of the same entity will be equal to the resources invested by that entity if it were single, producing no benefit to the attack.

Thus PoW, apart from being a fair mechanism for the origin of money, also helps mitigate sybil attacks on the platform and ensures enough liquidity of money over time to flow from content consumers to creators, thereby preventing starvation.

2.4 Bitcoin Protocol

A Proof-of-Work (PoW) blockchain, along with all its entities (pools, miners, etc.), forms a dynamic membership multiparty system(DMMS)[1] that is an independent network of its own. This enumeration of the bitcoin protocol, i.e. a new blockchain with a new token is required due to following reasons:

1. An independent network with a custom token in a free market helps determine the value of that token. Since this token will be used for Respectonomy only, it helps determine the true value of one 'respect'. This helps keep it isolated from the fluctuations caused by other markets that might be using the same blockchain, affecting the value of the token and further also helps in true evaluation of the entire network.
2. Using proof-of-work to generate bitcoin is infeasible for fair coin distribution since the bitcoin mined finds multiple usage, due to various markets competing for the usage of a coin. A new token, avoids this competition and coins originate as incentives for the securing the transaction chain to achieve an economic system towards a single purpose of providing a decentralized social network.

3 Respectonomy Design

Respectonomy is designed to implement an open social network in a layer above a peer-to-peer network built using BitTorrent-like protocol, that runs using a blockchain. This section describes how Respectonomy uses the blockchain and how that solves the technical limitations of current social networks.

3.1 Challenges

Current social networks face various kinds of challenges. This section divides these challenges in accordance to the types of information that causes them.

Primary information, which is information collected by oneself, when observed over social media online, encapsulates private messaging as means of directly obtaining information and primary research as means of gathering information from content presented [e.g. reading code] etc. and is seldom problematic since there is a direct voluntary connection between the source and consumer, which is often se-

cured and authenticated through encryption.
Since primary information is expensive to obtain and evaluate due to various factors, it is not feasible to consume all required information as primary. Trusting the secondary information then, is the root cause of challenges faced by entities online. Such data on social networks can then primarily be divided into ones sharing:

- Factual Knowledge and/or
- Qualitative Information

3.1.1 Quality of Content

Local social interaction teaches that a person's past reputation is often a good proxy to judge the quality of their future work, and the same psychological measuring criteria is applied to online interactions, where it doesn't work as expected because:

- Human beings produce work of inconsistent quality and
- Memory of reputation
  - Requires identifying and associating identities, which is difficult to implement online and
  - Such a memory is difficult to bootstrap and maintain in a social network with dynamic membership.

This psychological phenomena, where humans consider the source's reputation as a rough measure of quality of work produced by the source, when applied to limited human attention-span, causes entities to fight to grab the maximum mind-share of the user, which manifests itself as advertisements, spam, and trolling.
Hence, branding is a poor measure of quality, albeit it deceives humans to believe so. Some social networks aim to replicate this branding by representing cumulative upvotes as a means.

3.1.2 Reliability of Factual Data

Social psychology affects the measure of reliability of content solely based on peers endorsing it, but it is not an accurate measure of reliability of some information. Reproducibility - not peer review - is at the heart of the scientific method. Peer review can actually detract by magnifying cognitive bias.
Falsification or reproduction of factual and quantitative content is expensive. For news content, although authentication can be verified using the proof-of-existence by analyzing its hash fingerprint, further technical forensic tools required to verify the truthfulness of given proofs, that an event occurred, have not yet been developed.
Thus, channels, curators and press is not an ordinary industry but a civic calling. Journalism needs to flow from a hallowed institution to contain predetermined trust or else the determination of trust must be done on the spot using some protocol to determine it.
This reputation is dearly preserved and valued by social media networks and platforms are closed and proprietary, in an attempt to lock-in this gathered reputation and data. Strong influential third-parties, such as the governments, also participate in and support this content-controlling behavior.

3.2 Censorship

As discussed in section 3.1, some sort of moderation or censorship is often required in social networks to remove false/illegal information or to prevent ads, spam and trolls.
But a truly decentralized social networking system enables:

- Freedom of Expression
- Freedom to privately consume information
- Freedom of Universal access

3.2.1 Solution

Let us consider various scenarios of interaction in a social network and associated problems and their solutions. Some of them have been discussed earlier.

- Some social networks try to determine the desirability and reliability of data by votes. When extreme downvotes are received the content is often censored. The problem in this scenario is sybil attack. The power to upvote can be easily replicated using bots and sock-puppet accounts.
  A proof-of-work blockchain offers a solution to this as described in the hashcash protocol[2]. The stake of tokens earned through proof-of-work then represents an identity's reputation. The premise of this representation is that an individual identity is indistinguishable from multiple identities encapsulated as one. Rather than trying to solve it, the system assumes it.
- Reputation is not an accurate enough measurement of content quality due to human inconsistency and thus, finding a solution that depends on the character or attributes of the content creator is unrealistic.
  In addition to that, the quality of content is subjective. What is an advertisement to some, could be useful/desirable information for others. Therefore,
  (a) The social graph helps avoid advertisements (selectively following someone helps keep the ads out) but can allow paid advertisements. The threshold is fully tweakable, where user decides the amount of advertisements they want to see.
  (b) Paying, instead of voting, can help determine the accurate quality of content. However, this only works to avoid sybil attack if the payment is made using a PoW token.
- Trolling is an identity deception and hence not absolute. Since users pay for consuming content, invaluable and troll comments that do not add to the discussion will not get any payments and will run out of money.
- Replication of data is a solution against censorship. However, global replication of all content on the blockchain is a burden to all users. Since censored data is often controversial, the users who share such content endorse the existence of that content.
  In Respectonomy, sharing is a special behavior where user content is re-hosted on sharer's node. This means resistance against takedown of data via voluntary distribution and decentralization, that also gets paid, and is not a burden to to the user.

3.3 Architecture Overview

The Respectonomy platform is essentially an open-source pool running a website that uses the blockchain. Users can use the website hosted with the pool (trusted) or fork and run the code for themselves only interacting with other users through the blockchain and a bittorrent like content distribution protocol. Specifically, Respectonomy uses the peer-to-peer network as a closed market, by facilitating evaluation of content, to dynamically determine its own value, and uses this value to facilitate trade of content, which is further dependent on the market's evaluation of that content and so on. As an analogy to bitcoin, it is similar to saying bitcoin enables value-transfer because it is a valuable token and it is a valuable token because it enables value-transfer due to its rarity and so on. This is primarily the reason behind the need of a new custom blockchain; a closed market is required to determine the value of rarity of an object.

[*]**Login file format**

```
Auth Info:{
  Keys:[
        {   ....   }
  ]
}
Blockchain Info:{
  UTXOs:[
        {
          txid: ....
          vout: ....
          address: ....
          scripPubKey: ....
          amount: ....
          confirmations: ....
          spendable: ....
        }
  ]
}
App Info:{
  Following:[
     uid1: ....
     uid2: ....
  ]
}
```

Login file:
The Login file is used by a user to authenticate themselves on the platform. This file is uploaded and after verification, the user is connected to the platform which is a pool in itself. The file is encrypted and stored on the user's system. It consists of the following information:

- **Authorization information:** The encrypted file contains the private and public key pair information for the user. This key pair is used to verify the UTXOs from the blockchain.

- **Unspent Transaction Outputs (UTXOs):** The UTXO stores the various unspent RES that the user has in their wallet. The sum of all the UTXOs is the balance of RES that the user has from all the interactions on and off the platform.

- **Third party application information:** These include some external applications that can be used with Respectonomy platform. An example of such an application could be the list of IDs of the people that the user follows to get updates on new posts.

[*] format is only representative and is subject to change based on actual implementation.

Separation of social network and blockchain layer:
Respectonomy decouples the interaction of a social network from the availability and distribution of content by separating the networked data layer using bittorrent from the blockchain layer. The social network code can be programmed by any mining pool hosting it whereas the underlying blockchain code remains integral.
The blockchain layer runs the bitcoin protocol, enabling 'respect' to be created and distributed. The social networking layer is responsible for the social interaction and content distribution. This decoupling is a significant improvement over previous systems by not only increasing the capacity of content flow but also allowing each layer to implement features independently of the other.

Ability to construct niche social networks:
The design of Respectonomy allows creation of specialized social networks with weighted payments but still using the same token. This feature in the future enables creation of Respectonomy sidechains, each of which is a separate social network but developed independently of underlying token and assigning different weights to contents that pertain to a specific economic category. In an open network populist content can gather more upvotes than scientific content. If a network doesn't want to they can easily create a new social network with weighted payments and the creation of underlying sidechain and mining pool setup etc. is done on its own. This allows free market to determine fair compensation of content, both qualitative and quantitative.

3.4 Architecture

The application is structured in a series of functional layers.

- At the innermost layer, the domain language is that of application's environment to underneath libraries, foreign function interfaces and networking implementations.
- Beginning at the center, each layer is translated into interfaces with lower-level semantics.
- At the peripheral layer, semantics are encoded to the language of domain model exposed to services.

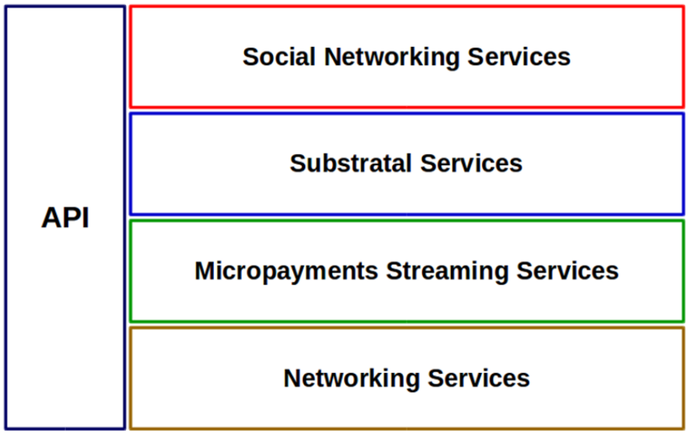
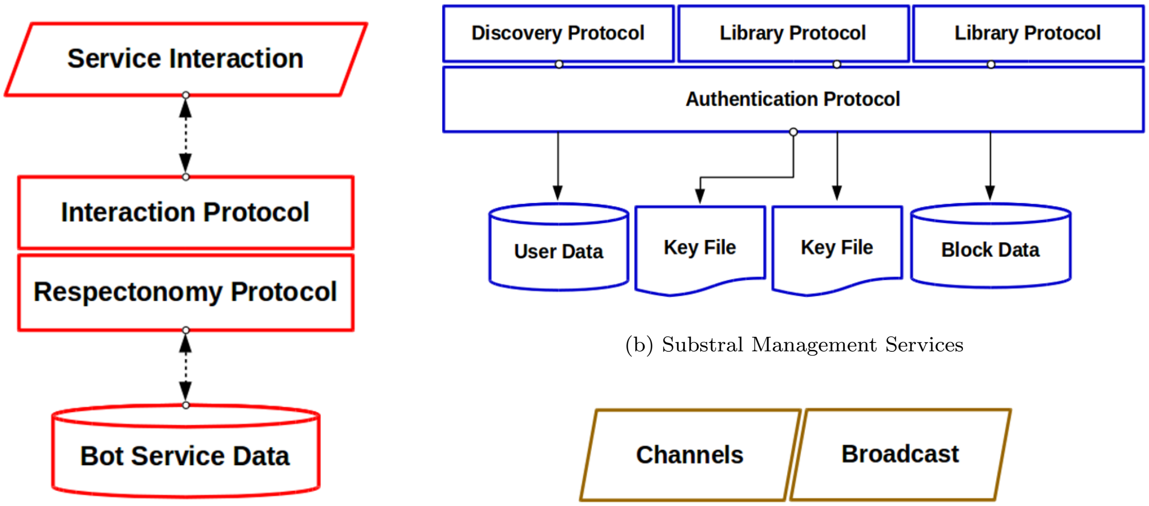


Figure 2: Diagram Overview

3.4.1 Social Networking Services

The API for upper layers has well-defined semantics, high level and composable, allowing complex service development interface. Because these are built from as few orthogonal operations as possible from the lower layers, development relies on composition to satisfy more advanced use-cases and is thus provides a powerful DSL. Bots and services use these domain specific interfaces to implement delivery logic to network's users. The services use other services at lower layers to expose and end-node's attributes and functional capabilities.



(a) Social Networking Services

(b) Substral Management Services

(c) P2P Networking Services

Figure 3: Layer Services

3.4.1.1 Interaction Services

These services deal with human-interaction events and handle the implementation of the UX further. Since a user interacts with respectonomy through an overloaded wallet interaction, this layer implements the nature of this interaction and provides an interpretation layer to host parallel service semantics.

3.4.1.2 Respectonomy Services

These services exposes those behavior interfaces that are not directly or synchronously triggered by an individual user's behavior. Services that expose calls to blockchain's behaviors, for instance.

3.4.2 Substratal Management Services

The layer is focused on the system's problem domain by speaking at the right level of abstraction, so the interacting service do not care or know about the implementation. Since the substratal services are completely isolated, the business logic remains untangled from the APIs. This allows a generalized structuring of the service programs and uniformity.

3.4.2.1 Authentication Protocol

This protocol decentralizes identity. An end-node's current user's identity is established, through local PKI-based authentication. This private information is managed by the user and forms the basis for interaction as well as respectonomy services.

3.4.2.2 Discovery Protocol

This protocol decentralizes the social graph. This protocol helps connect social identities as well as content, based on self-moderated information. However, the cost of decentralizing the social graph is for each user to bear the cost of one's own section of the graph.

3.4.2.3 Library Protocol

This protocol decentralizes content management & distribution. BitTorrent as protocol can not be used directly since there is no need for Kademlia like protocols for determining the 'nearness' for the distributed hash information. In respectonomy, the hash information is distributed on the basis of ownership instead of nearness.

3.4.2.4 Blockchain Protocol

This layer decentralizes value creation and management by implementing a proof-of-work blockchain.

3.4.3 Micropayments-based Content Streaming Protocol

By generalizing the applicatives at lower layers, the interfaces becomes less brittle and allow more flexible use-case. Blockchain data is a special case for micropayments based exchange where no payment might be required for exchange off blockchain data however, may allow a use-case.

3.4.4 Peer-to-peer Networking Services

This layer contains services for bootstrapping and networking.

3.5 Respectonomy Layers

Respectonomy enables new functionality in social networks by changing the meaning of behavior of interaction. It uses the user behavior to automatically gauge the interaction, independent of underlying content-distribution and blockchain protocols.

3.5.1 Peer-to-Peer Networking Layer

Respectonomy is totally decentralized. None of the nodes are privileged though some are differentiated from others by virtue of their actions performed, akin to the difference between mining pools and nodes in bitcoin. The centralized http/https website is open-source and is part of the open-source software that implements a mining pool. Anyone can fork and run the code freely, subject to supporting hardware. Any single, arbitrary chosen terminal entity can be removed from the network without having the network suffering any loss of network service.
The shared resources necessary to provide the service and content offered by the network are accessible by other peers directly without passing intermediary entities. The participants are thus resource providers as well as resource requesters.
The underlying peer-to-peer network abstracts:

3.5.1.1 Blockchain Layer

The mining pool software implements DNS seeds that resolve to provide information about active nodes on the network, just like the satoshi client. It uses similar fallback and pre-check algorithms, such as nodes from previous connection, hardcoded IP addresses of reliable nodes, etc. Anyone can clone this software, provide additional features in the Respectonomy system and run a mining pool.
Once webRTC based peer-to peer connections are established, a blockchain engine starts up in the browser that runs a proof-of-work mining process which generates just enough 'respect' in the user's system so as to make the system usable, but not enough to abuse (spam) while also prevent a need for user identity thus mitigating sybil attack. The expenditure of 'respect' introduces a built-in latency that does not affect humans but charges the bots to tap the firehose.
The system does not require a login since only the payments require user authentication and the information required for this blockchain interaction is carried by user.
Any developer can build a bot that can earn for service it provides. Services that require a database, such as usernames, would require a bot service. Bots can traverse the network and mine any data but since they need to pay 'respect' for it the bots either wait or mine 'respect' thereby strengthening the blockchain or buy 'respect' from the market thereby increasing its value.

3.5.1.2 Distribution Layer

User's data remains on their own system. When a user publishes some content their node starts acting as a torrent tracker for that content, while the process of publishing requires a transaction from user's address. Other nodes that are following this user by monitoring that address on the blockchain notice this transaction which contains a hash of the content it represents. The system then connects to its torrent tracker and downloads the content that is displayed on the follower's dashboard. A seed can ask for a payment in return for a torrent piece, in which case a micropayments channel is opened up between them. This price value is set at - cumulative sum of likes received divided by the number of seeds for that content - by default, but is overridable by the user. When downloading a file from a seed, the other files in their DHT appear as suggestions of similar content. Thus the DHT becomes each user's curated content list, which other users can pay for and download.

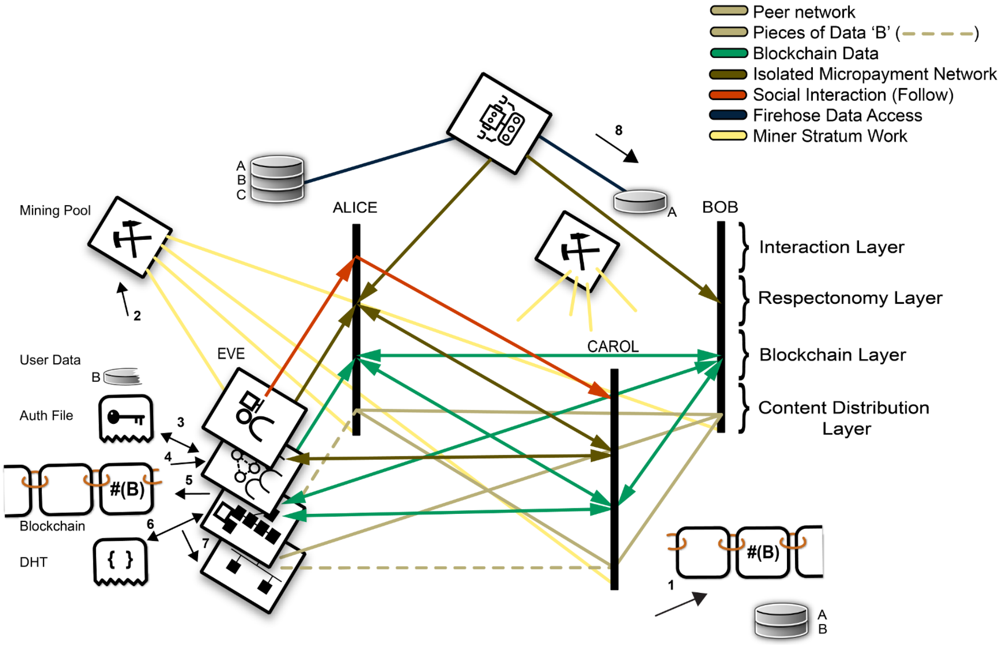


Figure 4: Distribution of content on Respectonomy Platform.
(1) Carol publishes some new content B. Alice follows Carol so Alice hosts B. (2) Eve connects to Respectonomy Network through the mining pool. (3) Eve follows Alice. (4) Eve syncs her blockchain. (5) Eve reads the hash of content B on the blockchain. (6) Eve syncs her DHT. (7) Eve Downloads the content B. (8) Bot accesses firehose data.

3.5.2 User-Interaction Layer

When users publish content a transaction is made on the blockchain and the node starts seeding while running a private tracker for it. When users like a content, they pay 'respect' to the address in the transaction in which the hash of that content first appeared on the blockchain, namely the content creator. When users share a content they add the tracking information to their DHT and start seeding the content.

4 Conclusion

We have presented Respectonomy, a blockchain based social network. Respectonomy introduces new design and user-interaction paradigms. The design of Respectonomy was informed by various technological improvements in social networks and various failed experiments at implementing a blockchain based social network.

5 Notes

Specifications Rationale:

5.1 Consensus Protocol

Proof-of-work is chosen so as to align incentives similar to bitcoin by fair distribution of reward for securing the network.

5.2 Hashing Algorithm

New cryptocurencies aim at building ASIC resistance to avoid 51% attack, or sometimes due to malicious reasons (such as limiting mining to self on coin launch). All processor based algorithms are prone to attack due to the existence of large GPU farms. Attempts have been made at memory based hashing algorithms but are not yet practical.

Thus, instead of concentrating on mitigating ASIC attacks, we recognize that no coin is 51% attack resistant. Assuming that a new coin will be attacked we rather facilitate miner competition by making it easy to mine for everyone, so that when multiple parties try to attack the coin and thus cancel each other's centralization effect.

Using SHA256 algorithm asides from being the most competitive, additionally provides a benefit that a miner is foregoing their bitcoin profit in order to attack Respectonomy, thereby incurring losses while attacking or else only doing so if they value the amount of 'respect' generated as relatively more valuable.

5.3 Genesis Block, Mining and Halving

Halving of the coin reward per block is done to create an incentive for early adopters. This subsidy reduces over a period of 8 years which we consider sufficient to test the spread of a social network. Te coin generation remains to be constant per block thereafter because we want to keep the fee as less a possible.

Bitcoin was designed to simulate gold and so 21 million bitcoins will ever be produced representing the total amount of gold on earth which is estimated to be a cube of side 21 meters. Also bitcoin's halving period of 4 years was designed to simulate a change in economic cycle globally.

Respectonomy is designed to simulate a social network which requires coin distribution over 8 years by starting from 16 per block and halving every 525600 blocks to account for a 2 year change in internet's social networks, reducing to 1 coin per block after 8 years forever.

The genesis block will contain the addresses of respectonomy supporters who shall be participating in the initial coin offering. It shall be mined at least 2 days after the release of code which is browser based. Miners will be able to connect to the network and listen for genesis block at least 2 days in advance.

6 References

[1] https://blockstream.com/sidechains.pdf

[2] http://www.hashcash.org/hashcash.pdf