# RESPECTONOMY

A Decentralized Social Network

First Draft

tbolt256@gmail.com

## Contents

# 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, Repectonomy 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) Propreitary 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.
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 [eg. reading code] etc. and is seldom problematic since there is a direct voluntary connection between the source and consumer, which is often secured 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 enitites 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 physchological 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 beleive so. Some social networks aim to replicate this branding by representing cumultive 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 analysing its hash fingerprint, further technical forensic tools required to verify the truthiness of given proofs, that an event occured, 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 pre-determined 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 propreitary, 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 recieved 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 rehosted on sharer's node. This means resistence 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 blokchain. 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.

**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 Respectonomy Layers

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

### 3.4.1 Peer-to-Peer Networking Layer

Respectonomy is totally decentralized. None of the nodes are priviledged 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 requestors.
The underlying peer-to-peer network abstracts:

**3.4.1.1 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.

**3.4.1.2 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 recieved 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.

### 3.4.2 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.

## 6 References


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

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