Yada

A blockchain-based social graph

January 2018

Abstract

The goal of Yada is to achieve an acceptable level anonymity, privacy, and freedom of expression while making available to the public a structure of relationships between humans.

Yada is a blockchain-based social graph that leverages the immutability and ownerless properties of the blockchain to decentralize social media and dramatically simplify the classic invite, register, and login workflows. The simplification of these processes grants freedom to all social media users currently trapped in the walled gardens of today's social media monopolies. Yada enables users to own their online relationships while giving online services the user data they need to create rich experiences. This value proposition is particularly attractive for startups seeking to quickly grow their user base as inviting and registering are simple, one-click processes. Large organizations will find it much easier to engage their audience in a variety of services with the ease of transitioning their users from one service to another. Services of any size will be very excited to adopt Yada to take advantage of user yada's streamlined authentication. Yada will also create a reliable space for controversial voices blocked by the ever expanding censorship of social media monopolies.

Table of Contents

Target Markets

General Public

Social Transactions

Social transactions symbolize real life emotional investments. When you request someone to be your friend, there is some emotional "risk" just as there is in real life, only this is represented by yada coins. When someone accepts your request, then your emotional risk is rewarded with some return of the amount of yada coins sent in your original request. App developers can have fun with these numbers and play with them as they see fit for the application they are developing.

1. **Friend Request**
   - Alice sends bob 1 yada coin plus a transaction fee to store that friend request on that blockchain.

2. **Approve Friend Requests**
   - When approving a friend request, the amount sent in the original friend request could be sent back to the requester

3. **Discouraging Bad Behavior**
   - Requiring an investment of yada coins to request a friend eliminates a great percentage frivolous friend requesting.

4. **Rewarding Bad Experiences**
   - When users are inundated with unwanted friend requests. They simply ignore the requests and keep the yada coins sent to them with the request.

Competitive Marketplace

Our motto is “put your money where your mouth is.” Sharing your ideas/content/voicing your opinion is worth more when there is a financial investment behind it. This investment, which for some will translate to an emotional investment, comes in the form of yada coins.

To post content, you must spend a free market determined amount of yada coins in the transaction fee. Miners get this fee. A marketplace similar to Google AdSense will emerge as content producers spend more money to get ranked higher on sites that sort based on this transaction fee. Higher transaction fees means a larger organization behind the content. This will help to maintain the current zeitgeist of media and advertising. Mid level expenditures are expected to be users/organizations who are promoting viral content for a profit. Lower level would likely be small businesses and individual users would spend the bare minimum just to share content with their friends. This expected class system will keep fees affordable to those who share content with friends while creating a competitive environment for large organizations.

Market Capitalization

Overall, this will manifest rapid and consistent growth in terms of market capitalization as more and more yada coins will be required to post content in the upper tiers.

Site Builders

Registering for an Online Service

When registering for an online service, you are simply becoming friends with the identity of an online service. On the blockchain, the relationship is indistinguishable from user relationships.

Sign In

Signing into an Online Service can be done on or off of the blockchain. In either case, an online service can present a user with an challenge string and tie that to a browser session. The user will take this challenge string, find the respective shared secret for that relationship established at registration, encrypt the challenge string using the shared secret, post a new transaction with that challenge string and answer(the encrypted challenge string) back to the online service where authentication is permitted by decrypting the answer to reveal the original challenge string. This method is more secure than simply exchanging the shared secret and also alleviates the need to expire the shared secret because it is never send over the wire more than once ever.

Creating a Relationship

A relationship is created by both users submitting transactions to the blockchain that contain the shared relationship information encrypted with their respective keys. Both users can confirm a relationship when a third transaction is submitted with relationship information encrypted using the shared secret encrypted in the previous two transactions. The relationship field for a transaction is always encrypted with either a hashed version of a user's private key or with the relationship shared secret.

Integration

Sites integrating Yada into their app will expect to see this pattern:

- API Endpoint for the user's social graph from the perspective of the implementer. This means only relevant relationships to that site will be retrieved from the endpoint. This maintains privacy for the user who may not want the implementing site to know all of the relationships they have.
- At this point the graph information is sent to the user's client. The graph information is comprised of a series of transactions. The transaction contains encrypted relationship information.
- User client will use their stored keys.

Anti-censorship

Identity

Yada does not store any personally identifiable information, nor does it assign a unique identifier to any identity on the blockchain. Instead, your identity is comprised of the relationships you've created on the blockchain. These relationships are simply a series of transactions containing encrypted relationship information that can only be decrypted with the user's private key.

Anti-censorship

Because your identity is stored on the blockchain, it cannot be removed. Because you do not have a unique identifier, you cannot be blocked. All of your relationship identifiers can be changed at any time.

If you are removed from a service, you can post a bulletin to the blockchain informing your followers of a new service to find your content.

This always gives you away to stay in contact with your audience and rest assured that you will not lose them due to arbitrary idealogical disagreements you may have with the operators of a given service.

Technical

Consensus Algorithm

Consensus is established when 51% of the peers on the network have all chosen the same block for a given block height.

Key Generation

Key generation is exactly the same as bitcoin. In fact, our current implementation is written using bitcoin libraries.

Bitcoin Differences

While we are using bitcoin libraries for key generation, signing, and verifying blocks and transactions, the data we are signing and verifying is different. The transaction hashes include rid, requester_rid, requested_rid, and other fields. Also, the inputs and outputs are limited to a maximum of two parties in the outputs. One party being the recipient and other being the sender to send back the remainder of a spent input. We use the same Merkle hash tree and root method for transactions as bitcoin though we do not double hash the transactions.

Conclusion

Having accomplished the goals of eliminating censorship in social media, the need for registration forms, usernames, passwords, and created an eco-system of user sharing to spur rapid growth of new online communities, we can all use yada as piece in the larger puzzle of freedom for humanity from corruption and coercion once and for all.