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 bases 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 benefit significantly by using Yada to take advantage of its streamlined authentication. Yada also will create a reliable space for controversial voices blocked by the ever-expanding censorship of social media monopolies.

Table of Contents

Vision for a New Social Media

The ultimate vision for social media is for every online service to act as a sort of airport where users can arrive from the atmosphere and create relationships in the context the online service creates. The relationships, however, are imprinted onto the fabric of this virtual world and those same relationships can be recalled at any airport where both users exist. Online services can be made aware of your relationships. This relieves the burden of having to request and accept all of your friends repeatedly again when you join a new online service.

Multiple Identities

Creating multiple identities is as simple as generating a new private key for an entirely new social graph.

Relationship Sharing

Online services will provide a sort of match-making service in exchange for the enormous value gained from the low barrier to entry when joining their services. It is a community mindset that is fair, balanced, and benefits everyone participating.

Inter-domain Friend Requesting

Online services will be aware of your relationships, should you decide to share that information with them. Therefore, they also will know when you receive a new friend request. Given that the friend request comes from the blockchain, this technically could be routed through any online service you use.

Micro-contexts

Micro-contexts will emerge because monolithic web sites will no longer be necessary. Yada will create an environment for highly focused app-like web sites with hyper-specific user interfaces and gaming mechanics.

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 large 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 of 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 receive this fee.

A marketplace similar to Google AdSense will emerge as content producers spend more money to be ranked higher on sites that sort based on this transaction fee. Higher transaction fees reflect 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 or organizations who are promoting viral content for a profit. Lower level likely would be small businesses and individual users spending 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. This need to purchase coins in order to post content is never-ending. Therefore, the price will continue to climb as adoption, friendship creation, registration, login, and content production increase.

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.

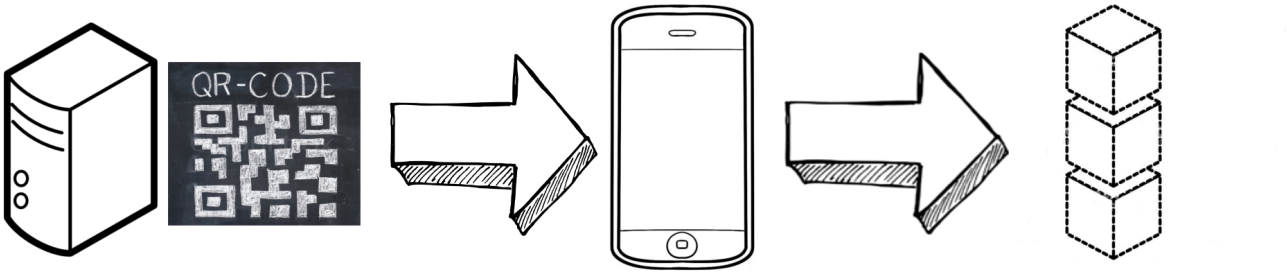
Sign In

Signing into an online service can be done on or off of the blockchain. For example, a service provider would generate a key that would also be tied to a browser session identifier and send it to the user as a direct message on the Yada blockchain. In the user interface, the user would approve a transaction which automatically sends the key back to the service provider as a direct message. The key is encrypted both ways but even if the key is compromised, the attacker still cannot use that key to hijack the browser session. For the user to be considered logged in, the verification process would be as simple as verifying the key was both sent and received.

Creating a Relationship

A relationship is created using elliptic curve diffie-hellman key exchange. This type of key exchange is preferable because of its ability to display key information publicly without compromising security for two or more participants who have never met. To form a relationship, Alice and Bob both submit transactions to the blockchain with private and public keys in their transactions. Alice and Bob now have enough information to generate a shared secret by decrypting the private key field of their respective transactions and using the diffie-hellman public key field from each other's transactions.

Yada Workflow

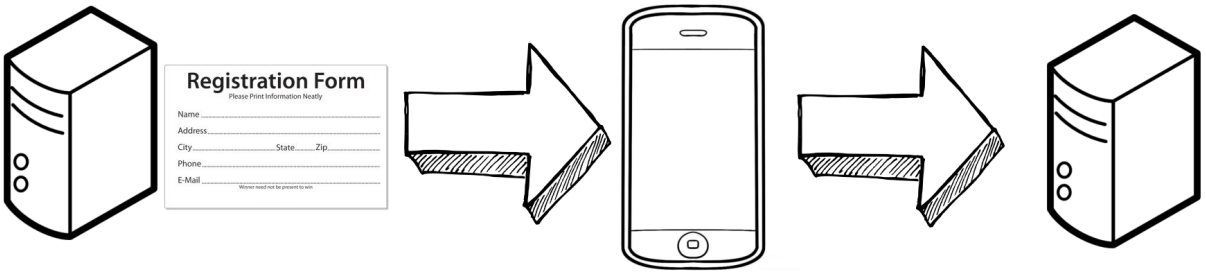


Server produces QR-Code

Mobile device sends QR-Code data to the blockchain

User account is confirmed on the blockchain

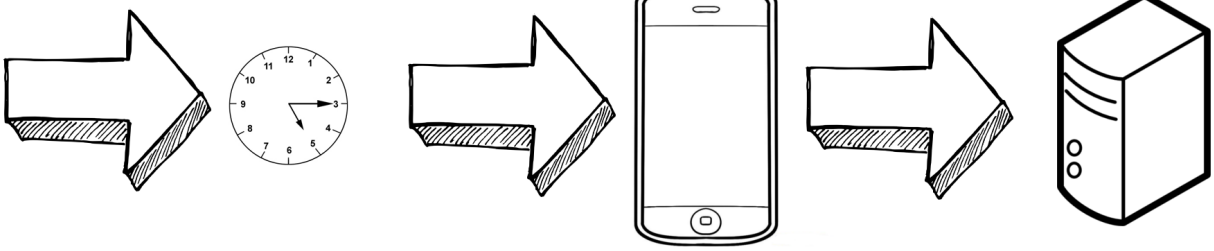
Current Registration Workflow



User fills out registsration form

Device sends registration data to server

Server sends confirmation email



Wait and hope the user receives the confirmation email

User clicks confirmation link in email

User account is confirmed

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 users 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 to decrypt the relationship data contained in the transactions in order to construct the remainder of the graph.

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 or a shared secret.

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 a way to stay in contact with your audience and rest assured that you will not lose them due to arbitrary ideological 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 for 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 is the recipient and other is 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 although we do not double-hash the transactions.

Conclusion

Having accomplished the goals of eliminating censorship in social media as well as the need for registration forms, usernames, passwords to create 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.