A Novel Method for Implementing Usernames in Cryptocurrencies

Rhett Applestone

Abstract

Traditional cryptocurrency addresses are quite cumbersome. There have been previous attempts to implement cryptocurrency usernames before, including the Ethereum Name Service [1], or as another layer in wallet software [2], however there has not been a decentralized system proposed in which everyone has a username, everyone transacts username-to-username, usernames are free, usernames don't expire, and you get to pick your username. This would be as close to mobile payment apps like Vennmo or CashApp as possible for decentralized systems and would radically improve usability. In this paper we attempt to lay out such a system.

1 Introduction

For our system we will use an account-based Proof of Work chain with an arbitrary block reward and at least two basic commits.

1. Username claim
2. Transaction of currency

The former of the two will be the main focus of this paper as the latter is relatively easy.

2 Username Claim

If we want the luxury of being able to transact solely with usernames instead of addresses and want to allow anyone to create a new username for free, we must accept that one person may claim multiple usernames. I will now attempt to explain the process of a username claim, and how we can highly disincentivize namesquatters and spammers from clogging up the network and wasting our disk space.

The Username Claim process is as follows: Anyone is allowed to claim a username by providing a small proof of work along with their desired username and a public key. The work is validated and the username checked against a list of existing usernames, disallowed names, and checked for disallowed chars. The claim is put into a mempool and a miner will get a small fee for including it in one of the next blocks. Once the claim is included in a mined block it is valid and the username is tied to the user's public key. Transactions can be sent signed with their corresponding private key.

2.1 Small Proof of Work

Requiring a small proof of work will act mainly as a speed bump in username claims. It's possible to make it harder or easier, but something most normal computers could do in ten minutes seems like a good benchmark. It's important to use an ASIC resistant POW algorithm such as RandomX [3] to favor normal users. The amount of work required can be updated every so often as computing hardware improves.

2.2 Disallowed names

The main reason people would want to spam the network with username claims would be for the purpose of buying and selling rare usernames which they believe might net them more money than just mining the chain itself. While this is a terrible idea as whoever claimed the name would have access to the private key controlling it, people would certainly try to do this.

Our solution is banning the majority of names that are rare or that may have perceived value. Most usernames or domain names that are bought and sold fall into a few basic categories:

1. Single words, usually nouns, i.e. “banana” or “lizard”
2. First names, i.e. “Alice” or “Bob”
3. Short 1-4 character names
4. usernames with a pattern, i.e., all the same character, palindrome, acending, decending,

Additionally, names of companies and famous people would be good to disallow.

There are many places to find lists of words and names. Dictionaries and Wikipedia/Wikidata seem to be good places, and it’s important to include other languages that use the latin alphabet.

While this disallowing may seem a bit exhaustive it is not likely to affect the average user trying to make a username that is some derivative of their own name or a combination of arbitrary words and numbers.

It is likely not possible to ban all the names that a namesquatter might want to claim, however this would ensure that the majority of “rare” names most people would want are not allowed which would stop a large resale market from developing.

2.3 Username Purge

It is still possible that even with these mitigations people will still clog up the network and take up disk space with unused names. Therefore, we suggest that once a year every username with an account balance of zero, and no transactions in the past year, be deleted and made available. Nobody who has any money in an account or just momentarily took their balance to zero will have their account deleted.

2.4 Miner’s fee

A miner’s fee is needed to allow new users to get their username claims included in the next block, however the fee should be lower than what could be made by just mining the chain itself as to incentivize miners not to “mine” for usernames and include them in their own block. A reward that equates to an ROI of half of what just mining the chain would give per work done seems reasonable.

2.5 Username Specifications

It’s a good idea to standardize what our username can be for transaction and data keeping purposes. We suggest that usernames consist of between 5-32 characters and only contain the lowercase letters (a-z), along with numbers (0-9). In practice it would be a good idea to make send transactions non case sensitive which allow the sends to both “exampleUser”, and “Exampleuser” both credit the same person, “exampleuser” to make transactions easier and reduce lost cryptocurrency.

3 Conclusion

We believe that in the system we’ve constructed normal users will be able to effectively claim a username while preventing and mitigating the effects of those trying to spam the network.

References

[1] Ethereum Name Service, https://ens.domains/ (2024)

[2] S. Coelho-Prabhu, "Send crypto more easily with Coinbase Wallet," (2020)

[3] Randomx, https://www.getmonero.org/resources/moneropedia/randomx.html/ (2019)