DOI: https://doi.org/10.30837/IVcsitic2020201368

Analysis of decentralized system identification schemes

Vlasov Andrii[1]

Lysko Viktor[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, andrii.vlasov@nure.ua

[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, viktor.lysko@nure.ua

Abstract. *A scheme of identification system that uses the concept of building decentralized systems and allows each user to analyze the identity of users and service providers is considered. The main parameter of significance in the system is the level of trust in consumers depending on other participants of the platform and external information. It supports the ability for the owner to fully manage their data (account, master and secondary data) and its associated identifier through the use of various cryptographic signature mechanisms, hashing methods, and trust definitions implemented in decentralized systems and networks. The scheme is compatible with the digital asset management and current identification tools (for decentralized blockchain systems)*

Keywords: *digital identification, protocol, public key, hashing, consensus.*

I. Introduction and Problem statement

Global services, which have a large community of users worldwide, allow users to use different services through the OAuth protocol [1 - 5], which does not provide data reliability by cryptographic methods and uses session mechanisms to access user data.

The development of decentralized systems has shown that the best practice is the cryptographic signature of each request sent to the accounting system and the signature of each response that the system returns [5, 6].

A global digital identification system (decentralized systems and networks) should provide for the binding of all personal data (PD) of a user and his or her public key (key set) to a unique global identifier.

The purpose of building such a scheme is:

– all information about confirmation of personal data is stored in a single system. Using digital signature mechanisms and linking transaction sets to each other will allow the authentication of specific PD confirmations with event-bound events according to timeline [6].

– the integrity and authenticity of the data linked to the account is verified exclusively by cryptographic methods (the control root hash value of the Merkle tree) [7].

– the management of personal data is completely controlled by their owner, all other members of the system can only confirm the set that is defined by the user.

II. Problem solution and Results

In order to receive personally identifiable information about a particular member of the system, the identification service provider must contact the person directly and obtain or immediately require the required data set or permission to obtain this data from another provider.

A global user ID is unique within an identification system that represents a specific entity and related information. The ID is created by the public key of its owner, a set of hash values from his personal data, a set of hash values from the identifiers of other data of the accounting system.

All the above data are linked into one structure, which corresponds to both the account in the existing digital systems and the account (identifier) in the decentralized system (Table 1).

Table 1. Structure of the global user identification

Name	Mechanism of formation
Account (global) identifier	Generate a unique number when you create a new user account (size and range must be consistent with digital system protocol)
Public key	Generation by cryptographic signature methods (must match cryptographic protocol parameters, size and range - digital system protocol)
Readable identifier list	Calculation of hash values of different personal data of the user (must match the parameters of the selected hash methods, size and presentation - digital system protocol)
Main data confirmation list	Set of records (permanent information of personal data of the user), which are verified by a cryptographic signature (the minimum required data set for user identification, size and presentation must be consistent with the digital system protocol)
Merkle Root for main data	Calculation of hash values of the user's basic personal data set (must match the parameters of the selected hash methods, size and presentation - digital system protocol)
Additional data confirmation list	Additional set of records (variable information) of user data that is authenticated to them by a cryptographic signature (additional user data set, size and presentation must comply with digital system protocol)
Merkle Root for additional data	Calculation of the hash value of the additional set of personal data of the user (must match the parameters of the selected hash methods, size and presentation - digital system protocol)
Recovery power	Set of data (conditions) for restoring account access and changing the public key (the minimum required data set to restore access, size and presentation must match the parameters of the cryptographic protocol)
Providers list	Set of data from vendors implementing an authentication service

If the user chooses to restore some of the data for the full set, then the Merkle Root value will completely change. As a result, a previously created and sent transaction that confirms data for a particular Merkle Root becomes invalid. That is why the structure of the account has the peculiarity of splitting the data into main and additional parts: if the user has confirmed the basic data set (and does not change it), then regardless of whether the additional data have been updated, the master data remains confirmed.

A feature of decentralized systems is the lack of information in the network that directly determines the validity of a specific identifier: there are only accounts and voices that confirm the data of the created accounts. Thus, the issue of trust is fully passed on to the client (he can personally determine the method by which his confidence level will be calculated).

Common methods of determining trust to date are:

– trust only to a specific (several) provider (the scheme is somewhat centralized if the number of providers the user trusts is small);

– trust by majority decision (number of IDs verified by network members). Being attacked by Sibyl - one of the accounts can create a large number of other accounts that confirm the identity of one of the members of the system);

– trust by most ISPs, vendors, and users (a more sophisticated validation algorithm that results in many levels of validation).

The main thing is that no matter how the consumer uses the results of the identification, the system provides the ability to fully customize the verification algorithm, which rests solely on the client's side.

Different algorithms (mechanisms) for reaching consensus are used to identify users' trust, determine their level of trust, and motivate validators in decentralized systems. In the blockchain systems, the Federated Byzantine Agreement and the Practical Byzantine Fault Tolerance are more expedient (rapid overall consensus on the network, advantage over participants' anonymity, and a higher level of decentralization) [7 - 9].

The key issue at this stage is protection against spam attacks: they cannot affect the decision-making mechanism of a specific ID, but this can negatively affect the system's bandwidth (since any user can add a transaction to the network, and in fact the number of such transactions is unlimited). Therefore, a mechanism should be provided for protection against this type of attack in the first place for validators.

The considered scheme of digital identification [7, 8] is capable of promptly responding to the compromise of user keys, since its states are homogeneous for all participants and all nodes at one point in time can receive information about the revocation of a separate certificate. It suggests using a secure method of recovering access to an account, which involves contacting multiple providers or other users (trusted by the user). The likelihood of collusion by all ISPs / other users (which support different authentication methods) is very low and allows the user to safely regain access to their account (although overall this complicates this procedure).

III. Conclusions

The blockchain digital identification scheme thus considered has the advantages over existing services:

complete control of users of their own data (change of account fields can be initiated only by their owners);

transfer of data management and decision-making to the end-user (independence of decision to make / reject individual identifiers);

making decisions by each party independently, focusing solely on the state of the database;

increased level of objectivity in verifying user data than using authentication from centralized providers;

the integrity and authenticity of the data linked to the account is verified solely by cryptographic methods;

the data set for the user implements multiple run of values with the calculation of their hash values;

repeated hashing of user data significantly increases the time needed for the attack from the attacker;

synchronization of events between independent parties through the use of blockchain technology (each party has the same state of the local database).

The use of blockchain technology to build different user identification schemes can solve the problem of providing an additional level of reliability and flexibility in the implementation of identification services (development of identification systems) in information and communication systems.

References

[1] Using OAuth 2.0 to Access Google APIs. [online] Available at: https://developers.google.com/identity/protocols/OAuth2.

[2] Facebook Login for the Web with the JavaScript SDK. [online] Available at: https://developers.facebook.com/docs/facebook-login/web/.

[3] OAuth with the Twitter APIs. [online] Available at: https://developer.twitter.com/en/docs/basics/authentication/overview/oauth.

[4] Authorizing OAuth Apps. [online] Available at: https://developer.github.com/apps/building-oauth-apps/authorizing-oauth-apps/.

[5] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – 2018. [online] Available at: https://tools.ietf.org/html/rfc6960.

[6] Distributed identities. [online] Available at: https://patents.google.com/patent/US7512649B2/.

[7] Oleksandr Kurbatov, Pavel Kravchenko, Nikolay Poluyanenko. "Global Digital Identity and Public Key Infrastructure." [ISCI'2019: Information security in critical infrastructures]. ASC Academic Publishing, Minden, Nevada, USA. pp. 237 – 247.

[8] Method, apparatus, and computer program product for providing a group based decentralized authorization mechanism [online] Available at: https://patents.google.com/patent/WO2009133419A1/.

[9] Protection of confidentiality, privacy and financial fairness in a blockchain based decentralized identity management system [[online] Available at: https://patents.google.com/patent/US20190182035A1/en?oq=US+2019182035+(A1).