DIGITAL IDENTITY VERIFICATION

Blockchain And Cryptocurrency Technologies

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

DIGITAL ASSIGNMENT 1

SUNEHA GHOSH (18BCB0075)
SIDDHARTHA MONDAL (18BCB0145)

SUBMITTED TO:
PROF. BOOMINATHAN P.

ABSTRACT:

We have all come across the term digital and identity as an individual term. Identity claim of a person in manual can be in the form of hardcopy of varied sizes and shapes. It becomes difficult for a person to carry all the documents everywhere to prove his/her identity to gain access to the desired services.

Therefore, with the Advancement in technology, many have started using the software version of documents that can be carried easily within mobile devices. Now when Digital and identity, these two terms come together, they give the digital identity of a person in the virtual world which they can use to gain access to websites and commit transactions, manage, buy and sell assets in the digital world.

INTRODUCTION AND DESCRIPTION OF MODEL

There are many examples in the internet about the implementation of digital identity and by referring to some of them, in this assignment we will try to execute the claiming of a digital identity for buying a real estate using ERC 725 735.

Basically, identity consists of **two parts**:

1)Keys that **owns** and **controls** the **identity**

2)Keys that **Claims** that **belong** to that **identity**.

Identity – that is, a person has a proof of his/her being. Basically, authentication of a person.

Claim of identity – that the person is claiming to be the person what he says he is and has proof to support his claim.

ERC725 → Identity Keys

- manage unique identity for humans, groups, objects, and machines.
- hold keys to sign actions (transactions, documents, logins, access, etc), and
- claims, **which are** verified from 3rd party (issuers) and self-verified (ERC735),

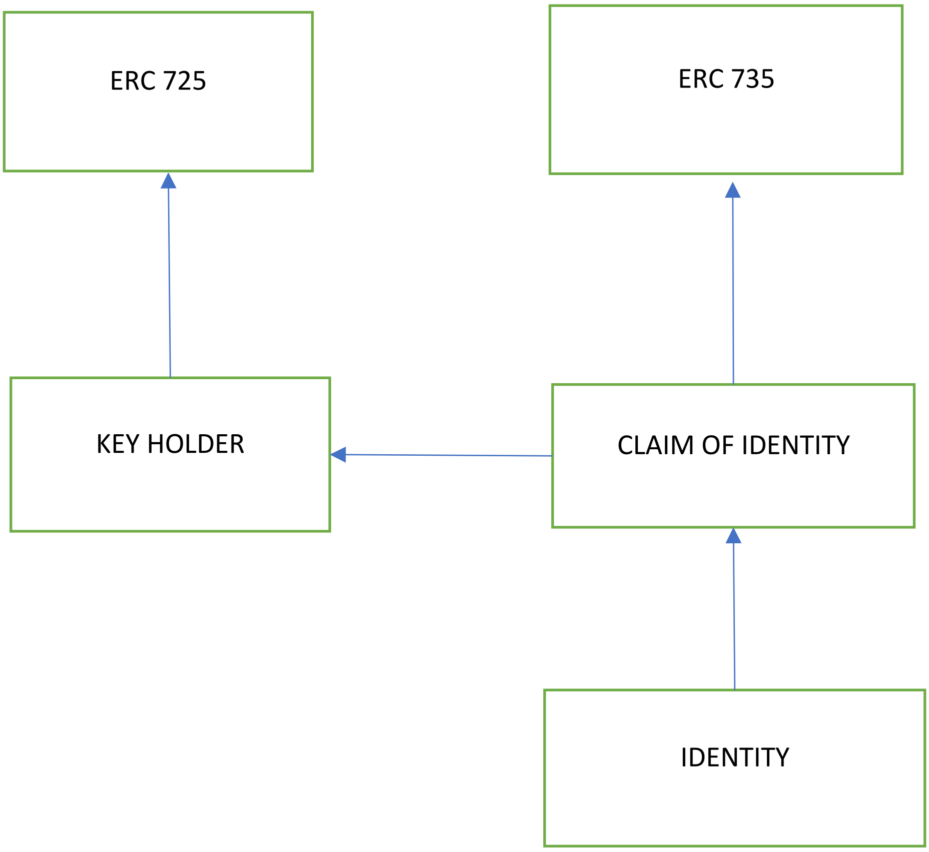
- a proxy function, to act directly on the blockchain.
- Claims are made via EVM-based blockchain ex: Ethereum. Therefore, identity is represented as chain addresses.

ERC735→ Claims of Identity

- standard functions for adding, removing and holding of claims.
- claims **can be** verified from 3rd party (issuers) or self-verified.
- claim holder interface will allow Dapps and smart contracts to check the claims about a claim holder.
- Trust is transferred to the issuers of claims.

The relation between ERC725 and ERC735

ERC 735 deals with the management of claims made about an ERC 725 identity. It provides an emergence of a web of trust, by relying on the claims of trusted 3rd party about a issued identity.



PROBLEM STATEMENT:

We want to deploy a company who wants to sell their real estates in an action to consumers with a legitimate google and a github ID. The whole process has to decentralised using blockchain and Ethereum,and has to be secured with public and private key encryption and decryption. So, to accomplish this we have to describe the entities that are going to be used.

ENTITIES

1)Auctioner: wants to sell their real estates in an auction to consumer with a condition that the applier must have google and github id.

2) Consumer: identity who wants to buy the real estate and needs to clear KYC claims and email claims.

3) Issuer (3rd party): identity provider which issues claims of type 'has google'and perform 'has github' checks of the consumer.

FLOW OF WORK

1) Issuer deploys its own identity contract.
2) Issuer adds a CLAIM key to its identity contract.
3) Consumer deploys their identity contract.
4) After Consumer successfully undergoes KYC and creates an email ID, Issuer signs 'has github'and 'has google'by using a cryptographic signature for consumer providing that the issuer controls the particular github and google ID.
5) Consumer adds Issuer's signed 'has github'and 'has google' to their identity contract.
6) ABC company deploys their token and sale contracts.
7) Consumer participates in ABC Company's auction by transferring through their identity contract to ABC company's sale contract.
8) ABC Company's sale contract confirms that the Consumer's identity contract contains a 'has github'and 'has google' claim by Issuer by recovering the public key from the claim signature and verifies if it is still valid in the issuer contract.

9) After confirming the deal is set and transactions are allowed to proceed

SOFTWARE REQUIREMENT

- Debian OS (we worked on Kali Linux)
- Nvm 9.11.1 version
- Npm
- The above two are required for running the Node Js files
- Yarn
- Memory: 20GB (for OS)