

Universal Digital Proof of Identity (UDPOI) & Universal Digital Proof of Person (UDPOP)

Over Minima BlockChain

by @elleDaniels

version 0.0.1

ABSTRACT:

The new technological changes are happening so fast that it is very complex to keep the pace of the new ideas and developments that are being made, lots of words came out like: Crypto coins, Tokens, NFT's, DAO, CEFI, DEFI, DEX, web2, web3, Exchanges, Staking, liquidity pools, decentralization, scalability, bonds, smart contracts, stable coins, play to earn, ledgers, hot wallets, cold wallets and thousands of crypto coins that already exist on the market with millions of money being invested on those projects that every day arise.

Lately a new word "METAVERSE" is gaining popularity while some countries are adopting crypto coins as their own coin, others are trying to regulate them, others are accepting them to pay taxes or goods, so, if we put all things together it leads us to a new world where it will be impossible for any country to try to control it or regulate, as they will not be able to keep the pace, as the new ideas and projects will arise from individuals, small companies, big companies, open source every day in the form of social projects, games, financial products, virtual worlds and so on, limited only by the imagination of the people.

The world is changing, and it will be unstoppable, so better to be ready than sorry. We are heading to a mix of virtual and real world that will converge into a "**Metaverse**" or multiple "**Metaverses**" or "**MinimaVerses**" as we are talking about minima, those worlds can be exclusively real, virtual or a mix of them, so everyone in some way will have to interact with them, the same way that the actual society has to interact with web pages, banks, credit cards, emails and so on.

That arises a big problem, how to avoid fraud, how to distinguish a machine from a human as the AI is so advanced that will have the ability to supplant identities on the new world that is coming, and how to identify yourself that you are the person that you are claiming to be and how to claim that you are a person but keeping your anonymity?

The other problem is the interoperability with different "Minimaverses" or "Metaverses", countries, games and IoT devices, exchanges, banks, and so on.

Building a common system, considering that Minima will be a mass adoption blockchain, is the smartest option to take into consideration, since one system for the whole world will be available and be able to be used for everyone, such a system will be very cheap to build and free or almost free to use it.

The solution is a UDPOI (Universal Digital Proof of Identity) and UDPOP (Universal Digital Proof of Person).

We are going to focus only on the first one as the second one would be derived from the first one.

How to build an UDPOI system that could be used for the whole world, cheap, easily to use and to develop and quantum secure?

The answer is using the Minima blockchain, a decentralized p2p, censorship and quantum resistant, and infinity scalable network that can run a full-node on a mobile or IoT devices, that has build from its inception with that concept.

With native NFT's token's system and a coin that has nothing to do for controlling the network, as there is no reward to run a node, creating blocks or validating transactions, in that way we can assure that minima will be ever decentralized and ruled by the utility and the applications that people develop over it.

How would work a system like that ?

We are going to consider the cheapest and simple way to build a system like that though there are lots of variations, the easy way is that the network and their users do the job.

Considerations:

- 1.- Everyone implied is running a Minima node.
- 2.- We have a group of people who want to get a UDPOI
- 3.- We have a group of people that act as a pool of validators and every person on that pool has an NFT special token that let him to validate people and a validation Dapp installed on their nodes.
- 4.- There is a DAPP that creates and NFT representing an UDPOI according to a set of conditions.
- 5.- The UDPOI is applied to the people of a Country in this concrete example.

Flow of Events.

1. Alice wants to get an UDPOI
2. Alice install a Dapp that manages the Proof of Identity on his Minima node..
3. Alice select **get an UDPOI** option from the Dapp.
4. The Dapp randomly select **three** validators from the pool of validators and the validation process begins:

Validation process:

1. The chosen validators receive a notification on their Dapp according to that, the validator has the special token that let him to validate people.
2. A validator establish a direct p2p connection to the Alice.
3. A video chat between Alice and the validator is started.
4. Alice show their passport, the photo and his face and whatever conditions were established on the considerations, the validator fulfill this information on a form with the personal data and the rest of conditions to be considered.
5. The validator if everything is correct then finish the process, and a temporal NFT is created with this information and send to the next validator selected (encrypted with the public address of the destination validator)
6. The process goes to step 2 **two** more times,
7. If the all three verification were successfully correct then the temporal NFT created is send back to the Dapp who started the process of getting an UDPOI.

5. The final NFT is generated with the private information of Alice and also the validators implied on the process and it is send to the Alice node(wallet) with special conditions, that the NFT token could not be transferred to anyone and which part of this private information could be public viewable or encrypted with Alice secret's key.

This is a basic approach and there are lot of thing to take into consideration and variations, but as starting point is a good way to begin with.

Things to take into considerations to look over it on other revisions :

- Api to interact with any system to be able to verify UDPOI from any system.
- How to decide what parts of the info embedded on the NFT are private or public and how to make them available to others under demand.
- What if someone change his mobile for a new one?
- Should the NFT be created base on the node ID too ?
- What to do if a mobile is stolen ?
- The NFT will be password protected adding an extra layer of security ?
- How to recover the NFT if it is stolen , as it is unique and cannot be transferred ?
- How to derive from UDPOI to UDPOP being it unique and anonymous ?
- How to deal with the conditions(rules) to satisfy when creating de UDPOI NFT and embedded that info into it, as smart contract or state vars.
- How to make UDPOI only available for specific systems, virtual worlds, games, IoT devices, Minimaverses, Metaverses.....