cAuth by AIM

State of the Art Research Report

Investigation into currently available and in-development solutions that provide authentication using blockchain

Introduction

Idea for cAuth appeared out of necessity to provide a login mechanism for tools our group has created for Cardano Catalyst over the course of a year. These tools include https://cardanocataly.st site with accompanying github organization https://github.com/Project-Catalyst/, discord server and an assortment of community tools (e.g. Proposal Review Tool, Voter Tool and PA/vPA tools) that can be found here: https://cardanocataly.st/tools/

As we didn't want to implement dependency to Web2 we didn't want to use Google, Facebook or Discord for login, joining the password hell was not an option either. Our next thought was to use Atala PRISM, but it turned out it is not production ready and its scope goes beyond simple login. While we are sure that Decentralized Identifiers and Verifiable Credentials will become part of Cardano ecosystem, we don't see this happening in the next 6 months, with widespread implementation taking another 6 months at minimum. Even when we do, we see a use case for the cAuth mechanism, which will ultimately allow people to use any Cardano wallet as a login mechanism, not only DID wallets.

Problem Domain Description

The problem space we are working in is Identity and Access Management (IAM). This domain is trying to solve to problems:

1. Establish who the user is (identity), beyond reasonable doubt
2. Establish what data can this user access

In case of cAuth we are aiming to solve the problem of identity, we leave the problem of Access Management to the website/service using cAuth, as these configurations are site specific they don't need to be managed by cAuth.

Conceptual Landscape of Identity

PGP and Web of Trust

In the early years of the Internet there was an idea that we could have passwordless authentication and therefore trust. It was a program that provided privacy through cryptography and also allowed authentication using private-public key cryptography. PGP had included in it a way of verifying a signature against a public registry. An email or username was attached to a key pair. It was a brilliant approach, but the trouble was in implementation and adoption. PGP was first released in 1991. Fastest PCs were 80846 DX clocked at 50MHz (back when computers still had “Turbo” buttons) and Windows 3.1 was about to be released. Computers were slow, software was buggy and hard to port. (I remember when Windows 98 crashed during a reveal demo).

Once we have the method of encryption and a server where the identity could be checked, how can we be certain that the server wasn’t hacked and identity stolen?

One way would be to have a trusted third-party a secure server guaranteed by some powerful entity a “Certificate Authority” or the distributed trust called “Web of Trust”, here your key would build up reputation by other entities certifying this public key in fact belongs to this entity. So if Bob trusts Alice and Charlie trusts Bob, Charlie will trust Alice, as the web grows the more good interactions Bob has, the more he is trusted. While this is a better solution, it has its own problems, albeit they are at a higher level of sophistication.

First, how do I know that the database I verify against is up-to-date or hasn’t been hacked by a group of malicious actors? How do we make sure that the database is live and maintained and doesn't depend on a third-party’s goodwill?

If these problems sound familiar, it’s because they are the same problems blockchain is trying to solve.

This system hasn’t gained widespread adoption, the majority went with login and password path.

An up to date, open source, implementation of OpenPGP standard (RFC4880) is maintained as GNU Privacy Guard (GnuPG). While used it's not widespread and most commonly used for email encryption. Key servers are hosted by willing organizations (like Ubuntu), so you can find a public key for an identity.

Fast forward 30 years and logins and passwords with some nice usability features sprinkled over the top have become known as "password hell", with databases being hacked, credentials leaked, the need for password managers, and the rise of third party 'walled garden' sign on (via Google, Facebook and others).

Trust over IP

Trust over IP is a vision of a new "trust layer" for the Internet and a foundation with the same name. It was founded in 2020 in response to the current status of trust in the Internet. However it would not be possible without current technological advances, especially in cryptography . It envisions a 4 layer stack of protocols, just like TCP/IP has 4 layers. [Fig.1] and the coincidence is not accidental.

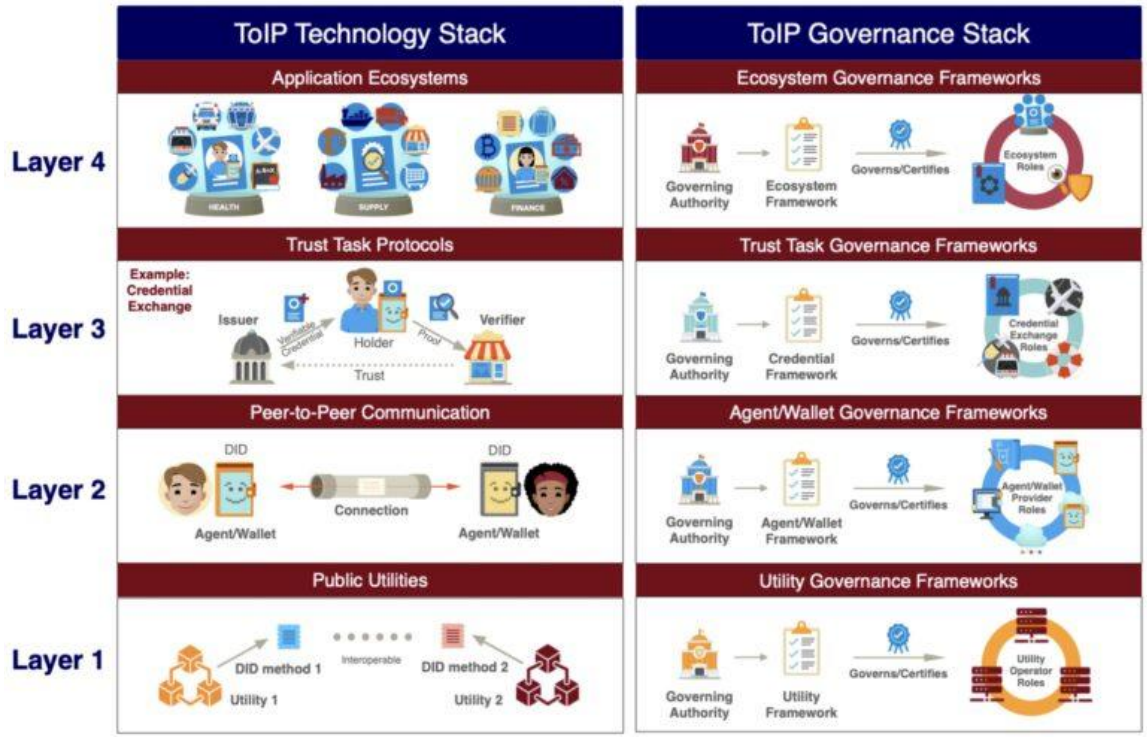

Figure 1. Source: trustoverip.org

Layer 1, on the technical side, is focused on the Decentralized Identifier standard itself, which allows decentralized trust roots to issue credentials. On the governance side, there is a governing authority which creates a framework and allows mentioned decentralized roots to operate. The governing authority could be a government agency or a group of blockchain enthusiasts creating a DAO. The main advantage of DIDs is that you no longer need access to the root utility to know whether the identity is valid.

Layer 2 deals with the way two agents owning DID can communicate. They can establish secure communication using just their DIDs. They can also use them to exchange Verifiable Credentials (eg. they can certify they are both over 18). The governance authority establishes rules and frameworks that providers need to follow and use to be certified. A specification for DIDComm Messaging has been approved by Identity Foundation [2]

Layer 3 deals with data exchange between a holder of data and a verifier of that data, for example a car lending company that wants to verify that a person has a valid driver's license.

Layer 4 deals with whole ecosystems eg. a person getting a better insurance rate, thanks to their health record.

ToIP provides a conceptual framework for discussing decentralized identity.

Regarding cAuth we see it as a simplified Governing Authority (a smart contract) responsible for issuing Verifiable Credentials (NFTs), which can be used either in peer-to-peer (L2) or credential exchanges (L3)

The Network State

It is worth mentioning that blockchain has already led to people thinking about innovating society, one view is the "network state" coined by Balaji Srinivasan, which describes a highly aligned online community. This is an excellent example of how we could have a governing authority that is not a government and how we could establish an ad-hoc organization.

Self-Sovereign Identity, Decentralized Identifiers and Verifiable Credentials

Self-Sovereign Identity and Decentralized Identifier are concepts used interchangeably. It is an alternative to centralized and federated identity infrastructures and is part of the ToIP stack. Verifiable Credentials are a way of verifying a claim without revealing the actual data it's based on (you are over 18 without showing your ID with all your data).

cAuth's approach is to compact a VC into an NFT.

eIDAS 2.0

eIDAS 2.0 is a proposed regulation[4] that is an evolution of eIDAS regulation of the EU. Its goal is to allow every European to have a set of digital identity credentials that are recognised anywhere in the EU.

It has significant problems, like unique wallet IDs (ideal for tracking people and subverting privacy), ability to lock and burn the whole wallet in order to protect eIDAS credentials within and limiting wallet to only hold eIDAS credentials.

Regardless of proposed regulation drawbacks it is clear that Decentralized Identity is here to stay and sooner or later users owning their digital credentials will be the standard. Looking at the state of the documents it's clear that the regulations are in the early stages. The European Commission adopted a Recommendation in June 2021 calling Member States to work towards the development of a Toolbox. Outline[21] was adopted in February 2022 and published for stakeholder feedback. Considering scope of the framework and number of stakeholders, it will take a considerable time (years) until a working solution is created.

VaultPoint: A Blockchain-Based SSI Model that Complies with OAuth 2.0

VaultPoint[5] is a research paper presenting a proof of concept implementation that proposes how a user can authenticate using a SSI using Ethereum blockchain. The user becomes his own authentication server by means of on-device application. Using a widely implemented web2, OAuth 2.0 standard makes it easy to integrate with almost any website or app. This solution is hampered by the Ethereum account model. The data is stored on-chain, unlike Cardano, where metadata can be attached to the UTXO and stored locally.

As a consequence VaultPoint requires multiple connections to the blockchain for every interaction. In case of cAuth we will leverage the local state of the wallet.

VaultPoint presents a valuable use case for further development of cAuth, where the user has the auth NFT stored in a device wallet, in this case a dApp could be used to proxy the authentication.

KILT

Kilt[6] is a protocol and a polkadot parachain. Its main purposes are DIDs and Verifiable Credentials. It is however seriously hampered by the use of account model instead of UTXO, which seriously limits offline capabilities. In order to verify DIDs interaction with the blockchain is required. Other than that it's just a dedicated blockchain for Self-Sovereign Identity.

Hyperledger Aries

Aries[7] Is a toolkit for building developers to build tools for peer-to-peer DID communication, as described in Layer 2 of ToIP. It demonstrates the importance of tooling for widespread adoption. Something to keep in mind regarding cAuth.

Sovrin & Evernym

Sovrin is a purposefully built Hyperledger Indy private blockchain for identity. They have 3 networks with the largest one consisting of 25 nodes. Every write to the MainNet costs $10.

Evernym is a digital platform providing apps and SDKs to the users of Sovrin network.

The network is owned and maintained by a set of private entities. Users own their identity inside the network and can decide and control who they share information with and what they share, but they don't have a say in how the network operates.

Civic

Civic[8] is an authentication platform created as a ERC20 token on Ethereum blockchain, Civic doesn't use DID as a standard, it's a custom solution, focused on solving

authentication, it has a number of integrations, a gateway solution and libraries. It is close to what we have envisioned for cAuth from the usability standpoint.

Atala PRISM

Atala PRISM is a SSI platform for issuing DIDs and VCs running on Cardano blockchain. While an excellent platform with tools, it's still in heavy development and sadly it's a proprietary IOG (IOHK) solution, not Open Source. There is no way to access the platform besides the Pioneer program. While it would be useful to integrate with PRISM, we see a path that will allow us to upgrade cAuth to use PRISM as source of truth. PRISM is a toolset for issuing on-chain. The problem is that all records on Cardano blockchain are public, troublesome if you want to preserve privacy. Therefore you need another mechanism for storing sensitive data. PGP has the same problem, you need a way to share your public keys or verify that certain credentials belong to a certain entity. There is no guarantee of consistency and security, it depends on the good will of organizations hosting the registries, in the end they end up controlling the system. We assume IOG reached similar conclusions, hence they intend to launch Midnight[10].

Midnight

Midnight[10] is a new data protection blockchain that safeguards sensitive data. It is an answer to the dilemma of where to host DIDs, VCs and other pieces of data, which require privacy and protection, without centralizing the architecture.

IAMX NFT Identity

IAMX[11] is a company that aims to provide a user-friendly SSI solution. They have a proof of concept that allows users to generate a DID and place it on IPFS. There is no way to do anything with the DID right now. They mention NFT that can be kept in any wallet, but don't provide any demo. Looking through their github repository[12] we can see examples of how NFTs could be linked to identity. IAMX seems to be aimed at linking NFTs to DIDs, to provide a degree of authenticity to NFTs issued by e.g. celebrities. They have initiated a CIP proposal together with NMKR (CIP-066).

RootsWallet

RootsWallet is an open-source standard based identity wallet developed by RootsID group. It aims to implement Decentralized Identifiers on Cardano. Ideally we would love to integrate with RootsWallet. We don't want to recreate the whole SSI toolchain, we would much rather connect to a dedicated SSI wallet to generate an NFT connected to a specific Identity that can be used in a light wallet to connect to dApps and web2 apps and services using OAuth 2.0.

F7 proposal NFT Based Authentication

Loxe has developed a PoC solution for OAuth 2.0 authentication using NFTs[14]. Our aim is to use their work as a starting point for cAuth to create a more flexible open source solution for creating and using authentication NFTs. While an excellent PoC, it is only a demonstrator of what is possible. We want to improve the smart contract, add a dApp to it and provide a library that can be included in apps authentication. We also want to address additional use cases: expiration, revocation and hopefully federation.

Relevant Cardano Improvement Proposals

Fortunately Cardano has evolved enough to allow building a solution like cAuth. CIPs that are essential to developing cAuth include: CIP 25 [15] which defines metadata format for NFTs, CIP 30 [16] which defines dApp-Wallet Web Bridge, this allows connection between light wallets and dApps, for all intents and purposes there is much similarity between dApps and regular websites.

Conclusions

Self-Sovereign Identity is gaining momentum. This is a clear feature that is missing from Web3. Early attempts like Civic or Sovrin Internet has grown enough

References

1. Decentralized Identifiers (DIDs) v1.0 (https://www.w3.org/TR/did-core/)
2. DIDComm Messaging v2.0 (https://identity.foundation/didcomm-messaging/spec/v2.0/)
3. Trust over IP Whitepaper (https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf)
4. Proposal for establishing a framework for a European Digital Identity (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN)
5. VaultPoint: A Blockchain-Based SSI Model that Complies with OAuth 2.0 (https://www.mdpi.com/2079-9292/9/8/1231/html)
6. KILT Website (https://www.kilt.io)
7. Hyperledger Aries Website (https://www.hyperledger.org/use/aries)
8. Civic Website (https://www.civic.com)
9. Atala PRISM Website (https://atalaprism.io/)
10. Midnight Blockchain (https://midnight.iohk.io/)
11. IAMX Website (https://iamx.id/)
12. IAMX Github (https://github.com/IAMXID/did-method-iamx)
13. RootsID Website (https://rootsid.com/)
14. NFT Based Authentication (https://github.comLoxe-Inc/F7-NFT-based-authentication)
15. CIP 25 - Media NFT Metadata Standard (https://cips.cardano.org/cips/cip25/)
16. CIP 30 - Cardano dApp-Wallet Web Bridge (https://cips.cardano.org/cips/cip30/)
17. CIP 31 - Reference inputs (https://cips.cardano.org/cips/cip31/)
18. CIP 32 - Inline datums (https://cips.cardano.org/cips/cip32/)
19. CIP 33 - Reference scripts (https://cips.cardano.org/cips/cip33/)
20. CIP 54 - Cardano Smart NFTs (https://cips.cardano.org/cips/cip54/)
21. European Digital Identity Architecture and Reference Framework – Outline (https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline)