Plurality

Bringing identity on blockchain while ensuring data privacy

Hira Siddiqui

Mujtaba Idrees

Tobias Jung

Table of Contents

Introduction

Ever since society's adoption of a monetary value exchange system, identification of involved parties has been the cornerstone of every transaction. Today, every monetary transaction is identified and tracked. The government bodies like FATF [1] track the money trails and travel routes via various regulations. Unidentified transactions are not considered legal, and every new value exchange technology, like Blockchain, is judged and examined under the same lens: *"Do we know who is sending payment to whom?"*

Humans trade their identity and personal information for the functioning of the larger society where it's tracked that money is not spent on illegal activities. It's not a bad trade per se, after all, safety is a basic human need. However, as a side effect, certain centralized organizations managing identity become strong enough to collude in manipulating user behavior through pervasive analytics. In some countries, additional legal and technical systems e.g. GDPR [2] have been created to protect individuals from privacy breaches but even then, the system is not bulletproof.

The problem gets exaggerated if you bring online services and social media in the mix. Every account you have online holds traces of information about you. Browsing through the internet, you are leaving digital breadcrumbs of your interests and personality, leaving you vulnerable to targeted advertisements, filter bubbles and in worst cases identity theft.

In the world of Web2, you cannot maintain a digital presence without entrusting your identity to a third-party. However, that is not how transparent systems operate.

> "Transparent systems allow us to operate with trust toward none, with integrity for all."

In 2009, a peer-to-peer transactional system called Bitcoin was introduced. The concept was simple: One world, one global ledger that has transparency in transactions without the need of any centralized party. Fast forward to 2022, we are living in a world where all the internet is shifting to programmable blockchains which are managed and enabled decentrally by the community. We call it web3.

While the key concept of this decentralization and web3 is revolutionary, it lacks one key piece of puzzle i.e., Identity. Blockchains provide pseudonymity – which means that it's impossible to know the actual people behind any transaction. This created two challenges:

1. **Legal Challenges:** The government regulations ask for identification of the sender and receiver in certain transactions – which is not possible natively in blockchain.
2. **Adoption Challenges:** It posed a hurdle in adoption of web3 in traditional use cases like lending, mortgage, social media, insurance etc. For example, how can you create a truly decentralized mortgage platform without knowing who you are lending to?

The legal problems were partially catered by the creation of centralized cryptocurrency exchanges or marketplaces. These exchanges or marketplaces are run by centralized organizations that identify users, let them buy cryptocurrency and crypto assets for fiat and then hold their assets. Examples are Binance, Coinbase, Kraken, Celsius etc. However, the paradox is that for buying the assets of the *decentralized world,* these platforms use the same *centralized* means that blockchain originally set out to disrupt. We basically ended up at the point where we started from.

For the adoption problems, currently, no native identification solution exists. Therefore, the blockchain is restricted as only a financial tool even though it has the potential to provide an improved, decentralized version of every solution we see today e.g., social media, lending, insurances etc. Until there is a native identification solution, the blockchains will be stuck to only being a "bank account".

Lately, there have been discussions around storing identification information on-chain e.g., Soul Bound Tokens (SBTs), however, they also do not solve the problem entirely. Publishing personal identifiable information on-chain has serious privacy concerns as blockchain is immutable. Moreover, it's easy to gather all the information about a single person since everything is public. Human relationships are complex, and so are their identification requirements. Humans have plural relationships with different parties. For example, your employer should not know how much crypto you hold. Similarly, your tinder date should not know which party you voted for.

To provide the ground for the next generation of innovative applications in the blockchain space, we need an identification mechanism that is:

1. **Decentralized**: no single party holds or controls it
2. **Off-chain**: Personal Identifiable Information is not stored permanently on the blockchain
3. **Privacy-preserving**: Protects the privacy of the individual by disclosing only the minimal required identity to the required party.
4. **Plural**: Different subsets of identity disclosed to different parties i.e., plural identity relationship

The decentralized society is not complete without an identification mechanism that's decentralized, protects and respects human beings and their inviolable right to privacy. This final piece of puzzle is enabled by Plurality.

Current state of identity in web3

Web3 has become one of the most protruding terms in the field of blockchain and crypto currencies. In the beginning, the web was “read-only”, which only consisted of unchangeable websites. Users mainly consumed the content in written form. Later it evolved to a state where it was possible for the users to dynamically share content. It is now referred to as the “read and write” web. This iteration of the web produced many popular social media and content sharing platforms which are being centrally managed and owned.

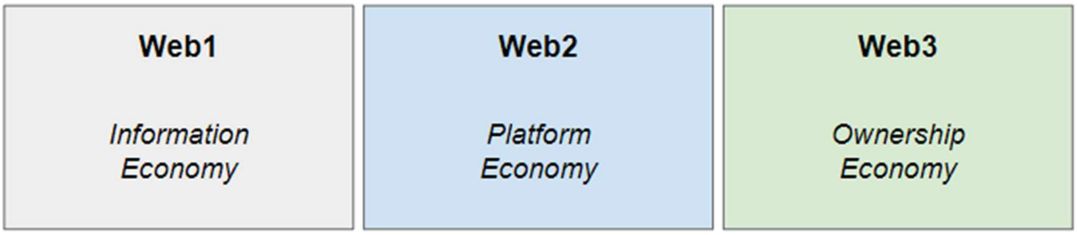

Figure 1 Generations of Web

This is where web3 comes into play, also known as the “read-write-own” web. In contrast to its predecessors, data is not owned by centralized entities anymore, rather it is owned by the individuals. Web3 enables the toolset for platform agnostic data transferability.

Blockchain technology is the backbone of Web3, enabling the trustless and immutable transfer of information. Blockchain networks are distributed ledgers which store information in a decentralized manner bundling sets of information on so called blocks. New information gets summarized into a block and added to the chain. Furthermore, network nodes or miners must reach an agreement on the network's current state. This agreement is reached through a consensus mechanism. Different blockchain networks also utilize different consensus mechanisms. Furthermore, the technology is still evolving and new mechanisms are being innovated.

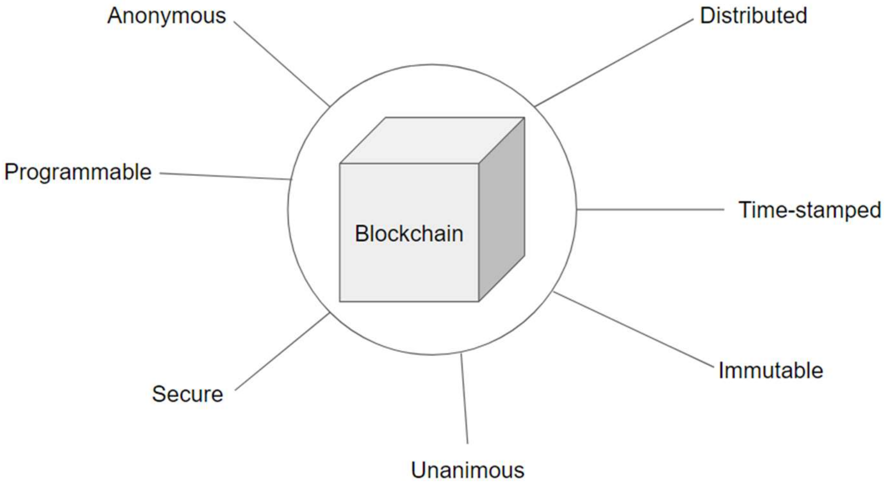

Figure 2 Properties of blockchain

Currently, two of the major blockchain networks are Bitcoin and Ethereum. Bitcoin has established itself as the major blockchain to store value. Ethereum on the other hand, enables decentralized applications (dApps) to be built on top of the blockchain through smart contracts. Smart contracts are programs which, when certain conditions are met, get executed in a decentralized fashion. This mechanism has fostered many new and innovative decentralized finance products. For instance, Automated Market Makers (AMMs) such as Uniswap, or decentralized lending and borrowing protocols such as Aave. All transactions on these dApps are transparently visible on the blockchain.

But this transparency is a double-edged sword. On the one hand, users can access the entire transaction history of the blockchain, enabling every participant to accurately verify information. On the other hand, if we use this same mechanism to store identity information, it is a breach of privacy and it is now fully traceable for everyone. Since Blockchains are also immutable, said information cannot be removed either, leaving users vulnerable to permanent disclosure of their identity publicly.

Moreover, immutability also means that an individual's right to remove identity information cannot be ensured, which is even supported by law in many western jurisdictions. Lastly, since the entire blockchain infrastructure is decentralized, the accountability of data protection cannot be pinned on any single party.

This creates a protruding data privacy paradox, where the current properties of public blockchains render them very difficult to be used as-is for identity management.

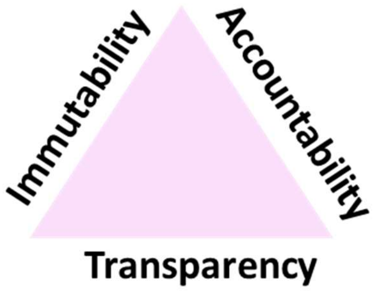

Figure 3 Data Privacy Paradox

But that doesn’t mean that the current centralized identity systems are perfect for usage.

When it comes to the current centralized systems, it has been proven time and again that the identity information can be misused through either malicious intent or attacks. In the past, millions of users have been affected through hacking attempts on social media platforms such as LinkedIn or Facebook proving that the current centralized systems cannot be trusted with identity information. A recent bankruptcy filing by a centralized crypto assets marketplace celsius leaked the identity data of thousands of users along with their crypto holdings [13].

On the other hand, if you study the current Know-Your-Customer (KYC) mechanisms, the information sharing procedures are very repetitive. A user needs to do KYC for each new organization making it costly and time consuming.

Thus, when it comes to identity and data privacy, there is still much room for improvement. We need a decentralized, privacy-preserving identification mechanism that removes redundancy in the current identification mechanisms and can take advantage of the immutability, transparency, and decentralized accountability of the blockchains while evading the challenges that come with them.

The next generation of identity management

The identity of a person is defined by relationships one has with different parties in different contexts. All these relationships contain a persona of an individual which can be summarized in the form of certain attributes. For example, one can have an *employee* relationship with an organization and at the same time can have an *owner* relationship with a buildings consortium where one owns a flat.

Hence, due to its complex nature, the identity of a person cannot be defined as a database file on a centralized server. The correct way to manage identity digitally would be to give users the control to manage, store, and share their identity at their will. The digital approach to identity should be analogous to the way it was being managed in the physical world. In the physical world the identity cards were issued to the users, and they were expected to manage and store them in their wallets and vaults. The users were always in control of how, when and to whom this identity information was revealed. This approach to manage user identity is often referred to as self-sovereign identity.

Self Sovereign Identity (SSI)

SSI allows individuals to control and own their information. Moreover, users only need to share the bare minimum of information needed for identification. Verifiable credentials (VCs) are issued by the organizations to the identity owners. VCs can be an accreditation of rights, certificates or privileges which are normally handed out in written and signed form. In other words, they are a means of identification. In short, SSI enables a privacy preserving digital identification system.

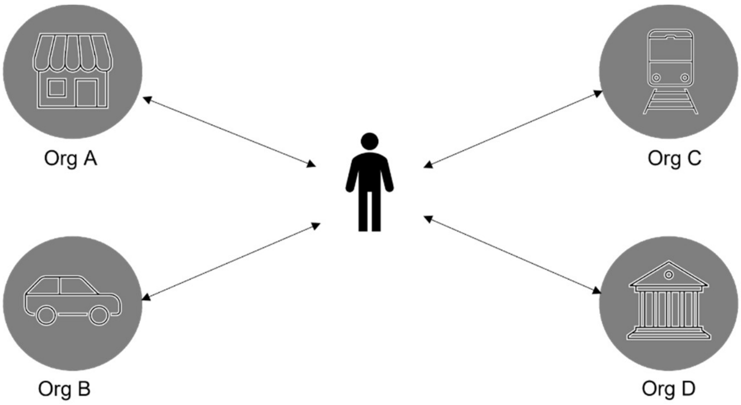

Figure 4 User in control of identity

SSI Ecosystem – Roles

In a typical SSI system, there are three crucial parties involved in enabling this process of identification:

1. **Holder** is the user, who owns the information. It can be an individual, a company or an organization.
2. I**ssuer** is an entity (organization, government, certifier or company) with a level of trust that issues verifiable credentials to the holders. The issuer is the attestant of the information about holder. For instance, a government issues passport to citizens.
3. **Verifier** is the entity, to whom the holder needs to prove the legitimacy of the information. For instance, a bank in need of identification of the holder.

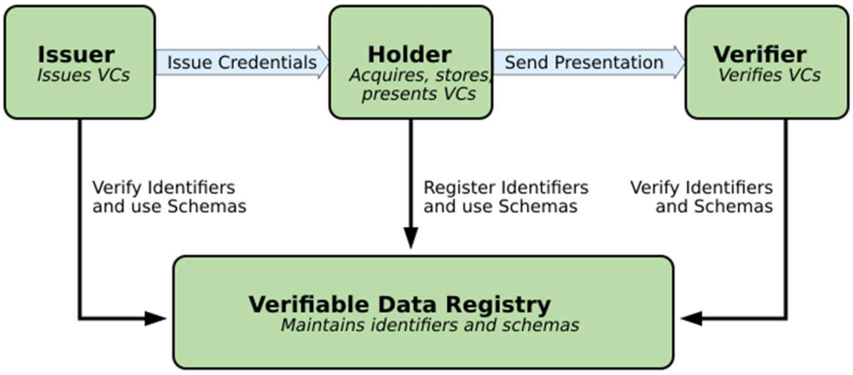
Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintains identifiers and schemas

Figure 5 SSI Ecosystem - Roles [14]

Verifiable Credentials (VCs)

VCs are the digitized, standardized, and signed version of real-life credentials such as passports, degrees, or certificates of vaccination. Therefore, they are the foundation of secure and instant access to digital services.

VCs can be verified through standard cryptographic signature schemes. Issuers sign VCs with their private key. The verifier can use the issuer's public key to check the validity of the signature.

VCs, oftentimes hold more information than needed by the verifying entity. In some cases, not all information needs to be shared. For example, to enter a club, one needs to prove that he/she is over 18 years of age. This can be done by only revealing the date of birth attribute from the ID Card credential. This is the concept of **selective disclosure**, i.e., no information should be shared beyond what is truly necessary. Similarly, a more privacy preserving approach could be that one can prove cryptographically that they are over 18 years of age without even revealing their date of birth. This can be achieved via **Zero knowledge proofs**. The holders can choose the level of privacy they want while verifying their identity to a verifier.

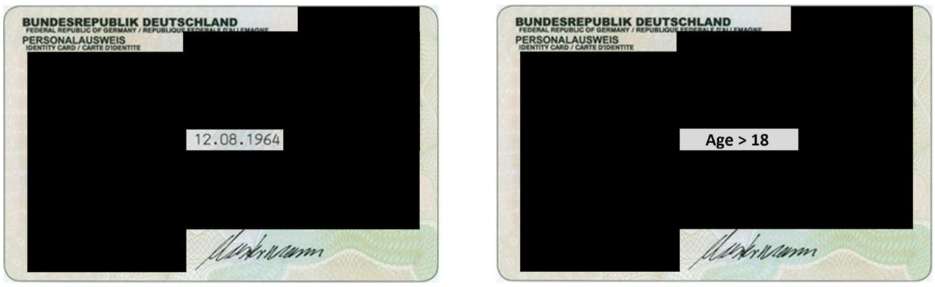

Figure 6 Selective disclosure vs zero knowledge proofs

Decentralized Identifiers (DIDs)

DIDs are cryptographic identifiers which are trivially used in an SSI based system to publicly identify the involved entities (Issuers, Holders and Verifiers). Multiple distinct DIDs can be generated by an entity using the same seed while it is virtually impossible to correlate between any two DIDs from the same entity. This property of **correlation resistance** acts as a cornerstone of ensuring privacy in SSI systems.

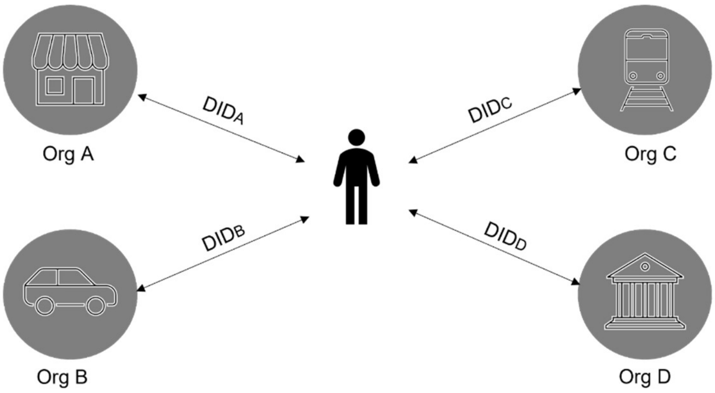

Figure 7 Correlation resistance in different interactions of a user

The main idea of DIDs is that the entities use a different DID in every relationship. For example, a holder would use a different DID while interacting as an employee with his employer organization and a different DID to interact with the building consortium as a flat owner. DIDs ensure that even if these interactions are put on public ledgers nobody would be able to identify that there is the same holder behind these interactions.

Plurality enables web3 identity

High Level Overview

Blockchains were created to remove the need of a centralized party for transactions between two parties. Identity is one of the biggest use cases in the decentralized world that can revolutionize the existing applications and pave the way for new innovative solutions. However, 13 years have passed since the development of the first blockchain, Bitcoin, and we still rely on centralized parties to identify the users on the chain.

Plurality removes centralization for identification of users, enabling blockchains to fulfill the promised vision of a decentralized society.

Using plurality any blockchain address can prove its identity to any other blockchain address in a privacy preserving manner without any centralized provider. This other blockchain address can represent either a person or an entity.

To achieve this, we are creating the **plurality wallet**, which is a blockchain aware identity wallet. Plurality wallet is aware of both blockchain and identity worlds; giving it the ability to hold your credentials and interact with your blockchain wallets.

Design Principles

Plurality was created with the following design principles:

- **Privacy preservation**: No Personal Identifiable Information (PII) would be stored on-chain. This principle is of paramount importance because blockchain transactions are publicly visible and immutable. Therefore, proposed solutions such as soul bound tokens are unsuitable for identity information.
- **User centricity and control:** Identification process should be user-first. It should be easy and transparent for users to disseminate their information. They should be in control of who is viewing how much of their information.
- **Trust minimization:** The system should follow the principle of minimal disclosure i.e., to only share as much information as needed.
- **Easy adoption:** Decentralized applications that are already in production should be able to integrate this identity system with minimal effort.
- **Blockchain agnostic**: The system should be able to support multiple blockchains without redesigning the entire system.
- **Built-in decentralized scalability:** There should be a built-in incentivization model for our infrastructure providers to ensure decentralized scalability.

Bridging the identity and the blockchain world

Plurality wallet has created a novel approach to pair your credentials to your blockchain address in a provable way - without compromising on privacy.

To understand how plurality does this, let’s assume an example where Alice wants to prove to Bob that she lives in London. She can do this easily by revealing to Bob her residence card. Or, if she wants to be more privacy preserving, she can use the technique of selective disclosure as explained previously.

However, if she also wants to prove that she is the owner of a certain blockchain address, all she needs to prove is that she also knows the secret of the wallet i.e., the private key.

To do this, we use the battle tested concept of public key cryptography known as signing.

$$\textbf{Sign}_{\text{BlockchainPrivateKey}}(\text{VerifiableCredentialProof})$$

Alice creates a VC proof of her residence city and then signs it with the private key of the blockchain wallet.

The actual signing implementation contains more nuances to cater to various attacks like replay etc., the details of those would follow in technical deep dive.

Once Bob receives the proof from Alice, he will unpack it with the public key of Alice and then verify the proof. If the unpacking of proof is successful, this means that Alice indeed was the creator of the proof since she was the only one who knows the private key of her blockchain wallet. This way, Bob would know whether Alice lives in London and what her public blockchain address is.

Use Cases

Currently, some use cases from the web2 world have been onboarded into the web3 ecosystem. However, it is not possible to onboard many other use cases due to the lack of a censorship resistant and safe digital identity mechanism providing individuals sovereignty over their personal data and information. Moreover, this limitation is also restricting the creation of new innovative use cases and large scale adoption of web3.

An identity layer is crucial to further develop the existing ecosystem of anonymity into an ecosystem of plural sovereign identity. Plurality will enable a spectrum of identity within web3 catering to everyone’s needs. From state citizen to guild leader to NFT artist, plurality serves all.

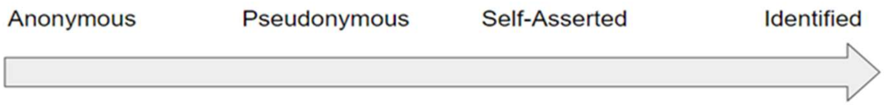

Figure 8: Spectrum of identity

Since one's real-life identity is just a part of one's plurality (web3 identity), use cases can be distinguished between the level of identification needed.

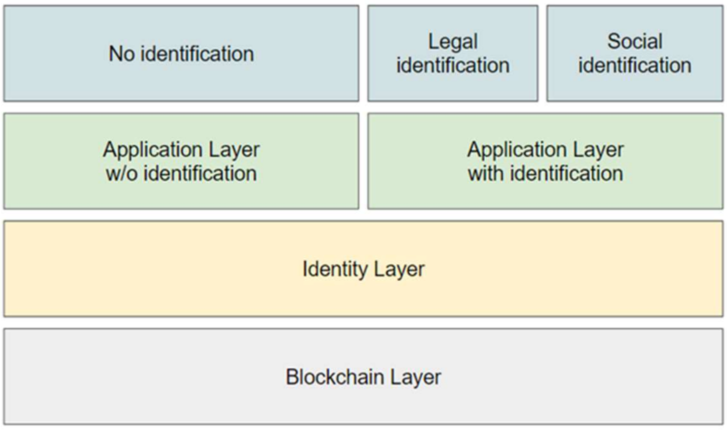

Figure 9: Layers of decentralized applications

We have identified two major domains for the plurality use cases. First are the use cases that need legally compliant identification mechanisms. The second category is of the use cases where identification can improve adoption and trust, but is not strictly necessary from a legal point of view. We differentiate these two categories as legal and social identification.

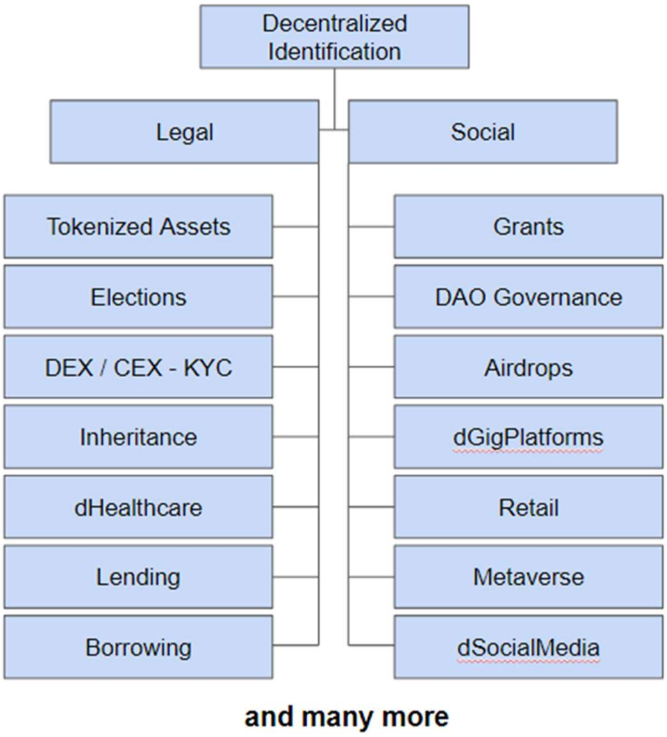

Figure 10: Identification categories

Social Identification

Social identification will prove beneficial for use cases that involves people to people interaction and requires trust between the transacting parties. This trust can be provided by plurality by enabling the parties to identify each other whilst ensuring their privacy. Social identification will enable web3's *use cases of tomorrow* and will be paramount to the widespread adoption of web3. Let's discuss some of these use cases.

Decentralized Autonomous Organizations (DAO)

In DAO governance, multiple problems protrude within the current status quo. DAO governance relates to the decision-making process within a decentralized organization. Even though there are already attempts to diversify decentralized governance procedures, the main form of governance lies within token vote, where the voters share of tokens represents their decision-making stake within the organization. Now, this comes with many problems.

First, token distribution. Oftentimes token distribution is heavily centralized amongst a tiny majority of token holders in comparison to many token holders with very limited voting power. Not only does this lead to little participation in governance, but also in governance directed by a few personal incentives rather than a collective decision-making process. In other words, there is no real decentralized governance. If we use identification via plurality where we can ensure that every unique address in DAO is a unique person, this problem can be resolved. This will give rise to a new mechanism of *people-vote* instead of *address-vote*, decentralizing the DAO governance in the real sense.

Airdrops

Currently, airdrops are used to reward initial users of a platform or to promote adoption. It is fairly easy to manipulate the current airdrop mechanisms by various hacks e.g. creating multiple wallets and interacting with the protocol. With the identification mechanism of plurality, *proof of personhood* can be made mandatory to receive the airdrops by disclosing an attribute from your identity in a privacy preserving manner.

Decentralized Job Marketplaces

Plurality can enable a new wave of use cases powering the next iteration of web3 necessary for adoption of the masses. In the area of education, through SSI, trusted universities could issue their credentials in a decentralized manner, expanding one's plurality and one's opportunity. At the moment, many foreigners run into complications when trying to prove their credentials to foreign employers. Paper documents can more easily be faked than a digitally issued credential by an entity of trust, so the processes involved in proving correctness right now, are of huge burden limiting opportunity for many people.

Moreover, using plurality, the whole job market could become more globalized by creating decentralized job marketplaces or gig platforms like dFiverr, dUpwork etc. On these platforms, the employer and employee could mutually identify and review each other based on the educational and professional verifiable credentials without involving a centralized party. Plurality will open doors for people from disadvantaged locations all over the world.

Decentralized Social Media

Verifying your identity on platforms like Tinder or Twitter involves centralized intermediaries. Moreover, your content is not yours as it can be censored or removed without your input. Decentralized use cases like dTinder, dTwitter and in general, dSocial Media will emerge and spread once plurality enables social identification.

Retail

Currently, when purchasing items online, in online stores such as Amazon, you are required to create an account and share personal data with the platform. There will be huge improvement once it is possible to simply connect your wallet holding your digital assets and your identity. Ownership of the data, such as name and address, will stay with the user and they will be able to use their digital assets to purchase real life goods.

Metaverse

As of now, the metaverse is a very broad term and not yet fully defined or established. But assuming the metaverse is a new form of virtual reality building on blockchain technology, there need to be identification mechanisms in a privacy preserving manner enabling the use of your various identities, the use of your plurality.

Overall, there will be numerous use cases. In the long term even governmental voting, health care documentation or even educational certification systems will emerge. In the end, privacy preserving decentralization fosters a global environment of equality, trust and transparency building upon the foundation of plurality.

Legal identification

Legal identification will be required by use cases that are bound by law to be compliant with certain regulations e.g., KYC and AML. Compliance with these regulations is not only expensive and hard, but is also deterring web3 to onboard some of the major financial use cases of the web2 world.

A huge amount of wealth today is locked in so-called illiquid assets like real estate, land, commodities, private equities etc. Some of these asset classes are limited to only the wealthiest individuals due to the necessity of large investment amounts.

	What is tokenized?	**Who tokenizes?**
Traditional Assets	Public Markets ● Real Estate ● Public Equity ● Fixed Income ● Commodities	● Investment Banks ● AMCs
On Chain Assets	Private Markets ● Pre-IPO stock ● SME revenues ● Public infra ● Private debt ● Private funds ● Wholesale bonds ● Digital assets ● Physical art ● Exotic beverages	● Asset originator ● Tech companies ● Protocol developers ● Private market exchanges

As an individual, getting access to these investment instruments is difficult. Apart from complex tokenization processes and stringent guidelines with access to certain asset markets, the process of gaining access is very complex due to compliance set ups across multiple centralized platforms. Overall, there is a lack of technologically scalable solutions enabling an efficient and compliant process available to everyone. A lack of privacy preserving identification will hinder web3 at its next iteration and hence could become a bottleneck for adoption. We believe that plurality will play a major role in expanding the reach of web3 use cases.

Potential for Plurality's Legal Identification

Conservatively speaking and only looking at use cases in need of legal identification, by 2030, the market value of tokenized assets can be predicted to be around 16 trillion $USD. Currently it is around 310 billion $USD and current solutions are neither scalable nor privacy preserving.

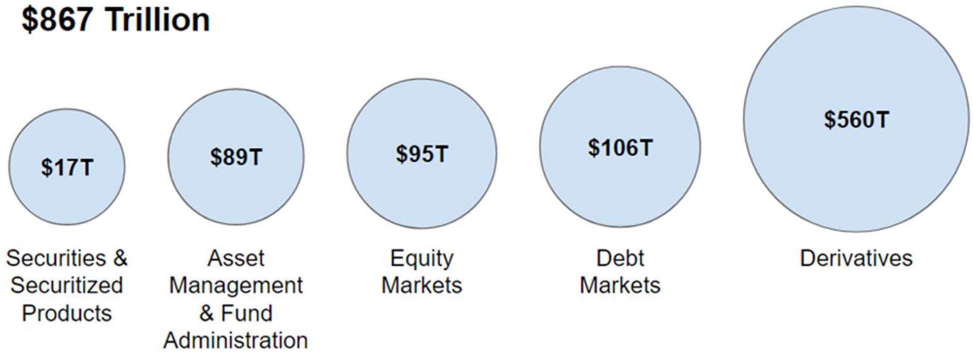

Figure 11: Value disrupted by web3

Adding to that, the recent BCG and WEF insights report [11] has predicted the total value to be disrupted by web3 to be $867 Trillion. This disruption value can be further broken down into several key areas as shown in Figure 10.

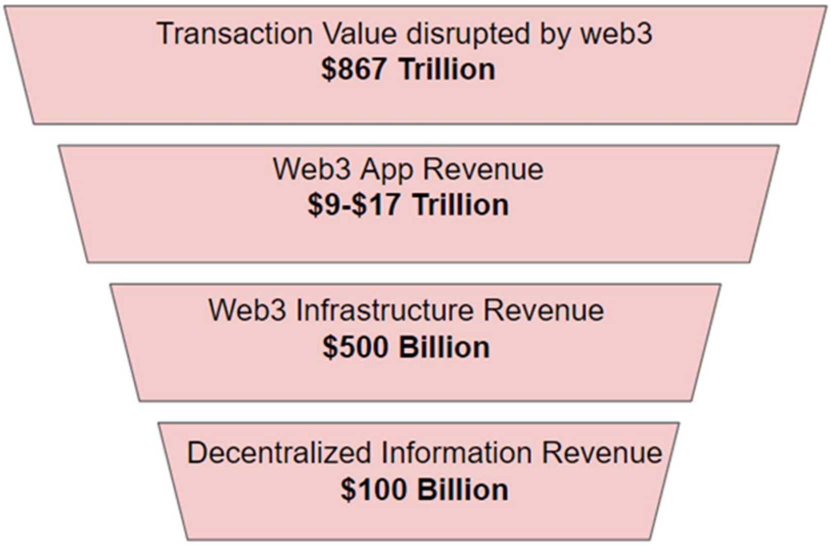
Transaction Value disrupted by web3
$867 Trillion
Web3 App Revenue
$9-$17 Trillion
Web3 Infrastructure Revenue
$500 Billion
Decentralized Information Revenue
$100 Billion

Figure 12: Breakdown of transaction value disrupted by web3

Web3 applications will likely capture 1%-2% of the value that is facilitated through them, which is in line with current rates at which the banking industry generates revenue [12]. Breaking this further down, web3 infrastructure will capture approximately 3% of said revenue through enabling those applications, which is comparable to web2 infrastructure services. It is expected that 20% of infrastructure revenue will flow into decentralized information networks. Here, Plurality will be a center infrastructure piece.

Let’s further discuss the use cases for legal identification.

Trading

Automated Market Makers enable users the possibility to trade different tokens against each other. However, these tokens are still only blockchain native tokens. In other words, trading is limited to stable coins, governance tokens and the blockchain native currency token. But there is way more potential through tokenization and exchange of real life assets on the blockchain. For instance, trading securities or properties. But trading those requires authentication mechanisms.

Borrowing & Lending

Currently the ability to borrow value in defi is very limited. One can only receive overcollateralized loans. Therefore, it is not yet possible to produce loans as we know them from real life on the blockchain. Decentralized identity is needed to overcome those limitations and expand possibilities of the web3 ecosystem.

Privacy Protocols

Public blockchains, as the name suggests, are public. Therefore, each transaction can be traced. Privacy protocols are trying to solve these issues but are also facing major problems through regulators who are trying to minimize money laundering activity, which is getting enabled through these privacy mechanisms. A privacy preserving identification mechanism may enable more possibilities in the realm of privacy protocols and compliance requirements.

Overall, there will be numerous use cases. In the long term even governmental voting, health care documentation or even educational certification systems will emerge. In the end, privacy preserving decentralized identification fosters a global environment of equality, trust and transparency building upon the foundation of plurality.

OWN your plurality and CHOOSE who to share it with.

Technical Deep Dive

Plurality ecosystem

The plurality ecosystem consists of several different types of roles and components. We will discuss each role and component in detail in this section.

Layers of architecture

The system architecture of plurality consists of multiple layers:

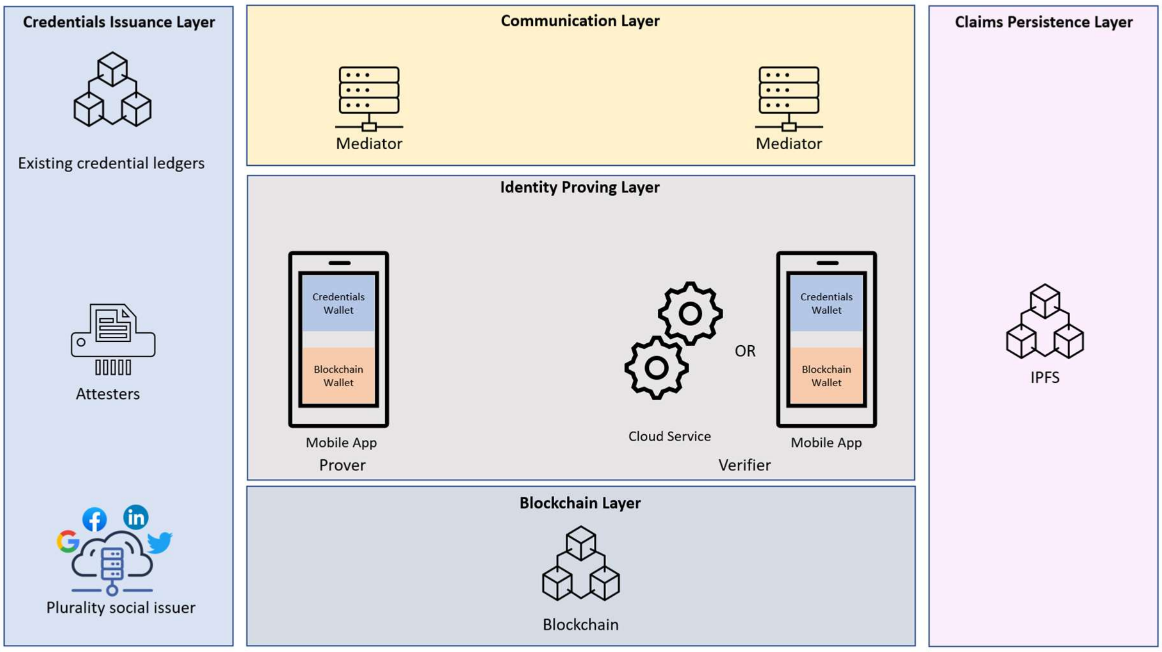

Figure 13 Layers of plurality ecosystem

Identity Proving Layer

The identity proving layer will consist of plurality provers and verifiers. The verifiers can either be another person with a mobile wallet or a decentralized application with a cloud verifier.

Communication Layer

The communication layer used in plurality is based on DIDComm [15] that is a peer to peer communication protocol developed specifically for SSI use cases. Provers and verifiers cannot directly communicate with each other without a communication channel. This communication is established using mediators which are servers that forward the messages between provers and verifiers without knowing about the information in the message. The communication layer is used to transmit the proofs from the plurality provers to verifiers.

Further details of this communication can be found in the infrastructure section.

Credentials Issuance Layer

In order to prove something to a verifier, the provers need to have the required credentials in their wallet. These credentials are issued through the components in the credentials issuance layer.

The issuance layer has three possibilities from where to get credentials:

1. Government credentials from existing credential ledgers
2. Attested credentials from third-party attestors
3. Social credentials from social media accounts

Existing credential ledgers are networks like BCGov, IDUnion, Sovrin Network, EBSI, ESSIF, KILT, Ceramic etc. which are operated by different governments and corporate consortiums. Various governmental and non-governmental issuers are registered on these ledgers that issue official documents as a verifiable credential. Moreover, we have multiple projects like GAIA-X, Catena-X, EUDI Wallet, Ecosystem of digital identities by Germany etc. which are directly or indirectly developing the SSI ecosystem based on W3C standard verifiable credentials. The plurality wallet is being developed fully compatible with W3C verifiable credential standards and that is how it will be able to receive credentials from existing issuers.

Attesters are companies that have the licenses to do Know-Your-Customer (KYC) checks for people. These companies can manually check identification documents from users once and then issue them a verifiable credential for each of their documents. Attesters will be used in cases where the required documents can not be imported as verifiable credentials.

The third possibility is getting a social credential by logging in the plurality app using social media accounts. The app will use oauth protocol to sign in and then plurality issuers will issue the corresponding social SSI credential.

Blockchain Layer

After a proof has been verified, the verifier can store the verified addresses on blockchain.

It can be read by any other smart contract on the blockchain and can be used to allow decentralized apps to read this information and make decisions about who to give access to their on-chain service. The details of the plurality smart contracts on chain will be covered in the decentralized mediation protocol section.

Claims Persistence Layer

After a proof has been verified, the verifier can optionally store an encrypted backup copy of the proof. This backup is optional and can be used for logging purposes or for compliance reasons.

Mediator Nodes

Plurality ecosystem will have a pool of decentralized mediators that anyone can setup and run by providing some stake in the plurality ecosystem.

A mediator is a special server that acts as a participant in the communication between a prover and a verifier. It has its own keys, and anyone can request it to mediate communication between two parties.

Every message that a mediator gets is encrypted with its public keys. Mediator decrypts it with its private key, finds information where to forward it, and sends it to the relevant party.

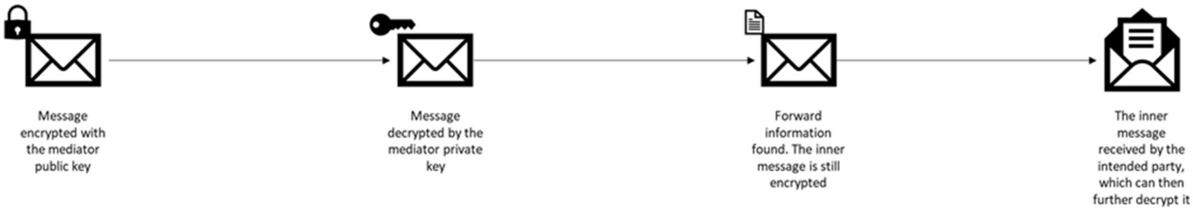
Message encrypted with the mediator public key
Message decrypted by the mediator private key
Forward information found. The inner message is still encrypted
The inner message received by the intended party, which can then further decrypt it

Figure 14 Decryption of a packet as it travels through mediator

Mediators are used for several reasons in the plurality ecosystem:

- **Notifications:** Communication between mobile phones is not straight forward. The reason for that is that mobile phones are not always-up servers. Their charging can die, they can switch networks and do not have a fixed IP address. Therefore, the other communicating party doesn't always know where to send the messages to. For this reason, a mobile phone can register itself with a mediator, which is an always-up server, and then tell the communicating party to always send the messages intended for him to this specific mediator. The mediator receives the intended messages for the phone, and then sends it to him. If the phone is unreachable for any reason, the mediator will queue the messages for him and try to send again at a later point in time.
- **Privacy of messages:** The messages sent to a mediator are always sent encrypted with the mediator keys. This means that even if somebody snoops a packet in-flight, they will not be able to make any sense of it. The mediator simply unpacks the message, sees who to forward the packet to, and then sends it there. No other information is revealed during the whole communication process.
- **Privacy of sender:** Since many mobile phones may use the same mediator, therefore, the messages get lost in the crowd and it's difficult to know which message originated from whom. This is good to protect the privacy of the sender.

In the plurality ecosystem, anyone can become a mediator and will be compensated depending on their quality of service and how many proof communications they enable.

Decentralized Mediation Protocol

The vision of a decentralized society cannot be complete without a decentralized identity protocol. Therefore, the decentralized mediation protocol is a protocol designed for bringing Self Sovereign Identity into the blockchain world.

It's a protocol that:

1. Creates a decentralized infrastructure to handle the identity ecosystem
2. Allows anyone to become part of the identity infrastructure
3. Incentivizes entities running identity infrastructure
4. Promotes scalability by ensuring monetary benefits to infrastructure providers

The decentralized mediation protocol is enabled by a mediator pool and a set of smart contracts on the blockchain. Let's dive into the details.

Registration of mediators

For the registration of mediators, we have a smart contract on blockchain called mediator contract.

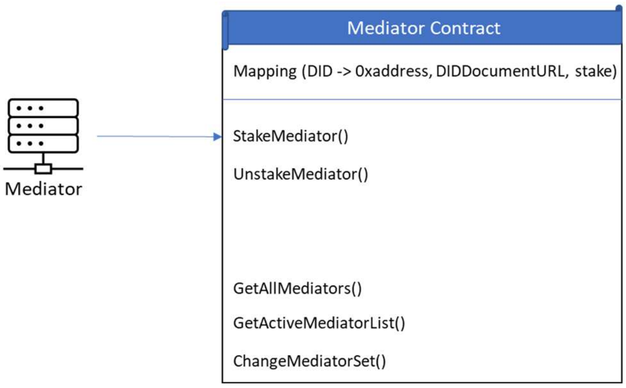

Figure 15 Registration of a mediator on the plurality smart contract

Any person or organization can set up a mediator and then register on the mediator contract by providing some predetermined stake. This stake would be paid in Plurality tokens.

Apart from the stake, the mediator also provides a Decentralized ID (DID), a URL where to find the DIDDocument and a blockchain address.

Once the stake is submitted and information is provided, the smart contract will add the mediator to the active mediators list.

At any later point in time, the mediator can unstake and exit from the system.

Health monitoring of mediators

The coordinator is an independent entity that is handled by the Plurality ecosystem. The coordinator is responsible for monitoring the health and uptime of the mediators and checking if any of the mediators are not up according to the Service Level Agreements (SLAs).

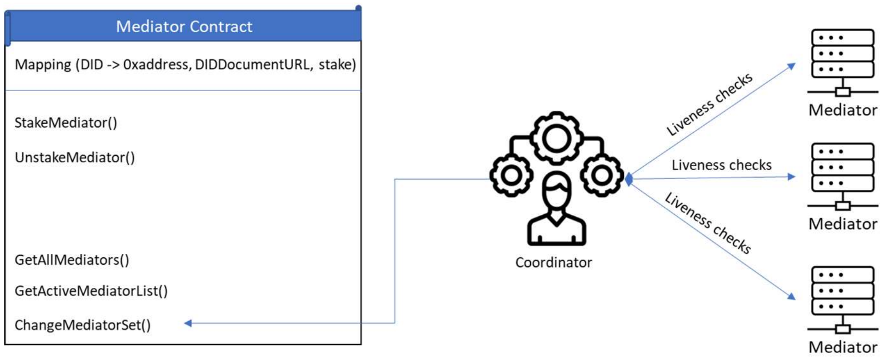

Figure 16 Health monitoring of mediators by the coordinator

If the coordinator realizes that a certain mediator is not running properly for a certain time, it calls the mediator smart contract to remove this mediator from the active mediator list. This is done to protect the users of the system to face lags or downtimes when they select mediators for communication.

If a mediator is repeatedly not a part of the active mediator list, there will be slashing from the deposited stake. Details of the slashing will be covered in the section economic model.

Once we have a mediator pool setup and registered, there are two workflows where mediators are involved. These are:

1. Prover to Verifier communication
2. Holder to Issuer communication

Let’s discuss them one by one.

Prover to Verifier communication

Creation of a proof template

Every time a verifier needs to ask a prover for a proof, he needs to make sure he has a proof template published on the blockchain.

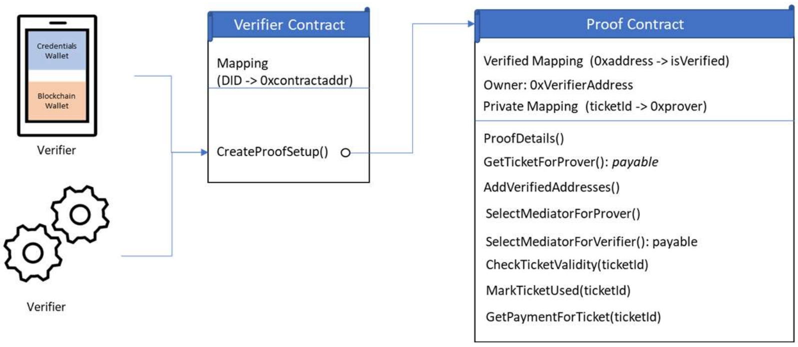
Credentials Wallet
Blockchain Wallet
Verifier
Verifier
Verifier Contract
Mapping
(DID -> 0xcontractaddr)
CreateProofSetup()
Proof Contract
Verified Mapping (0xaddress -> isVerified)
Owner: 0xVerifierAddress
Private Mapping (ticketId -> 0xprover)
ProofDetails()
GetTicketForProver(): payable
AddVerifiedAddresses()
SelectMediatorForProver()
SelectMediatorForVerifier(): payable
CheckTicketValidity(ticketId)
MarkTicketUsed(ticketId)
GetPaymentForTicket(ticketId)

Figure 17 Proof setup by a verifier on blockchain

To do this, the verifier (either a mobile app or a cloud verifier), needs to call the Create Proof Setup function on the verifier smart contract. The verifier needs to provide all the details needed in the proof e.g., age should be <18 and should be provable via a European ID Card etc. This would be a paid function which would require verifiers to spend PL tokens.

Once the verifier calls this function, a dedicated proof contract is created and deployed for this specific proof template. The owner of this proof contract is the verifier.

This contract contains a list of verified addresses that only the verifier can add. Moreover, it also has a couple of functions to enable the mediator selection and communication between the prover and verifier.

Selection of mediators for verifiers and provers

Using the functions of proof contract and mediator contracts as shown above, the mediators for verifier and provers can be selected.

When the verifier wants a prover to prove something, he needs to send the prover a simple hash i.e. a proof address. This address would be a so-called invitation that would contain the following information

1. Verifier service endpoint
2. Proof requirements
3. Proof of payment so that the prover can select a mediator.

Our economic model is such that the verifier always pays the mediators for the entire communication, not the prover.

The following are the steps taken for the mediator selection:

- **Verifier selects mediator for itself using SelectMediatorForVerifier() function:**

  The verifier pays in plurality tokens when calling the SelectMediatorForVerifier() function. This function calls the GetActiveMediatorList() function from the mediator contract to get a sorted list of active mediators. The sorting happens based on the stake of the mediator and the quality of service of the mediators. One mediator from the list of top mediators will be selected using mediator selection protocol.

  The payment done in this step will be used to pay the mediator that has been chosen for verifier after successful proof transmission.

This step only happens when the verifier is a mobile app. When the verifier is a cloud service, it doesn't need its own mediator.

- **Verifier creates a mediator ticket for Prover using GetTicketForProver() function:**

  The verifier then calls GetTicketForProver() function and pays in plurality tokens. This creates a ticket id entry in mapping for a specific prover, which will allow the prover to use a mediator for proof transmission without paying for it, since the verifier already paid. The verifier pays the fees for mediator usage + some extra fees as deposit which will be explained in the next steps.

  After this step, the verifier creates a proof invitation and embeds the ticket id in it. Then, it sends it to the prover off-chain.

- **Prover selects mediator using the SelectMediatorProver() function:**

  The prover calls the SelectMediatorProver function with the ticketId without paying anything. The function checks if there is an entry in the tickets private mapping for this prover address.

  If the function finds such an entry, it gets the ActiveMediatorList from the mediator contract and then chooses one of the top mediators using mediators selection protocol.

- **Prover provides this ticketId to the mediator**

  The prover contacts the mediator and provides the ticketId. The mediator will then call the function CheckTicketValidity(ticketId) to check whether the ticket is valid and intended for it. If yes, the mediator will know that its fee is paid and it needs to serve this request.

- **The proof reaches the verifier and it completes the transaction**

  Once the request reaches the verifier, the verifier needs to call the function MarkTicketUsed(ticketId). This removes the ticketId from the mapping and refunds the extra deposit of the verifier that was paid in step 2. Then, the verifier adds the verified address in the smart contract using the AddVerifiedAddresses() function.

  The extra deposit acts as a security fee that incentivizes the verifier to update the mediator contract for completion of identification. After an epoch the mediators are able to withdraw their rewards for completed identifications.

  If the prover never sends the proof and the ticket is unused, then after completion of the epoch, the verifier can reassign this ticket to some other prover address. The payment of the verifier does not get wasted.

- **Payment of Mediator Services**

  After the mediator completes the proof communication between the prover and verifier, it can then ask for its payment using the GetPaymentForTicket() function. The mediator will send the ticketId and if the ticket has been closed, then the mediator will get his payment on its blockchain address.

Holder to Issuer communication

The holder to issuer communication works in a similar fashion to prover to verifier communication. One difference is that in the earlier scenario, the verifier pays for the mediator services. However, in this case, the holder pays for the mediator services since the holder wants verifiable credentials from the issuer.

The following are the steps taken for the mediator selection:

- **Holder selects mediator for itself using SelectMediatorAndCreateTicket() function:**

  The holder pays in plurality tokens when calling the SelectMediatorAndCreateTicket() function. This function calls the GetActiveMediatorList() function from the mediator contract to get a sorted list of active mediators. One mediator from the list of top mediators will be selected using mediator selection protocol and a ticket for that mediator will be created in that mapping. Once the mediator completes its mediation job, it can then then claim its payment using the ClaimMediatorPayment() function. It will mark the ticket as used and give the payment to the mediator.

- **Holder pays for issuer services by creating a ticket for issuer using the CreateTicketForIssuer()**

  The holder pays in plurality tokens for creating a ticket for the issuer. This would allow the issuer to check using the smart contract that payment for its services have already been done. After the issuer issues the credential to the holder, it can then claim its payment using the ClaimIssuerPayment() function.

Workflows

Now let’s take a deeper dive into the various workflows that allow our users for identity verification.

Credential Issuance Protocol (CIP)

The credential issuance protocol refers to the process using which a plurality user can get credentials.

Plurality will support multiple channels from where to get credentials. These channels are:

- Issuers which support government credentials
- Third party attestors that can attest your physical credentials and provide you the equivalent SSI credential
- Plurality social issuers that can issue a social credential when the user logs in a social media account through the mobile app using oauth protocol

No matter which issuance channel the user decides, the issuing of credentials will occur according to the W3C SSI standards.

The process is simple and can be seen in the following diagram:

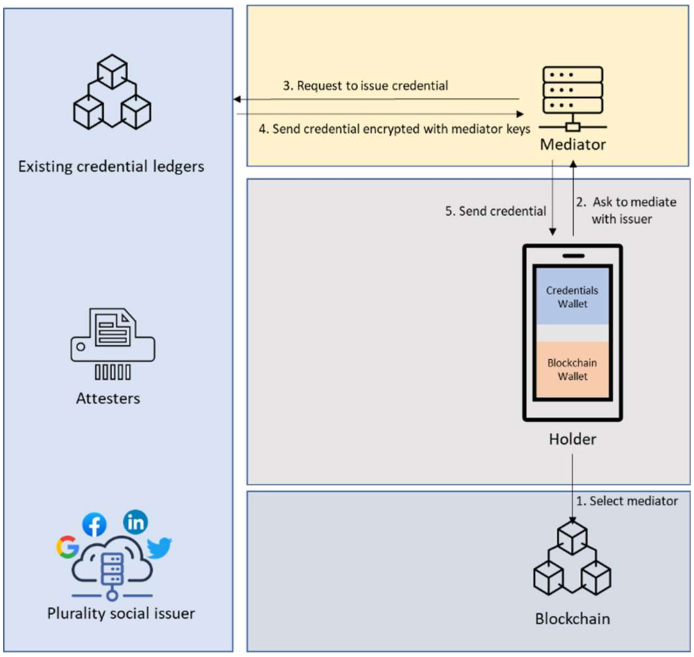
Existing credential ledgers
Attesters
Plurality social issuer
3. Request to issue credential
4. Send credential encrypted with mediator keys
Mediator
5. Send credential
2. Ask to mediate with issuer
Credentials Wallet
Blockchain Wallet
Holder
1. Select mediator
Blockchain

Figure 18 Holder requests for a credential from issuer

The holder app first interacts with blockchain and pays to select a mediator as discussed in the mediation protocol. Then it contacts the mediator and asks it to mediate with the selected issuer. The mediator then forwards the issuing request by the holder to the selected issuer. The issuer can then respond to the holder's request using the mediator as a middle party.

The actual credential issuance may take multiple messages between the holder and the issuer where they exchange information about what information needs to go into the credential. However, every message between the holder and issuer will go through the mediator and each message will be encrypted with the mediator keys. Therefore, the mediator will have no information about the actual information being passed between the two parties.

Regarding the payment for the issuer, if the issuer is the plurality issuer or third party attestor, then they will be able to collect their payment from the holder smart contract. If it's from another existing network, then that network will be responsible to monetize them.

Proof Exchange Protocol (PEP)

The proof exchange protocol refers to the process where a verifier (either a mobile app or a cloud verifier) asks a prover to provide certain proof.

There are three steps for the proof exchange protocol:

1. Mediator selection for verifier and prover using the mediation protocol
2. Proof Creation by the prover
3. Proof transmission for prover to verifier

As explained in the mediation protocol before, the first step that happens when a verifier needs to ask a prover for a proof is that mediators are selected. The details of this process have already been discussed in the previous sections.

Once the mediators have been selected, the only thing that's left is the request for proof and the creation and transmission of proof.

Let's first talk about how proofs are created.

Proof Creation

Let's assume that a verifier needs to ask the prover about his/her full name. To do this, the prover needs to create a cryptographic proof using the identity card verifiable credential.

The proof block is signed and encrypted with several keys to ensure integrity and privacy. The following are the steps:

1. First, the verifiable credential proof for the prover's DID is created.
2. Then this packet is signed by the blockchain wallet's private key to correlate the DID and the blockchain address.
3. Then it is encrypted by the public key of the verifier.
4. Finally, it is encrypted by the public keys of the verifier and prover mediators respectively.

Please note that the verifier's mediator will only be present in case the verifier is a mobile app.

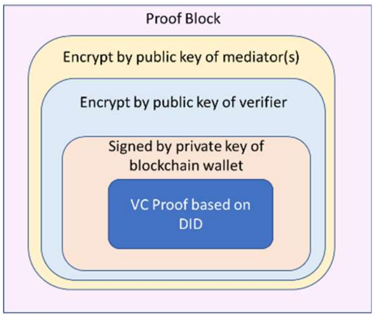
Proof Block
Encrypt by public key of mediator(s)
Encrypt by public key of verifier
Signed by private key of blockchain wallet
VC Proof based on DID

Figure 19 Proof block encrypted by public keys of all parties it needs to go through

Proof Transmission

After the mediator selection and proof creation, the final step in the proof exchange protocol is the transmission of proof.

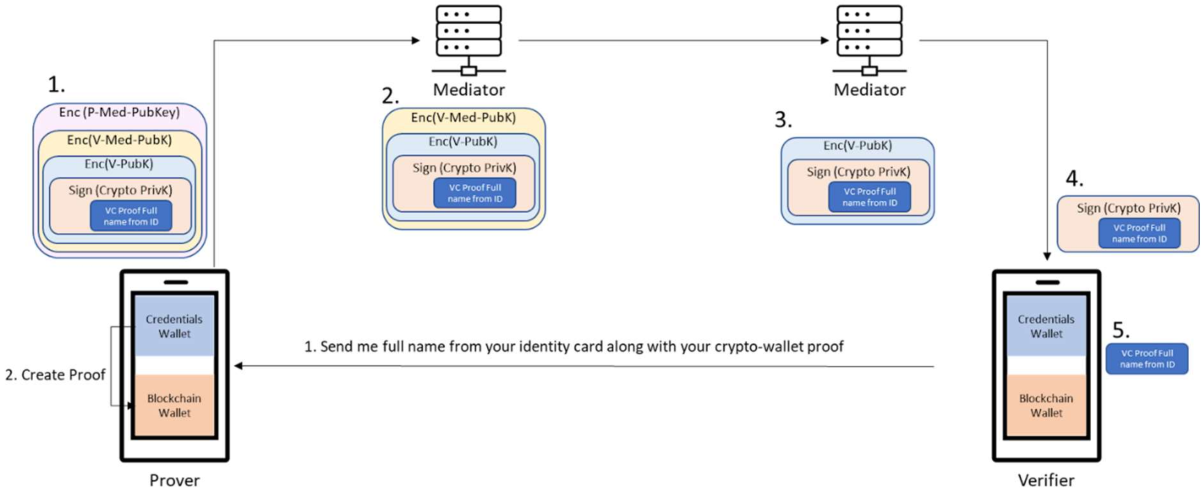

Figure 20 Proof block being decrypted step by step as it travels through mediators to verifier

The image above explains the whole process.

The prover forwards this proof packet to the verifier using the intermediary mediators.

Proof reaches prover's mediator

When the proof packet needs to be sent to the verifier, it first goes to the prover's mediator. The prover mediator decrypts it with its private key and gets the information where it needs to send the packet next. Note that it doesn't get any information of the proof information that is being shared.

Proof reaches verifier's mediator

Then, the packet is sent to the verifier's mediator which decrypts it with its private key and gets the metadata of where it needs to send this proof packet. The verifier's mediator forwards the packet to the verifier. Note that the verifier's mediator has no idea what is being transmitted and the original sender of the proof.

Proof reaches verifier

The verifier first decrypts the proof packet with the public key of the sender's blockchain address. A successful decryption proves the integrity of the proof's sender.

Proof verification by verifier

Finally, the proof is extracted and is verified using self-sovereign identity mechanisms where proof is checked against the issuer's public key and DID to ensure that the proof was generated from a non-revoked credential issued by a valid issuer.

Secure Backups

After a successful verification, the verified addresses are published on the verifier contract on blockchain so that other dApps on the chain can access information about verified addresses.

Moreover, if needed, the verifier can also choose to take an encrypted backup of the proof for logging and reporting purposes. The encrypted decentralized backups make more sense in case of a cloud verifier representing an organization.

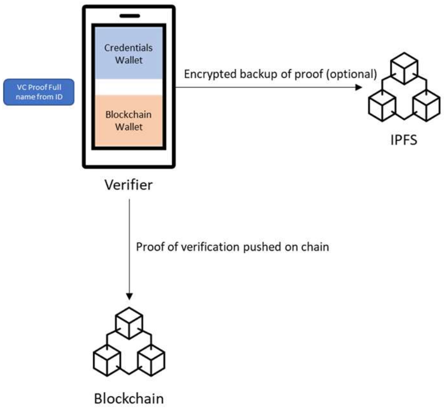
VC Proof Full name from ID
Credentials Wallet
Blockchain Wallet
Verifier
Encrypted backup of proof (optional)
IPFS
Proof of verification pushed on chain
Blockchain

Figure 21 Encrypted backups of proof verifications and storing the verified addresses on blockchain

Tokenomics

Plurality Token

PL is the native token of Plurality. Its main utility lies in being the means of exchange, the network currency, which is being used to maintain the network and incentivize its privacy-preserving stakeholders such as mediators, issuers and coordinators. Furthermore, it represents the collective value of the PL protocol privacy economy. Each PL holder is part of the network and can freely participate in its economy and governance.

Allocation	Quantity (in Mio)	Percentage	Description
Ecosystem	35	35%	Incentivization of ecosystem enablers
Investors	20	20%	In order to build strategic partnerships
Treasury	15	15%	Reservation for future token allocations
Community	10	10%	Incentivization of the community
Team	20	20%	In order to retain a world class team
Total	**100**	**100%**	**To foster a strong adoption for the protocol**

Table 1: PL Token Distribution

PL is a utility token. Furthermore, the distribution of its 100 million PL tokens can be seen in Table 1. In order to foster a strong and sustainable community around the protocol, key network stakeholders are being incentivized to participate.

Drawing on the token distribution, investor and team tokens are being locked and then linearly vested over a set time interval whereas community and infrastructure providers from the beginning. As privacy messaging will increase with network growth, so will token supply. Projected token supply can be seen in Figure 22

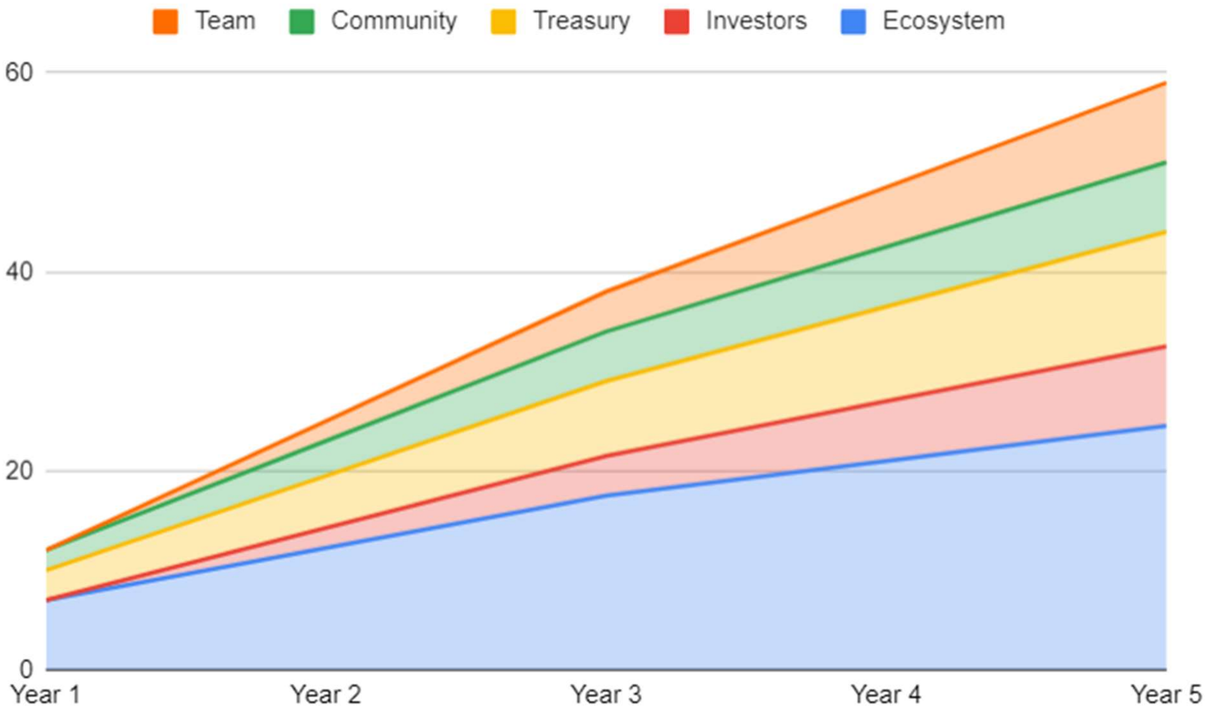

Figure 22 Token supply over time

Incentivization

Every infrastructure provider in the plurality ecosystem i.e. mediators, issuers and coordinator will be incentivized in PL tokens based on the service they provide.

The details of incentivization have been previously discussed in the plurality ecosystem section.

Slashing

Unlike Proof of Work (PoW) where off-chain capital expenses are already deployed at the time of block construction/voting, Proof of Mediation (PoM) systems require capital-at-risk to guarantee active mediation of data packages. We **intend** to implement slashing rules which, if broken, result in some amount of the offending mediator's deposited stake to be removed from circulation.

Conclusion

Decentralization is a major step in the vision for a better world. Blockchains are bringing us one step closer to that vision. However, a key piece of this puzzle i.e. identification of people still remains highly centralized and restrictive. This not only goes against the principles of web3, but also poses serious privacy concerns for the parties involved. Moreover, it limits the innovative use cases that can be created in this ecosystem.

A better way to handle identification is self sovereign identity (SSI), which lets users be in control of their data. SSI users can decide when, how much and to whom the data needs to be revealed.

Plurality brings self sovereign identity into the blockchain space and attempts to create an identification system that protects the inviolable dignity of humankind by ensuring privacy and decentralization. By design, it supports all programmable blockchains and can support multiple types of identification credentials.

Plurality brings the complexity of human relationships on the blockchain, giving rise to a new era of decentralized society.

References

[1] FATF: https://www.fatf-gafi.org/about/

[2] GDPR: https://gdpr-info.eu/

[3] Filipcic, S. (2022). Web3 &amp; DAOs: an overview of the development and possibilities for the implementation in research and education. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1278–1283. https://doi.org/10.23919/MIPRO55190.2022.9803324

[4] Momtaz, P. P. (2022). *Some Very Simple Economics of Web3 and the Metaverse*. https://www.metagreats.com/article/how-much-land-available-in-decentraland/

[5] Korpal, G., & Scott, D. (n.d.). *Decentralization and web3 technologies*. https://2018.web3summit.com/speakers/

[6] Kshetri, N. (2022). Policy, Ethical, Social, and Environmental Considerations of Web3 and the Metaverse. *IT Professional*, *24*(3), 4–8. https://doi.org/10.1109/MITP.2022.3178509

[7] Garon, J. M., & Garon Page, J. M. (n.d.). *Legal Implications of a Ubiquitous Metaverse and a Web3 Future LEGAL IMPLICATIONS OF A UBIQUITOUS METAVERSE*.

[8] Wang, Q., Li, R., Wang, Q., Chen, S., Ryan, M., & Hardjono, T. (2022). *Exploring Web3 From the View of Blockchain*. http://arxiv.org/abs/2206.08821

[9] Almeida, F., D. Santos, J., & A. Monteiro, J. (2013). E-Commerce Business Models in the Context of Web 3.0 Paradigm. *International Journal of Advanced Information Technology*, *3*(6), 1–12. https://doi.org/10.5121/ijait.2013.3601

[10] Bambacht, J., & Pouwelse, J. (2022). *Web3: A Decentralized Societal Infrastructure for Identity, Trust, Money, and Data*. http://arxiv.org/abs/2203.00398

[11] *Digital Assets, Distributed Ledger Technology and the Future of Capital Markets* (2022)- Insight Report https://www3.weforum.org/docs/WEF_Digital_Assets_Distributed_Ledger_Technology_2021.pdf

[12] *McKinsey's Global Banking Annual Review* [2021] https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review

[13] Celsius Exposes User Information in Public Court Docs https://blockworks.co/celsius-exposes-user-information-in-public-court-docs/

[14] Verifiable Credentials Ecosystem https://www.w3.org/TR/vc-data-model/

[15] DIDComm https://identity.foundation/didcomm-messaging/spec/