Plurality

Bringing identity on blockchain while ensuring data privacy

Hira Siddiqui

Mujtaba Idrees

Tobias Jung

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

Currently, the most innovative decentralized applications (dApps) are built on top of programmable blockchains like Ethereum. Most of these use cases require that the participating users identify themselves due to compliance reasons. Some of these dApps are 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, making it clear which address is interacting with whom.

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 as blockchains by design are transparent and immutable.

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.

Figure 1 Data Privacy Paradox

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.

Therefore, currently in the web3 space, centralized identity mechanisms are being used. But this 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, similar to how it was being handled in the physical world. 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 identity information. Identity documents, known as 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. Users use these VCs to prove their identity to other parties in a privacy preserving manner.

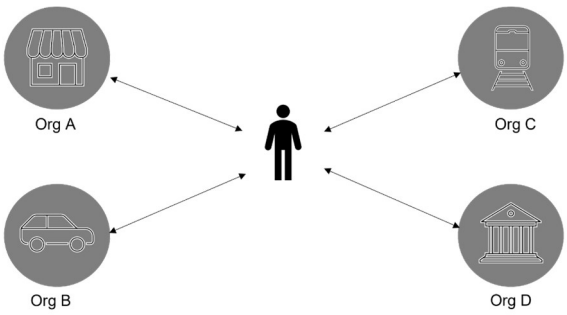

Figure 2 User in control of identity

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.

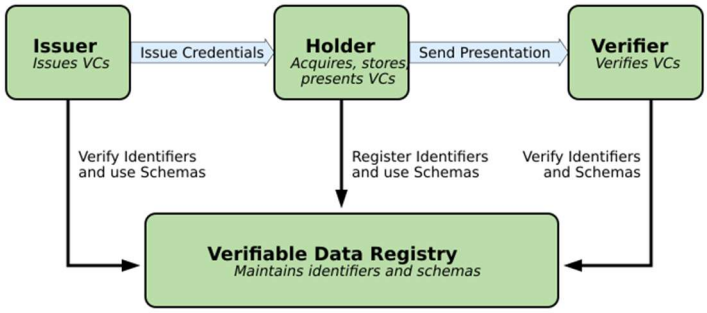

Figure 3 SSI Ecosystem - Roles [14]

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 4 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.

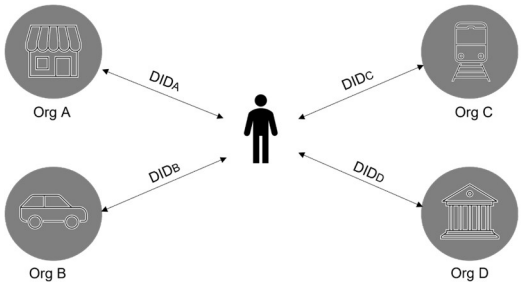

Figure 5 Correlation resistance in different interactions of a user

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.

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

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. but are outside the scope of lightpaper.

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 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.

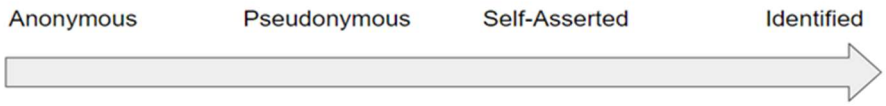

Figure 6: Spectrum of identity

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.

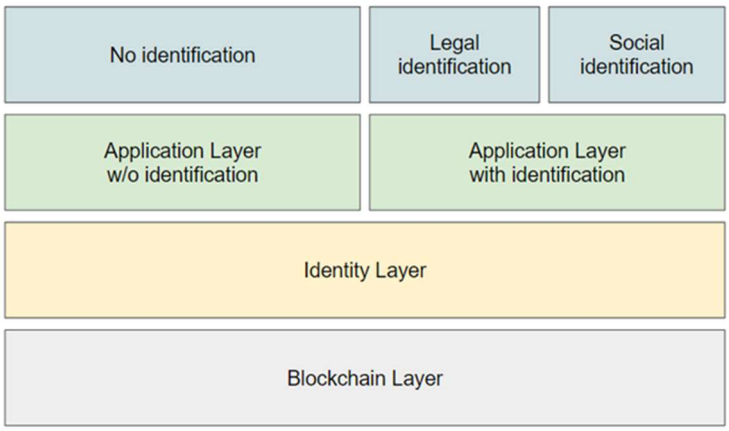

Figure 7: Layers of decentralized applications

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.

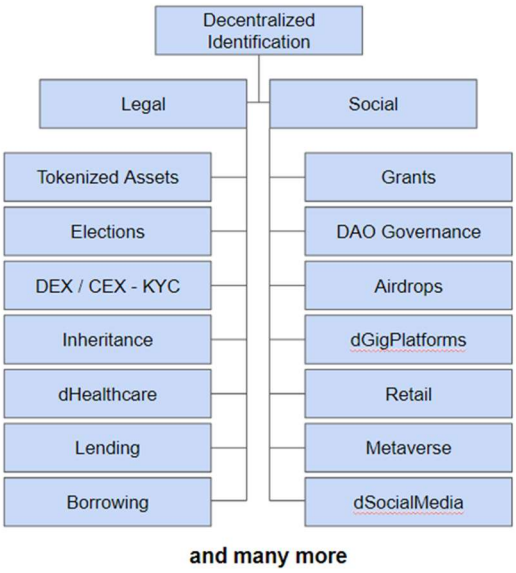

Figure 8: Identification categories

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.

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.

	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

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.

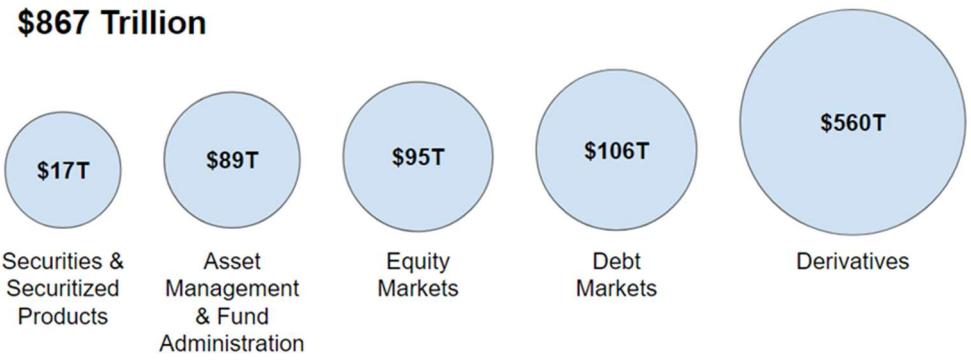

Figure 9: Value disrupted by web3

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.

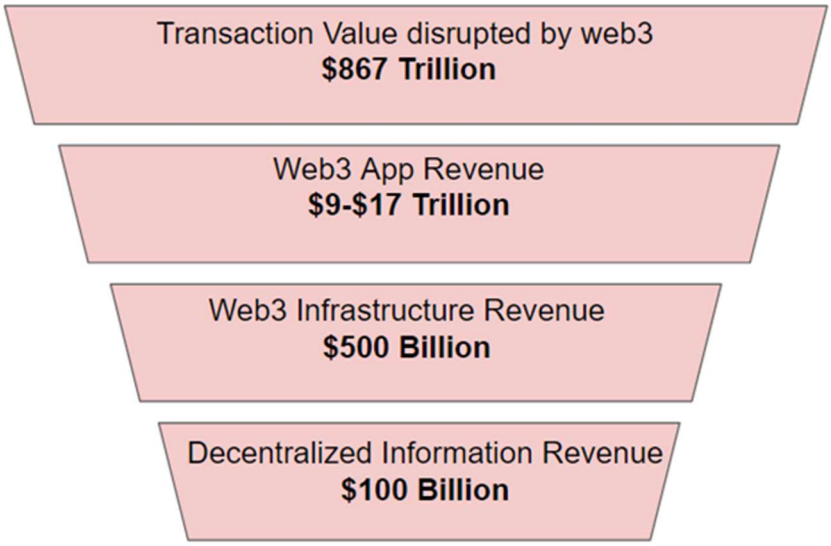

Figure 10: Breakdown of transaction value disrupted by web3

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.

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 & 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/