THE GRAIL – LITE PAPER

V 0.1

Table of Contents

Introduction

The advent of blockchain technology has brought about a revolution in the way we store and transfer value. By creating a decentralized, transparent, and secure network, blockchain has enabled people to transact with one another without the need for intermediaries. With its ability to provide a tamper-proof and auditable record of transactions, blockchain has the potential to increase trust and transparency in various domains and could play a crucial role in shaping the future of our digital world.

While blockchain has the fullest potential to create a more decentralized and transparent ecosystem, where trust is built through cryptographic verification rather than centralized authority, It makes it difficult to track and attach different transactions and activities to individuals in the real world. At its core, the transactions in the blockchain are pseudonymous in nature, where in every transaction is attached to a public address, however the real life identity of the owner of that address and the transaction is unknown. While this at the face of it seems to give tremendous privacy benefits, the lack of accountability associated with such pseudonymous blockchain transactions has led to some individuals using blockchain for illegal activities such as fraud, scams, and cyberattacks. This has caused some individuals and organizations to view blockchain technology as a threat rather than an opportunity. The anonymous nature of blockchain has made it difficult for businesses and individuals to establish trust with other users

The above set of issues have raised several problems related to security and fairness. Sybil attacks, where a single user creates multiple fake identities, can be used to manipulate the network and gain control over the system. Wash trading, where a user artificially inflates trading volume to create a false impression of liquidity, can lead to market manipulation and unfair trading practices. Money laundering, where blockchain transactions are used to hide the origin or destination of funds, can facilitate criminal activities. Market making, where traders artificially create demand for a particular asset to profit from the price difference, can lead to unfair practices. Finally, the lack of transparency and accountability in blockchain transactions can create an uneven playing field, leading to market inefficiencies and distrust among users.

The rest of this paper will discuss the below

- Regulatory commentary and conclusions
- Privacy, the need and challenges
- Zero Knowledge Cryptography
- Grail's approach to tackling these challenges

Regulatory commentary

While there are not many clear regulations around blockchain and web3 in specific, we attempt to paint a broad picture on perspectives from various regulatory agencies and bodies in the western world, with a particular focus on the United States and European Union. We aim to expand the scope of this document with perspectives from regulators in other parts of the world in the upcoming versions of this document

Securities and Exchanges Commission (SEC)

Commissioner Caroline Crenshaw in this article talks about the issues around “Lack of transparency” and “Pseudonymity” in the blockchain. She states that the Inability to know the identity of traders or owners of smart contracts presents fundamental hurdles. She says “Without an efficient method for determining the actual identity of traders, or owners of smart contracts, it is very difficult to know if asset prices and trading volumes reflect organic interest or are the product of manipulative trading by, for example, one person using bots to operate multiple wallets, or a group of people trading collusively”

Financial Action Task Force (FATF)

The Financial Action Task Force, in their latest set of recommendations state clear definitions for Virtual Asset Service Providers (VASP). Further, FATF strongly recommends that the “Travel Rule” be implemented for any and all peer to peer transactions on the blockchain, including cross border transactions. This recommendation squarely expects all VASP’s including CeFI, DeFi exchanges, NFT exchanges and more to identify the identity of all the users on their platform

European Central Bank (ECB)

In this article written for the European Central Bank, the authors argue that regulatory frameworks need to be brought for Decentralized Platforms, and it is important to “identify” all actors involved in this ecosystem, so that appropriate regulations can be enforced

Summary

Apart from the commentary, we are seeing an increase in enforcement actions against all kinds of blockchain companies, majorly focussing around lack of KYC/AML checks of users and their transactions. Such enforcement actions have been applied to both centralized and decentralized platforms in the blockchain, leading many to question if code and smart contracts can even be “regulated”. Notwithstanding all the criticism, we continue to see increased regulatory scrutiny, sometimes with years of investigative effort put in

Based on the overall commentary and actions being taken by regulatory authorities, our strong conclusion is that, the responsibility for doing KYC and AML checks on users and their transactions will continue to rest on the platforms, developers and governance owners of these platforms / smart contracts

Privacy, need and challenges

Background

In the backdrop of the current regulatory environment and the push for strong customer identification (KYC/AML/CFT), it is important to understand the background behind the pseudonymous nature of public blockchain and what could be the strong drivers of privacy. As we are aware, the bitcoin paper and the advent of blockchain happened with the 2008 financial crisis in its backdrop. The original thesis, motivations and early adoption of the Bitcoin and the Blockchain ws based on the premise that, the functionality of value store and value transfer can happen without the need for intermediaries, that can potentially avoid centralized control leading to misuse and meltdown of financial institutions. A platform or a system that can operate without an intermediary is purported to be “trustless”, since one does not have to trust an individual or an institution to store and transfer value in such a platform. A 100% peer to peer trustless platform, did not need and have any authority to verify and validate user identities. This resulted in largely pseudonymity being part of the core platform. User’s used long string addresses to identify their accounts on the Blockchain, and used such addresses to identify the individual to whom value needs to be transferred

The majority of early user’s of public blockchain cherished and celebrated privacy. Or rather we can say, blockchain attracted the attention of privacy conscious individuals, who found value in being able to transfer value without having to go through hoops, or share personally identifiable information at every step. However, recently, we have seen the advent of many protocols that aim to attach short names and domain names to user addresses, thus publicly attaching a real user identity to an address. It is arguable that this is by choice and privacy is still an option for people who want to use such public blockchains.

Also on the other side, as identified in this paper earlier, the pseudonymous nature has been mis-used by illicit actors to launder and transfer stolen cash and fund more illicit activities. This has pushed governments and law enforcement agencies to push for enforcement and legislations to mandate customer identification in blockchain applications

Need for privacy

While it is debatable if users of applications running on top of public blockchain need pseudonymity, and as few have argued “What do they have to hide”, we think the real need for privacy rests elsewhere, in need for ease of access and a trustless application layer to achieve true decentralization

- ### Moving beyond pseudonymity

While the initially set of decentralized applications aimed to and to some extent provided value for users with full pseudonymity, we feel there are below growing reasons as to why a decentralized application might want to know more about its users and attach real identity behind a wallet address

- **Experience & Use cases** - Decentralized applications can power new use cases and deliver enhanced user experience if they are able to understand more about the user. This could include both data from user’s on-chain activities (from multiple addresses) and / or user’s off-chain data. For eg undercollateralized loans is a big use case if a lending app is able to understand the user's credit score based on their off-chain activities.
- **Regulation** - As identified, governments of the world are increasingly becoming clear that, smart contract based decentralized applications act as intermediaries and hence will have the same obligations as a financial institution under the Bank Secrecy Act, which means such applications need to employ Know your customer techniques to identity and verify user’s real identity based on government issued identification
- **Security** - Attaching real world identity to wallet address, allows users to operate in a safe and secure environment, especially when it comes to financial value transfer, advice and more. This is even more true as more useful application delivering real value are built on the blockchain. Applications can provide a safe experience and ensure their systems are sybil attack resistant and cannot be gamified

- **Need for trustless and seamless intermediaries**

Open source code base and trustless nature of code execution on the blockchain has reduced the need and levels of trust required. It is arguable that this reduced level of need for trust is actually the reason behind widespread adoption of decentralized applications. However, as the need for user identification in decentralized applications (also called as intermediaries) arises it results in 2 major problems

- In a conventional user identification process, users are forced to trust the application and its developers / governance to secure their personally identifiable information. This essentially creates a new trust layer, which feels more like a bug than a feature in blockchain
- Also the typical user identification process is cumbersome and without a seamless experience, users are not incentivized to explore and use a host of applications

As users are forced to review and trust the people behind such applications (which are subjective, unlike trusting code), users will be forced to abandon using a large majority of the applications and veer towards applications that are backed by well known individuals. Also, users don't want to go through the usual and lengthy identification process and would rather transact via only a handful of applications for ease of use(like how they bank today). Both will result in large sized monopolies and stifle innovation, much like what we witness today in the area of internet and mobile applications (a.k.a web2). Alas, it seems like we will be back to square 1.

The challenge of delivering privacy in web3

As it might probably be clear by now, the conundrum of user identity in web3 needs to satisfy the below

- Seamless and easy user identification process, preferably one click
- Private user identification, on a strictly need-to-know basis only with limited information sharing
- Decentralized and trustless, in a way that the user is aware information is not being shared without their knowledge

Muck like the Blockchain trifecta, the Identity trifecta presents unique technical challenges

Zero Knowledge Cryptography

Zero Knowledge Cryptography is a set of primitives that allow a prover to verify a set of statements without revealing the details based on which those statements are constructed. This is being widely used to build scalable Layer 1 solutions, including several ZK based EVM's. We strongly believe that Zero Knowledge Proofs (ZKP) provides a promising approach for privacy in identities and helps accomplish the trifecta mentioned above

ZKPs can enable individuals to prove their identity without revealing any personal information. This approach can be used to build privacy-preserving applications that comply with regulatory requirements while ensuring the privacy of users and delivering a seamless experience. By leveraging the immutable and decentralized nature of the blockchain, businesses and applications can conduct user identification processes in a secure and privacy preserving manner.

ZKP based Identity X Know Your Customer (KYC)

Privacy: ZK-based KYC provides a way for users to prove their identity without revealing their personal information, which can help protect their privacy

Compliance: AML regulations require financial institutions and service providers to identify and verify the identities of their customers. ZK-based KYC can help these institutions comply with these regulations while also protecting the privacy of their customers

Security: ZK-based KYC can be more secure than traditional KYC methods that require users to share sensitive personal information. ZK proofs provide a way for users to prove their identity without exposing their personal data to potential hackers or other malicious actors.

Conventional KYC	ZK KYC
Repetitive process	Reusable
Security risk	Secure
Platform dependant for Trust (Intrusive)	Privacy preserved
Single point of failure system	Failure proof
Non Composable	Composable
Poor experience	Enhanced one click experience

Overall, ZK-based KYC has the potential to be a useful tool for AML crypto regulations, as it provides a way for service providers to comply with regulations while also protecting the privacy and security of their customers.

Grail - Introduction, Experience and Use cases

Introduction

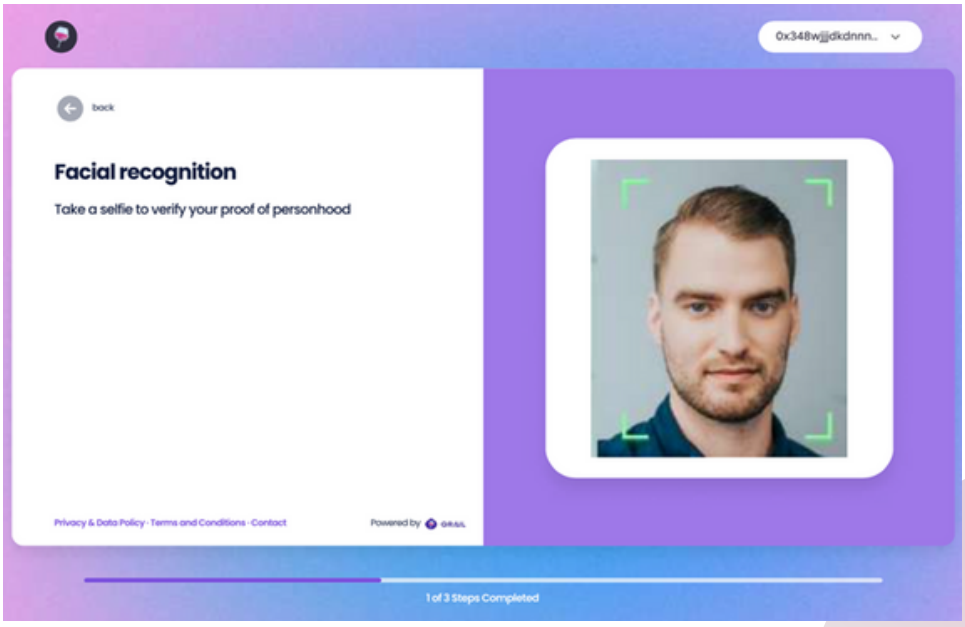
Grail is a ZK-powered reusable KYC platform that aims to solve the regulatory compliance and privacy issues faced by the blockchain industry. By utilizing Zero-Knowledge Proofs (ZKPs) and the latest cryptography techniques, Grail enables individuals to verify their identity and gain access to decentralized applications (dApps) without compromising their personal information. Grail aims to deliver a seamless experience with utmost privacy for its users.

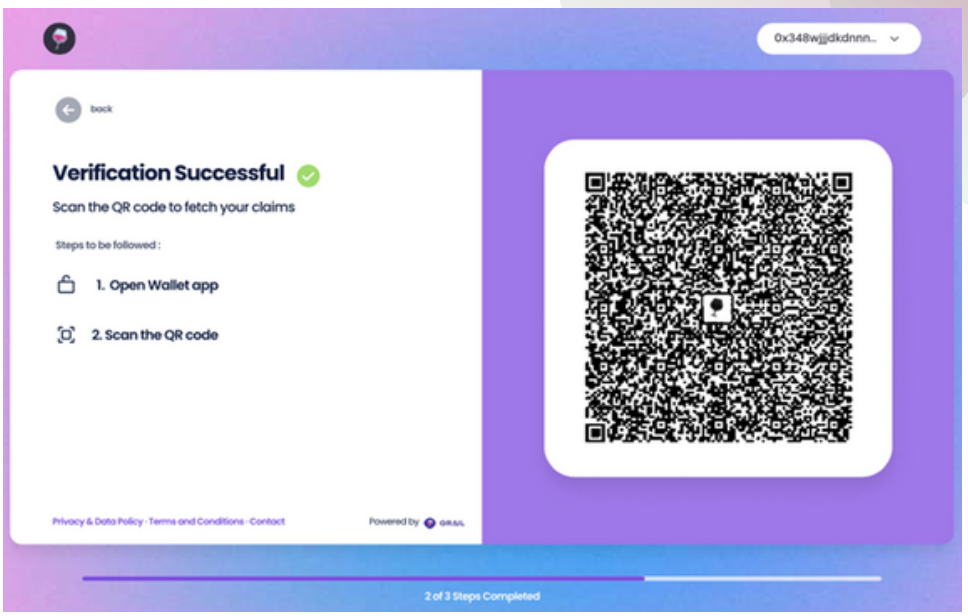
Experience

The Grail experience for users consist of 3 steps:

Step 01 - Credential issuance (5 mins - one time)

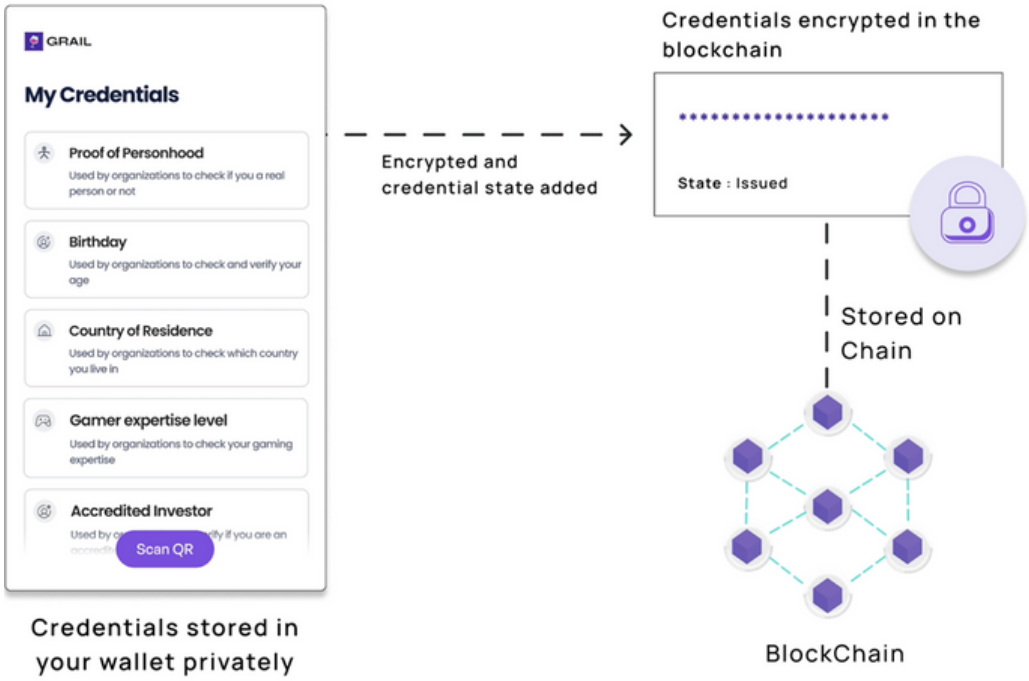
The user has to do a one time set up of their credentials from the Grail platform. User identify and verify themselves in this one-time process to get their credentials issued





Step 02 - Credential store (1 min - one time)

Users are able to have their credentials stored privately in their self-custodial wallet. This is a one-time process and takes less than a minute. Along with credential storage in their wallet, an encrypted version of the credential and the state of the credential is stored in the blockchain, along with the issuer information



Step 03 - Verification (5 seconds)

This is a key part of the Grail experience, where it takes less than 5 seconds for a user to verify their credentials in a private manner with decentralized applications. This happens in below steps

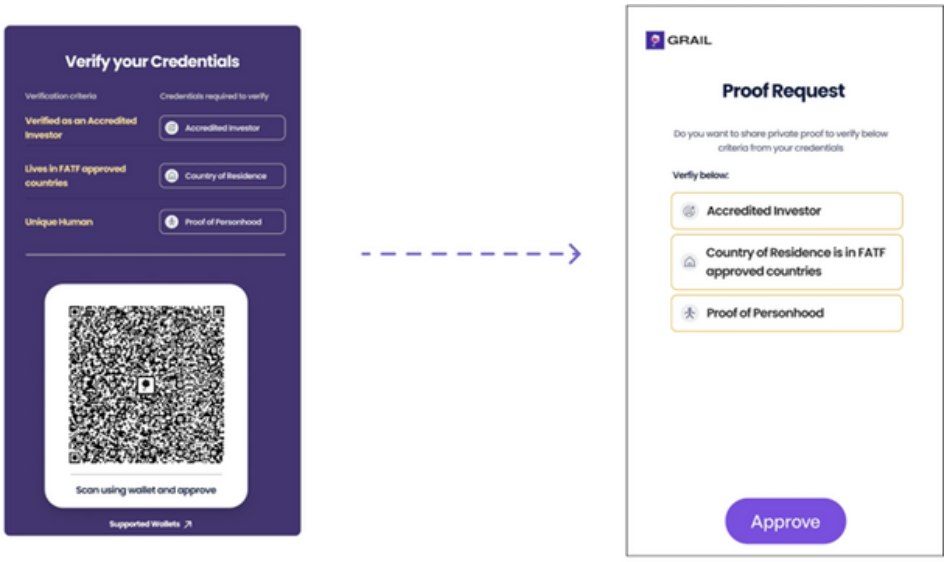
- Users are presented with a QR code to scan and verify themselves.
- Upon scan, a supported wallet opens and requests user permission to share private proof to verify certain aspects of their credentials. It is important to note that rather than sharing the actual credential information, the user is able to prove certain statements in their credentials (as shown in the examples below). This preserves user privacy
- Post approval, the user is able to go back to the application and continue their verified experience

Use case examples

With the help of Grail, decentralized applications can power innovative use cases and safe experiences across a multitude of ecosystems including Decentralized Finance (DeFi), Games, Decentralized Autonomous Organizations (DAO) and more. Below are examples of how such user verification can work for some use cases.

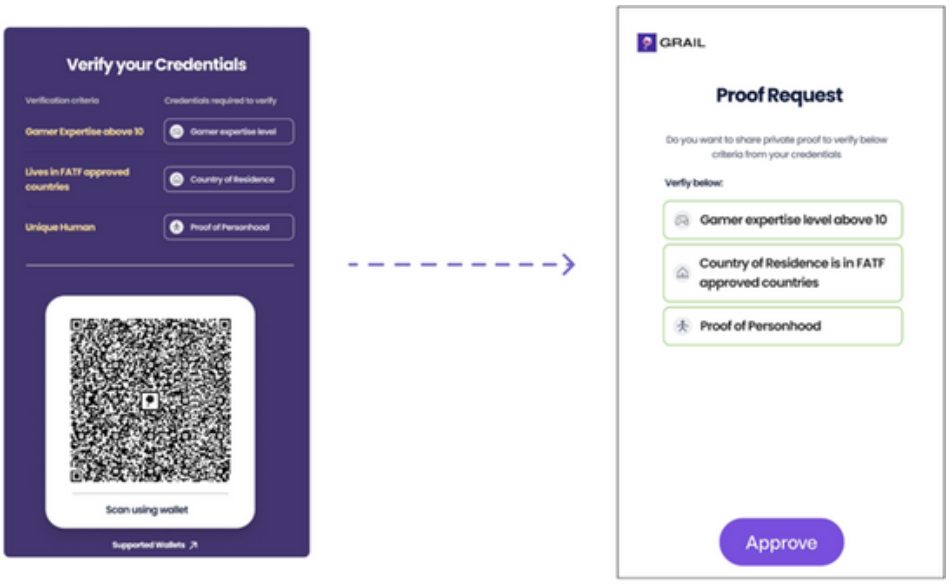
Airdrop eligibility check

Approve to receive airdrop



Verified Investor Check

Approve to get verified



Gamer expertise and verification check

Approve to get verified

Below are some resources that can help the reader understand more about Grail and our solution

- A high level introduction to Grail can be found in this video
- A high level solution document for Sybil resistant Airdrop can be found here
- A high level solution document for better game design can be found here

Team

Prasanna Venkatesan, Founder

Prasanna comes with a strong identity background. Previously he founded Insent.ai that was a leading AI Automation software for Marketing and Sales professionals. Insent.ai was acquired by publicly listed ZoomInfo (Nasdaq:ZI) in June 2021, where he served as Vice President. ZoomInfo is the leading provider of business contact information with sophisticated identity extraction techniques. Prasanna comes with very strong understanding and experience of business identity and how identity plays an extremely key role in several key business and customer facing functions

The Grail team further consists of several professionals with relevant background including Web3 marketing, public policy and practicing lawyers.