Lite paper: XRPL Solvency

Privacy is at the core of the blockchain ecosystem and at the center of the original ideals of the Cypherpunks. However, today with the growing number of blockchain applications in our ecosystem with use cases increasingly connected to the rest of the world (apartment rental, tokenization of real-world assets, DID…), it is becoming increasingly difficult to detach one's on-chain identity from one's own identity.

1. Executive Summary

XRPL Solvency is a solution that addresses the growing need for privacy in the blockchain ecosystem by providing a means for individuals and businesses to prove solvency without revealing their wallet address or transaction history. This is achieved through the use of cryptographic ring signature technology and other cryptographic means to generate verifiable, solvency proofs at a specific point in time. The solution is designed for individuals who value their privacy while transacting on blockchain platforms, and it offers a unique value proposition by allowing users to prove solvency without compromising their privacy. Businesses can also benefit from the solution through use-cases we will detail bellow.

2. The problem

The XRP Ledger is a decentralized, open source blockchain technology that enables fast and secure transactions of digital currencies. While XRP Ledger is serving as a global settlement platform for various types of transactions, generating solvency proofs can be a solution for many problems that actors in the ecosystem will be facing. This interest in solvency proofs creates an opportunity for solutions like the XRPL Solvency project to offer a new, innovative approach to generating proof of solvency that provides greater privacy and security for users, enabling new interactions possibilities.

By leveraging cryptographic ring signatures and other cryptographic means, XRPL Solvency can generate verifiable solvency proofs that do not reveal the user's on-chain assets and history associated with their own identity, filling a need that is currently unmet by XRP Ledger-based solutions. XRPL Solvency could be used to offer a new level of trust and transparency to the XRP ecosystem, while ensuring the privacy and security of users' on-chain assets.

Theoretically, zero-knowledge proofs and more particularly ZK-SNARK are a very good solution to our problem.

Nevertheless, in practice, many problems arise. Due to their complexity, potential compatibility issues with existing cryptographic primitives, and the need for a trusted setup in some cases, ZK-SNARK are not very user friendly and require for the moment on SECP256k1 very heavy proof files to verify ECDSA (>1Gb).

SECP256k1 is a widely used elliptic curve cryptography algorithm that is used in many blockchain applications, including Bitcoin, Ethereum and is one of the curves used in XRP Ledger. While SECP256K1 provides a secure means of generating cryptographic signatures and keys, it is not ideally suited for use in zero-knowledge proofs (ZKPs) such as ZK-SNARKs. ZK-SNARKs require pairing-friendly elliptic curve cryptography, which is not a property of SECP256K1. This means that implementing ZK-SNARKs with SECP256K1 is not straightforward and requires additional workarounds that can significantly reduce the efficiency and security of the system.

As XRPL Solvency is designed to provide a highly secure and efficient means of generating verifiable solvency proofs, we carefully consider the cryptography algorithms used in the solution. While SECP256K1 is a widely used and secure algorithm, it is not ideally suited for ZK-SNARKs, and other cryptography algorithms may need to be considered to ensure the best possible security and efficiency for the solution. Moreover, using ZK involves a lack of scalability, portability, and compatibility with other chains. Which is inconvenient for further expansion.

This is why we turned to ring signatures. Being simpler, based on elliptic curves and not requiring a trusted set-up, ring signatures are more suitable for our project. Moreover, ring signature does not require any change at the protocol level. Making it a scalable and customizable solution.

3. The solution

Our solution stands in 2 words: Ring Signatures. Ring signatures are a type of digital signature that allows a member of a group to sign a message on behalf of the group without revealing which member signed the message. In other words, a ring signature makes it impossible to determine who exactly in the group signed the message, while still proving that someone in the group did sign it.

The name “ring signature” comes from the way the signature is created. It involves a “ring” of public keys belonging to group members, and the signature is formed by combining the signer’s private key with the public keys of other members in the ring. The result is a signature that can be verified by anyone using the group’s public keys but cannot be traced back to the individual who signed it.

Ring signatures have a variety of applications, including enhancing privacy in blockchain transactions. They are often used in privacy-focused cryptocurrencies like Monero for example, to preserve the sender’s identity. This technology can then be expanded to many other fields and has a wide spectrum of application that we will explain bellow in the document

Ring signatures are XRPL and EVM (Ethereum Virtual Machine) friendly because they are based on elliptic curve cryptography. In addition, ring signatures do not require any heavy computation.

Moreover, ring signatures are a proven and well-established cryptographic technique that has been widely used in the cryptocurrency industry, particularly for privacy-focused applications. The underlying math is well-understood, and implementations of ring signatures have been tested and reviewed by the cryptography community, providing a high level of confidence in their security.

Ring signatures are also highly efficient, allowing for fast and scalable computation of cryptographic signatures, which is important in the context of blockchain applications where

speed and scalability are critical. As a result, ring signatures are a good choice for applications that require fast and secure cryptographic operations, such as XRPL Solvency proof generation.

Overall, the use of ring signatures in XRPL Solvency makes it an efficient and secure solution for generating verifiable solvency proofs on the XRPL lockchain.

Ring signatures are considered scalable because they can be verified quickly and efficiently, even when the size of the signing group is very large. This is because the verification process only involves checking a single signature, rather than verifying multiple signatures from each member of the group.

When a signature is generated using a ring signature scheme, it includes information about the entire group of public keys, but does not reveal which specific key was used to create the signature. This means that anyone can verify the signature by checking that it was produced using one of the public keys in the group, without having to perform additional computations to verify each individual key in the group.

This makes ring signatures particularly useful in applications that require fast and efficient signature verification, such as in the context of blockchain transactions, where multiple signatures may need to be verified in a short period of time. Additionally, the fact that ring signatures are scalable makes them well-suited to use in decentralized systems, where many participants may need to sign and verify messages on a regular basis.

Proof of reserve Current PoRs are carried out by independent entities. With our solution anyone can generate a PoR via an open source and verifiable mechanism based on cryptographic concepts. This concept will be more developed in the future for institutions.

4. How it works

Step 1: Generating the solvency proof

Alice wants to generate a solvency proof for Bob:

1. Alice visits our website
2. She follows the easy steps
3. She uses our Solvency proof generation program by downloading it
4. If her proof is valid, Alice will receive a SoulBound Token (NFT) on her communication address as a proof of her solvability
5. The SoulBoundToken can now be shown to anyone

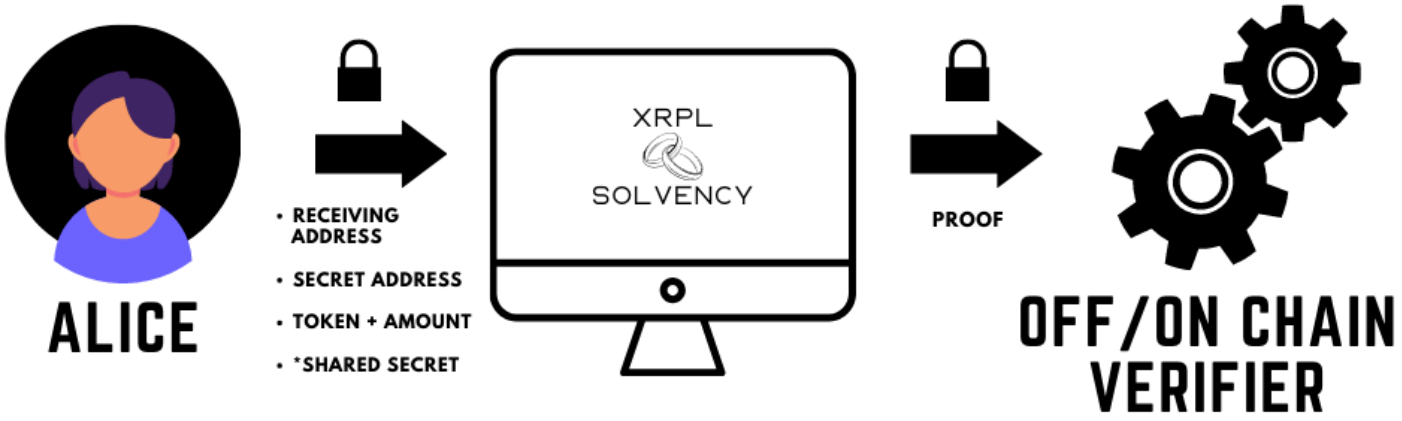
Step 2: Agreement

Bob wants to verify Alice's proof:

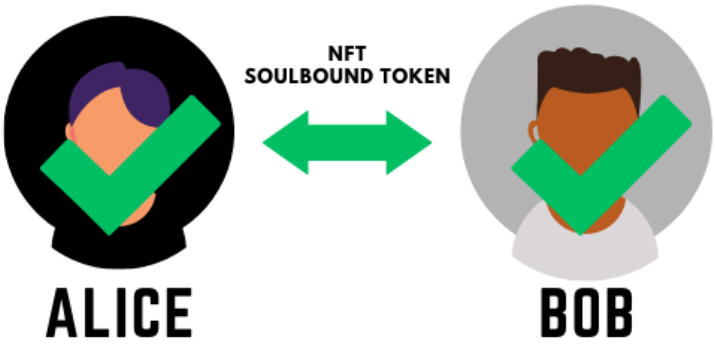
1. Bob goes to XRPL Solvency's Dapp, in the check proof section
2. He fills in Alice's communication address as well as the ID of the SoulBound token given by Alice
3. If a corresponding SoulBound token owned by Alice exists, it will be displayed with all the relevant information
4. Bob verifies all the information that he needs to know

Step 3: Transferring the funds Once an agreement has been reached between Alice and Bob, Alice can send the various funds directly to Bob. But to increase his privacy, he will have to use a different wallet than the one linked to the generation of the proof of solvency.

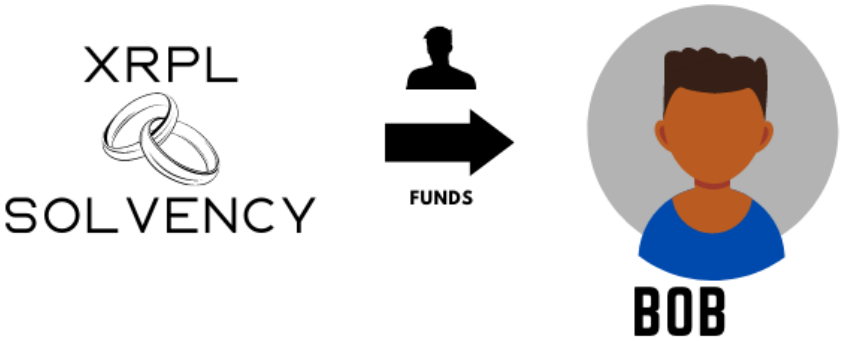
Step 1:



Step 2:



Step 3:



5. Use Cases

Solvency proofs open possibilities for many things, particularly those involving financial transactions on the blockchain. Here are some examples of use cases for solvency proofs:

Renting: As described in the original MVP, solvency proofs can be used in the context of renting apartments or other properties. Landlords can require proof of solvency from tenants to ensure that they have the financial means to pay rent for a certain period of time. Solvency proofs can be generated without revealing the tenant's wallet address or transaction history, protecting their privacy.

Loans: Solvency proofs can also be used in the context of loans, where lenders may require proof of the borrower's solvency before extending credit. By providing a solvency proof, borrowers can demonstrate their financial status without revealing their wallet address or transaction history to the lender.

Investments: Solvency proofs can be used in the context of investments, where investors may require proof of a company's or individual's solvency before investing in them. By providing a solvency proof, the company or individual can demonstrate their financial status without revealing their wallet address or transaction history to the investor.

Insurance: Solvency proofs can also be used in the context of insurance, where insurers may require proof of the policyholder's solvency before issuing a policy. By providing a solvency proof, the policyholder can demonstrate their financial status without revealing their wallet address or transaction history to the insurer.

Procurement: Solvency proofs can be used in the context of procurement, where government agencies or private companies may require proof of solvency from contractors before awarding contracts. By providing a solvency proof, contractors can demonstrate their financial status without revealing their wallet address or transaction history to the agency or company.

Real estate transactions: Solvency proofs can be used in the context of real estate transactions, where buyers or sellers may require proof of solvency before entering into a contract. By providing a solvency proof, the buyer or seller can demonstrate their financial status without revealing their wallet address or transaction history.

Gaming: Solvency proofs can be used in the context of gaming and online gambling, where players may need to demonstrate their solvency in order to participate in certain games or tournaments. By providing a solvency proof, players can demonstrate that they have sufficient funds to participate without revealing their wallet address or transaction history.

Charitable donations: Solvency proofs can be used in the context of charitable donations, where donors may want to ensure that their contributions are going to a financially stable organization. By providing a solvency proof, the organization can demonstrate its financial status without revealing its wallet address or transaction history.

Crowdfunding: Solvency proofs can be used in the context of crowdfunding campaigns, where organizers may need to demonstrate their solvency to potential backers. By providing a solvency proof, the organizer can demonstrate that they have the financial means to carry out the project without revealing their wallet address or transaction history.

Supply chain financing: Solvency proofs can be used in the context of supply chain financing, where suppliers may need to demonstrate their solvency in order to secure financing. By providing a solvency proof, the supplier can demonstrate its financial status without revealing its wallet address or transaction history to the financing party.

These are just a few examples of the many potential use cases for solvency proofs. Any situation where a party needs to demonstrate their financial status without revealing their wallet address or transaction history on the blockchain could benefit from the use of solvency proofs.

6. Compliance

Compliance with institutional requirements is of paramount importance to XRPL Solvency. We offer a service that remains 100% compatible with the laws put in place by the different states since our modules do not allow money laundering in any way. In case of off-chain computation, it could even be possible to keep track of the original proof transmitter in case of legal control.

7. Market Analysis

Potential customers:

The potential customers for XRPL Solvency solution could include:

Individuals: Individuals who are concerned about privacy on the blockchain could be potential customers for XRPL Solvency's solution. These individuals could be cryptocurrency users who want to protect their transaction data from being traced or linked to their real-world identity.

Businesses: Businesses that use blockchain technology for various purposes, such as supply chain management, payment processing, and data storage, could also be potential customers for XRPL Solvency's solution. These businesses may want to protect their transaction history and main wallet info from competitors, hackers, or other third parties.

Financial Institutions: Financial institutions that deal with cryptocurrency transactions, such as exchanges and wallets, could also be potential customers for XRPL Solvency's solution. These institutions may want to enhance the privacy and security of their customers' transactions to protect them from fraudulent activities. During a financial check, for example, the platform will be able to prove that such a user does indeed hold a certain number of tokens without having to leak his address.

Non-profit Organizations: Non-profit organizations that rely on donations or fundraising through cryptocurrency transactions could also be potential customers for XRPL Solvency solution. These organizations may want to protect their donors' transaction data and maintain their privacy and pseudonym on the blockchain.

Competitors:

While XRPL Solvency is a unique solution that offers a specific set of features and benefits, there are a few potential competitors that offer similar solutions for privacy-enhanced transactions on the blockchain:

Mixers: Mixers are a popular solution for enhancing privacy on the blockchain by obfuscating the transaction history. There are several mixers available in the market, such as Wasabi Wallet or CoinJoin applications.

Private Chains: Private blockchain networks offer enhanced privacy by restricting access to the network and the transaction data. Solutions like Corda and Hyperledger Fabric are examples of private blockchain networks that offer enhanced privacy and confidentiality.

Mimblewimble-based Blockchains: Mimblewimble is a protocol that offers enhanced privacy by obfuscating transaction data. Blockchains like Grin and Beam are examples of Mimblewimble-based blockchains that offer enhanced privacy for transactions.

TumbleBit: TumbleBit is a solution that offers privacy-enhanced transactions by using a combination of cryptographic techniques like coin shuffling, encryption, and hashing. It is currently available as an extension for the Bitcoin Core wallet.

Privacy based blockchains: Zero-knowledge proof blockchains like Zcash, Monero, Horizen, and others use cryptographic techniques to ensure the privacy and confidentiality of transactions on the network. These blockchains offer enhanced privacy for transactions, similar to XRPL Solvency.

Market trends:

As privacy become increasingly important in the blockchain ecosystem, there is a growing demand for solutions like XRPL Solvency that offer enhanced privacy for user interactions. The market trend for privacy-enhanced blockchain solutions has been on the rise in recent years, with a particular focus on the Ethereum ecosystem. Many new privacy-focused projects have emerged, offering unique features and benefits to users.

The trend towards privacy on the blockchain is being driven by several factors, including concerns about surveillance, data breaches, and identity theft. As the number of blockchain applications and use cases expands beyond the traditional cryptocurrency sphere, the need for privacy is becoming more acute.

As a result, we can expect to see continued growth in the market for privacy-enhanced blockchain solutions like “XRPL Solvency” as more individuals and businesses seek to protect their transaction data and maintain their privacy on the blockchain. However, there may also be challenges in this market, such as regulatory issues and concerns about the use of privacy-enhanced technologies for illicit purposes.

8. Business model.

Our Core Product will be to develop and maintain the open-source XRPL Solvency solution, which provides privacy and proof of solvency to users through the use of cryptographic ring signatures. This core product will be the foundation of our business and will help establish our reputation within the XRPL community. However, we will develop other strategies that will help us generating income through various avenues, such as:

Customizable Modules: Offering customizable modules or plugins for different platforms, such as e-commerce websites, exchanges, or other blockchain-based services that require solvency proofs. These modules can be licensed on a subscription basis or with a one-time fee, depending on the complexity and the level of support required.

Enterprise Solutions: Providing tailored enterprise solutions for larger companies that require more extensive customization or integration with their existing systems. This could include additional privacy features, advanced analytics, and reporting capabilities. Enterprise solutions can be priced based on the scope of the project and the level of support needed.

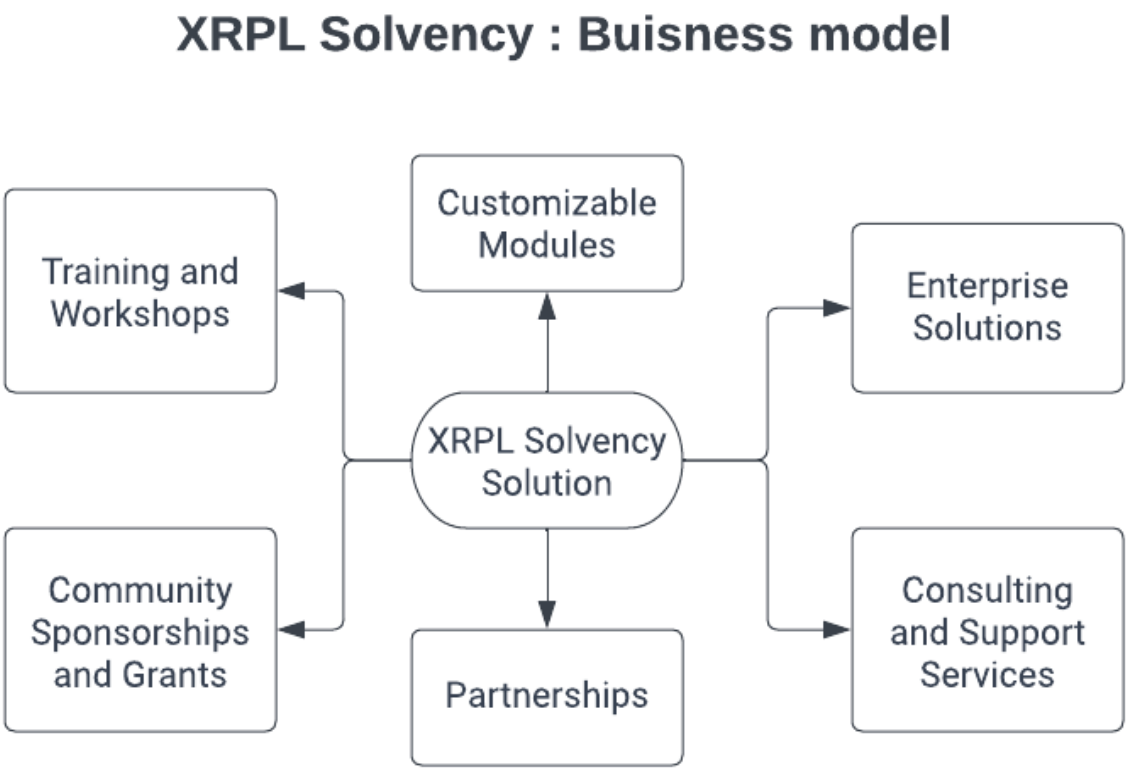
Consulting and Support Services: Offering consulting and support services to help businesses implement and make the most of our XRPL Solvency solution. This can include assistance with integration, customization, best practices, and troubleshooting. We can charge an hourly rate or offer fixed-price packages for these services.

Partnerships: Forming strategic partnerships with other companies and platforms in the blockchain ecosystem to promote and integrate our XRPL Solvency solution. Revenue-sharing agreements or referral fees can be established with partners to create a mutually beneficial relationship.

Community Sponsorships and Grants: Applying for sponsorships, grants, or funding from organizations within the XRPL or broader blockchain ecosystem. This could help support the development of the open-source XRPL Solvency solution while fostering a stronger relationship with the community.

Training and Workshops: Conduct training sessions and workshops for developers, businesses, and other interested parties to educate them on the benefits and use cases of our XRPL Solvency solution. These events can be monetized through ticket sales or sponsorships.

By combining these revenue streams, we can create a sustainable business model that allows us to contribute to the XRPL community while also generating income through various avenues.



9. Marketing strategy

Target Audience: As previously mentioned, our target audience includes individuals, businesses, financial institutions, government agencies, and non-profit organizations. Each of these groups has different needs and pain points that should be addressed in our marketing strategy.

Key message: Our key message emphasizes the unique benefits of XRPL Solvency solution, which is enhancing privacy, and solvency verification. Giving our users several benefits such as:

- **Protecting Personal Information:** Privacy is essential for protecting personal information on the blockchain. By enhancing privacy, users can protect their real identity, transaction history, and other sensitive information from being exposed to third parties.
- **Reducing the Risk of Fraud:** Enhancing solvency verification can help reduce the risk of fraud on the blockchain. By verifying a user's solvency without disclosing their wallet address or transaction history, it becomes harder for fraudsters to fake or manipulate their financial status.
- **Encouraging Adoption:** Enhancing privacy and solvency verification can help encourage adoption of blockchain technology. By addressing concerns about privacy and security, more users may be willing to use blockchain-based applications and services.
- **Increasing Trust:** Enhancing privacy, and solvency verification can also increase trust in the blockchain ecosystem. By providing users with a greater sense of security and control over their information, they may be more willing to engage in transactions and interactions on the blockchain. This can lead to increased trust among users and stakeholders in the blockchain ecosystem, which can ultimately drive greater adoption and usage.

Create Content: The next step for us will be to create content that resonates with the target audience. This includes blog posts, social media content, case studies, whitepapers, and webinars.

Attend Conferences and Events: Attending blockchain and cryptocurrency conferences and events is an effective way to network and connect with potential customers. Our marketing strategy includes a plan to attend relevant conferences and events and showcase XRPL Solvency solutions. Our genesis event, PBWS Hackathon, is a perfect exemple.

Measure Results: Finally, it's important to measure the results of our marketing strategy. This includes tracking website traffic, social media engagement, lead generation, and conversion rates. Based on the results, the marketing strategy should be adjusted and refined to optimize our results

10. Product development

XRPL Solvency enhances features that require to develop technical solutions for front-end and back-end development.

XRPL Solvency – Front End Application

The front-end application in react developed during the PBWS 2023 hackathon aims to offer the possibility to interact with the different ring signature functionalities and to issue proof of solvency for different use cases.

Structure:

Home page: In this section you will learn more about our XRPL Solvency project and the "proof of solvency" that we can generate and issue thanks to ring signatures. There are many use cases and we have detailed some of them for you.

What are ring signatures?

Ring signatures are a cryptographic technique that allows a member of a group to sign a message on behalf of the group without revealing which member actually signed it. The concept was first introduced by Rivest, Shamir, and Tauman in 2001. The primary purpose of ring signatures is to enhance privacy and anonymity in digital communication.

What is the difference with ZK Proofs?

Ring signatures and Zero-Knowledge Proofs (ZKPs) are both cryptographic techniques that enhance privacy and anonymity. However, they serve different purposes and have different properties. The reasons why ring signatures are a better fit to our model are the following:

Ring signatures offer a relatively simpler cryptographic mechanism compared to ZKPs, which could make them easier to understand, implement, and maintain in our solution. This simplicity might lead to a quicker development process and easier adoption by the community.

Also, as mentioned earlier, ring signatures are compatible with both XRPL and Ethereum Virtual Machine (EVM) environments due to their reliance on elliptic curve cryptography. In contrast, some ZKP schemes (e.g., zk-SNARKs) may require additional workarounds to be compatible with the existing cryptographic primitives used in these platforms, making the integration process more complex.

Moreover, some ZKP schemes, like zk-SNARKs, require a trusted setup phase where cryptographic parameters are generated. This process could introduce a centralization risk and might not align with the open-source and decentralized nature of our project. Ring

signatures do not require a trusted setup and are, therefore, more in line with the goals of our solution.

Another advantage is that ring signatures are specifically designed to provide signer anonymity within a group, which is the primary requirement for our solvency proof application. While ZKPs can also provide privacy, their broader scope might be overkill for our specific use case and may introduce unnecessary complexity.

Finally, given that ring signatures are already used in privacy-focused cryptocurrencies like Monero, developers and users in the blockchain community might be more familiar with the concept. This familiarity can make it easier for our solution to gain traction and adoption.

How Ring Signatures Work:

First step is Group formation. A group of participants is formed, each with their own public-private key pair. The public keys of all members are combined to create a “ring” of public keys. Anyone can form this group, and it doesn't require the members to collaborate or even know each other.

Then we generate the Signature. When a group member wants to sign a message, they use their private key and the public keys of the other group members to create the ring signature. The signature generation algorithm ensures that it is computationally infeasible to determine which member's private key was used to create the signature. The generated ring signature is attached to the message.

Finally comes the signature verification When someone receives the signed message, they can use the ring of public keys to verify that the signature is valid and that it was created by one of the group members. However, they cannot determine which specific member signed the message.

Technologies used:

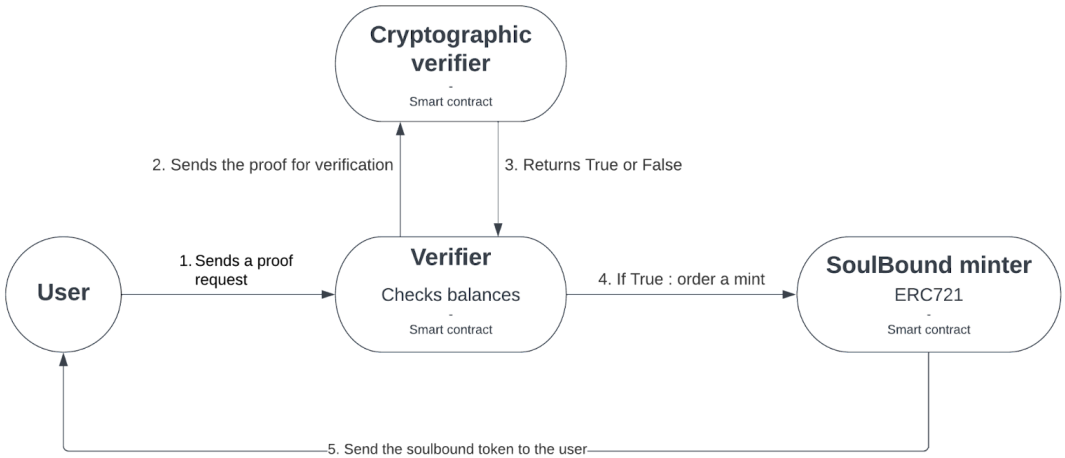
- React
- Python
- Cryptography librairies
- XRPL

Supported networks:

XRPL Testnet.

Architecture

Proof generation:



Here is a recap of why we think XRPL Network is a perfect fit for our solution:

Benefit	Description
Fast and Low-cost Transactions	Enables users to quickly generate and verify solvency proofs without incurring significant costs.
Decentralization and Security	Offers a secure platform for our privacy-focused solvency proof solution, thanks to its decentralized nature and consensus mechanism.
Wide Adoption and Ecosystem	Allows us to tap into the existing XRP Ledger Network user base and enhance the value proposition of our offering.
Built-in Exchange and Tokenization Capabilities	Facilitates seamless integration with various use cases, such as tokenized real-world assets or DeFi applications, requiring solvency proofs.
Commitment to Privacy and Innovation	Aligns with a platform that shares our dedication to user privacy and innovation within the blockchain space.
Scalability	Provides a platform designed to handle high transaction volumes efficiently, ensuring our solution can grow without compromising on performance.
Developer-friendly	Offers developer resources, tools, and compatibility with various programming languages for easy development and integration of our solution.

Here is a recap of why we think XRPL Network is better than other famous networks:

Feature/Benefit	XRP Ledger Network	Ethereum	Binance Smart Chain (BSC)	Solana
Transaction Speed	Extremely fast, settling transactions in 3-5 seconds.	Slower, taking from 15 seconds to several minutes, depending on network congestion.	Faster than Ethereum, with transactions taking around 5 seconds.	Extremely fast, with transactions settling in under a second.
Transaction Cost	Low transaction fees, typically around $0.00001 per transaction.	Higher fees, especially during network congestion, which can range from a few cents to several dollars.	Lower fees compared to Ethereum, but higher than XRP Ledger Network.	Low fees, competitive with the XRP Ledger Network.
Scalability	Designed for high transaction volumes, making it suitable for growing demand for privacy-focused solvency proofs.	Limited scalability, facing challenges with high transaction volumes, potentially impacting our solution's growth.	More scalable than Ethereum but may face challenges with extremely high transaction volumes.	Highly scalable, handling up to 65,000 transactions per second.
Decentralization and Security	Decentralized platform with a consensus mechanism, ensuring a high level of security for privacy-focused solvency proofs.	Decentralized platform, but may face security challenges with certain DeFi applications and smart contracts.	Less decentralized compared to Ethereum and XRP Ledger Network due to the consensus mechanism used.	Decentralized and secure, employing the Proof of History (PoH) consensus algorithm.
Ecosystem and Adoption	Established and growing ecosystem with numerous use cases and applications.	Largest ecosystem with a wide variety of use cases, including DeFi and NFTs.	Rapidly growing ecosystem, with many projects migrating from Ethereum due to lower fees and faster transactions.	Growing ecosystem with a focus on high-performance and scalable applications.
Built-in Exchange and Tokenization Capabilities	Built-in decentralized exchange and custom token (IOU) support.	Supports custom token creation through ERC standards, but no built-in exchange.	Supports custom token creation through BEP standards, and has a built-in decentralized exchange, PancakeSwap.	Supports custom token creation through SPL standards, but no built-in exchange.
Developer Resources	Provides developer resources, tools, and compatibility with various programming languages for easy development and integration.	Extensive developer resources and the largest developer community among blockchain platforms.	Developer resources and compatibility with Ethereum, allowing for easy migration of projects.	Growing developer resources and documentation, with compatibility to several programming languages.

TECHNOLOGY

Here is how our solution works in technical details.

There are 3 steps to building a proof of credit:

The first is the construction of the ring that will serve as the anonymity set. This construction is done for the moment by recovering the last transactions on the network, then by checking that the different addresses participating in the transactions have at least the necessary amount to prove. In the future, we will try to make the construction of the ring more intelligent. Indeed, let's imagine that a known address associated to an exchange is in the ring, we will then be able to know that this address is not mine and thus increase the chances to link my identity to my address.

The second is the signature itself. To do this we need the private key of the address that has the funds. Once in possession of this address and the anonymity set, the user can perform the signature. This signature serves as proof of possession of an address with at least the minimum required funds.

The third is the SBT mint containing the signature data. To do this, we need the private key of the address where the person wants to receive the proof. Once we have this key, we can issue a mint transaction, where the signature data is stored on IPFS, and the URI of the NFT is an IPFS link.

To verify the proof there are 2 steps:

The first one is to retrieve the data from the SBT. To do so the user has to go to our website and in the page verify proof look for the desired address.

Once this address is found, it only remains to copy the proof and to verify it on our executable. The executable checks the proof and then indicates if it is valid or not.

11. Sales Strategies

We aim our solution to be open source. However, the implementation would require some support. This help we provide would be how we generate profit in order to develop and extend. Here are some sales strategies that could be effective for our solution:

Targeted Advertising

Using targeted advertising to reach potential customers who are interested in privacy and solutions for the blockchain. This can include targeting users of existing blockchain applications, social media advertising, and content marketing.

Partnerships and Referral Programs

Establishing partnerships with existing blockchain companies or service providers and implementing referral programs that incentivize current users to refer new customers to the solution.

Content Marketing

Creating valuable and informative content about the solution and the importance of privacy in the blockchain ecosystem. This content can be shared through social media, email marketing, and other digital channels.

Public Speaking and Networking

Engaging in public speaking opportunities, attending conferences and events, and networking with key stakeholders in the blockchain ecosystem to raise awareness about the solution and build relationships with potential customers and partners.

Free Trials and Demonstrations

Offering free trials or demonstrations of the solution to potential customers, allowing them to experience the benefits of the solution firsthand and build trust in the product.

Influencer Marketing

Collaborating with influencers in the blockchain space who have a significant following and a strong reputation to promote the solution to their audience.

Discounts and Promotions

Offering discounts or promotions for early adopters or for customers who refer new business to the solution can help incentivize customers to try the product and spread the word to others.

12. Team

That is the key: the team consists of committed people who love what they do. We are 4 engineering students bound by our passion and commitment for blockchain and Web3. We want to develop innovative solutions that will help the whole ecosystem expand. Too many times have we seen privacy being set aside in projects, and we want to be able to change that. That is why Maxime, Thomas, Nathan and Adam are glad to present XRPL Solvency, the solution for real privacy.

By addressing the need for privacy in the blockchain ecosystem while having a real utility in our daily life, XRPL Solvency has the potential to be a valuable tool for individuals and businesses alike.

13. Technical roadmap

Q3 2023:

- Switch from a python implementation of ring signatures to a typescript implementation.
- Development of a browser plugin to include directly the signature and verification process in the front-end.

Q4 2023:

- Audit of the cryptographic implementation in typescript. Audit of the plugin.
- Release of the implementation as an open-source library.
- Release of the V1 product (proof only possible on the XRP coin)

Q1 2024:

- Creation of an indexer allowing to make proofs on the tokens and NFT present on XRPL.
- V2 beta release (proof possible on all tokens and NFT on XRPL).
- V2 release.