Web3 Foundation Grant Proposal

Project Name: Silent Data Polkadot Integration

Team Name: Applied Blockchain Ltd

Payment Address: USDC (Ethereum) address:
0x91a5ade2522ac8c3761922a4255e0fef89116a37

Project Overview

This application is in response to an RFP

Overview

Applied Blockchain has developed Silent Data as a platform for proving properties of private off-chain (web2) data in blockchain smart contract (web3) applications (dApps).

Silent Data leverages hardware secure enclaves with attestation, in particular, Intel SGX in order to enable privacy-preserving retrieval and processing of off-chain data, and generation of cryptographic proofs that are verifiable in blockchain smart contracts. This ensures that sensitive information is never revealed, not even to those hosting the platform, and code attestation with a smart contract link ensures that the code used to retrieve the data and generate the proofs cannot be modified or interfered with by the operator.

Silent Data proof certificates are powerful because they can verifiably demonstrate that private data meets certain requirements without the need to reveal that data, and without that data being accessible to Silent Data operators. The service is initially centrally hosted, and will be decentralised over time in order so that it cannot be censored by the operator.

Silent Data enables verification of web2 account ownership, including social media services such as Instagram. This enables enrichment of web3 identities and assets with attestations from the web2 world, for example, if someone is using web3 to purchase from a brand with a web2 presence.

NFT creators with verified Instagram accounts, for example, can use Silent Data to prove they are behind a specific wallet. This will help to reduce fraud in NFT and web3 commerce.

Silent Data will also be extended to enable verification of web2 financial credentials, to augment web3 DeFi and tokenisation dapps.

- **An indication of how your project relates to / integrates into Substrate / Polkadot / Kusama.**

Silent Data provides privacy-preserving cryptographic proofs about properties of web2 data. We refer to the output as a “proof certificate”, consisting of a set of key-value pairs signed by a manufacturer attested hardware secure enclave. The signatures can be verified using various cryptography primitives available on different blockchains, including Polkadot (Substrate) and Ethereum. A blockchain wallet is associated with a Silent Data proof certificate by having the wallet owner sign the private data that is encrypted and sent to the enclave with their wallet private key.

Silent Data will integrate with both Moonbeam (EVM) and a Substrate chain to provide maximum coverage within the Polkadot ecosystem.

Integrating and enabling Silent Data in Polkadot parachains will help to bring additional functionality and security to Polkadot dapps that have some reliance or interaction with the web2 world and web2 accounts.

Pokadot will benefit through enabling identifies to be further verified where necessary using cryptographically verifiable proofs of web2 accounts (social media, such as Instagram, or otherwise), enabling the DeFi ecosystem to grow more securely beyond native on chain assets to those assets whose origin, provenance and/or price are anchored in web2 accounts (through additional integrations with other web2 accounts). Polkadot DeFi investors will benefit from increased cryptographic verifiability when backing off chain and real world assets.

- **An indication of why your team is interested in creating this project.**

Applied Blockchain was founded by Adi Ben-Ari, in London in 2015 when the Ethereum code base was first released, and he spent the early months with some members of what became the Parity team exploring and understanding the platform. Since then Applied Blockchain has closely followed developments at Parity and Polkadot (including some minor collaborations along the way), and is particularly interested in bringing the Silent Data technology to Polkadot parachains and dapps.

Polkadot parachains already offer a broad range of dapps and functions, and coupling the strong security fundamentals of Substrate with those of Silent Data will create compelling additional optionality for Polkadot dapp developers.

Project Details

your project's expected final state.

- Mockups/designs of any UI components

  September 2022

- Data models / API specifications of the core functionality

  September 2022

- An overview of the technology stack to be used

Silent Data includes a public facing web application and API that facilitate communication with a secure enclave. DApps can request an individual to securely transfer their data to the enclave for verification. Generally, the subject of a check will provide access to their data to the enclave via an OAuth flow which generates credentials that can be used to fetch data from APIs on behalf of the subject. These credentials are encrypted and sent to the enclave along with a signature of the private data used to verify ownership of a blockchain wallet.

The enclave decrypts the credentials and uses them to retrieve data from trusted data sources over HTTPS (initially Instagram). The enclave will then perform the preconfigured calculations and checks on the data in order to verify that the input query is true or false. The wallet signature and decrypted credentials are also used to prove that the owner of the wallet had access to those credentials and is most likely the owner of the data.

The enclave can optionally associate and attest to non-private data relating to the check (e.g. Instagram account name) by including it in the proof certificate data as key-value pairs. The proof certificate includes some standard information such as an identifier of the check performed, the wallet address of the user, a timestamp, and the identifier of the proof certificate on Silent Data, along with any extra non-private data. The enclave will then sign this certificate using an algorithm compatible with the target blockchain and send it to the the dApp smart contract for persistence and verification.

Substrate and Moonbeam dApp smart contracts will initiate the Silent Data proof of Instagram account ownership check. The smart contracts will receive the proof certificate from the Silent Data enclave, and verify the attestations, proving that the owner of the wallet is the owner of an Instagram account, but proving they have direct access to login to the web2 account.

- **Documentation of core components, protocols, architecture, etc. to be deployed**

  Documentation of core components, protocols and architecture to be deployed can be found here: Silent Data Architecture

- PoC/MVP or other relevant prior work or research on the topic

  Silent Data News: https://silentdata.com/news

Ecosystem Fit

- Where and how does your project fit into the ecosystem?

We believe that as part of the evolution of web3, web2 and web3 will converge before diverging. This will enable users to leverage their identies and assets, currently anchored in web2 to the web3 world. In order for this to occur, web3 DApps, including those deployed in many of the Polkadot parachains, need a way to securely and safely verify off-chain web2 data.

Regular web2 API integrations require trust in additional third parties, as data can be compromised, viewed and manipulated. Standard blockchain oracles reveal sensitive web2 data to validators. With Silent Data, DApps can now fully verify web2 data properties, without any data being revealed.

There are already numerous parachains deployed in the Polkadot ecosystem, primarily focussed on DeFi, NFTs, identity and tokenisation services. Many of those parachains and dApps can benefit from integrating with Silent Data to verify web2 credentials, including Instagram account ownership to provide proofs that can then be leveraged by the parachain dApps (for example to augment the identify of a seller wallet) without the need to share any user data during the verification process and without storing the user data in the parachain. Silent Data will also be extended to enable verification of web2 financial credentials, to augment web3 DeFi and tokenisation dapps.

.

- What need(s) does your project meet?

The project enables smooth and user-friendly proof of web2 account ownership and credentials in web3 dApps. This can be used to reduce fraud, but augmenting web3 wallet identities and assets with verified web2 account data (e.g. Instagram account ownership), without revealing sensitive account data and credentials to any third parties or platform operators..

Silent Data can be used to verify web2 account ownership, such as social media accounts ownership such as Instagram, for example, to provide proofs that can be used inside the web3 environment. The solution guarantees complete confidentiality and that no user data is visible during the verification process, no even to the platform operator, nor is it persisted anywhere outside the web2 platform.

NFT creators with verified Instagram accounts, for example, can prove they are behind an NFT and prove their wallet owns a certain verified Instagram account. With this they can avoid it being impersonated or having fake assets being associated with their identity by providing cryptographic proof of Instagram account ownership and associating this with their wallet and minted NFT.

Future implementations will apply not only to Instagram and NFT’s, but also to other identity and asset credentials useful in DeFi.

Team

Team members

- Adi Ben-Ari
- Francesco Canessa, Andrew Campbell, Shawn Derouard, Mario Gemoll, Thomas Brooks, Shay Har-Zion

Contact

- Adi Ben-Ari
- adi@appliedblockchain.com
- https://appliedblockchain.com/

Legal Structure

- Level 39, One Canada Square, Canary Wharf, London E14 5AB, UK

Team's experience

Adi Ben-Ari is the founder & CEO at Applied Blockchain. Prior to starting the company Adi spent 20 years as a developer, technical lead and solution architect in telecoms, insurance and banking.
LinkedIn: https://www.linkedin.com/in/adibenari/

Francesco Canessa is the CTO at Applied Blockchain. Francesco is a seasoned technology expert and a serial hackathon winner, with a decade of experience in software development and four years within building blockchain applications. Francesco has worked on large-scale enterprise projects and with startups, building solutions for Sky TV Italia, 5Apps, and Quill Content to name a few. He has also developed tools and libraries for Ethereum and Bitcoin. Francesco is a fan of reading, writing and talking about software development, and is an open source enthusiast. When he's not looking at code, Francesco builds and rides electric skateboards.
LinkedIn: https://www.linkedin.com/in/makevoid/

Andrew Campbell is a solution architect with over 10 years of development experience including over 6 years industry experience. He has spent the last 6 years working with a range of London based startups. As an architect he has designed solutions for a range of enterprises including Shell, Vodafone, UN - World Food Programme, SITA. He has been the architect of tens of blockchain and advanced cryptography projects and many of his architectures have been taken into production.
LinkedIn: https://www.linkedin.com/in/andylnd/

Mario Gemoll leads R&D at Applied Blockchain. Mario studied Computer Science (BSc TU Munich, MSc Oxford) and has several years of experience as a software engineer. He joined Applied Blockchain in 2017. At the company, Mario has led research into blockchain protocols, advanced cryptography and hardware secure enclaves, as well as leading design and development of a major NFT platform. Mario leads the research and development of Silent Data for privacy-preserving proofs of off-chain data using Intel SGX secure enclave technology. Prior to Silent Data, Mario led development of the K0 blockchain protocol bringing transactional data privacy to existing smart contract blockchains using zero-knowledge proofs. Mario also led research and developed a secure multi-party computation protocol for privacy-preserving price discovery in trading environments.
LinkedIn: https://www.linkedin.com/in/mariogemoll/

Ricardo Seromenho is a full stack developer at Applied Blockchain. He is a Node.js application/services certified developer with a degree in Information Technology and 7 years experience. He is a hands-on software engineer with a big passion for best practices and reusable patterns and proficient in a wide range of technologies.
LinkedIn: https://www.linkedin.com/in/rseromenho/
GitHub: https://github.com/seromenho

Thomas Brooks is one of the core developers on the Silent Data platform at Applied Blockchain. He joined the company after completing a doctorate in high energy particle physics, developing software and machine learning algorithms for 3D particle interaction reconstruction. Thomas has a broad range of experience in software development, from creating open source visualisation and analysis tools used by world leading biology labs to writing Ethereum smart contracts for DeFi applications.
LinkedIn: https://www.linkedin.com/in/tom-brooks-a940a9a7/
GitHub: https://github.com/tgrbrooks

Shay Har-Zion is a product manager with over 17 years of experience in leading product and project software developments, with majority of them in the financial services and Fintech industries. Shay puts in front the focus on teamwork, communication and collaboration, in order to produce highest value and quality towards innovative solutions for clients.

Team Code Repos

- https://github.com/appliedblockchain
- https://github.com/appliedblockchain/silentdata-defi-core (The SGX components)
- https://github.com/appliedblockchain/silentdata-defi-app (The web app components)

Please also provide the GitHub accounts of all team members. If they contain no activity, references to projects hosted elsewhere or live are also fine.

- https://github.com/seromenho
- https://github.com/tgrbrooks

Team LinkedIn Profiles

- https://www.linkedin.com/in/adibenari/
- https://www.linkedin.com/in/shay-har-zion-3a31933/
- https://www.linkedin.com/in/andylnd/
- https://www.linkedin.com/in/tgrbrooks/

Development Status

If you've already started implementing your project or it is part of a larger repository, please **provide a link and a description of the code here**. In any case, please provide some documentation on the research and other work you have conducted before applying.

Silent Data Architecture: Silent Data Architecture

Development Roadmap

Milestone 1: Substrate and Moonbeam adapters (**2 months duration**, 1 full-time employe, 3 part-time employees, **$30,000**)
-Extend the Silent Data confidential computing oracle to generate proofs verifiable by Polkadot and Moonbeam smart contracts. Deploy Silent Data smart contracts to the Polkadot and Moonbeam testnets and implement Instagram account verification from a DApp.
The testnet examples will be shared with Polkadot developers to integrate Silent Data into their dapps and parachains.

Overview

- Total Estimated Duration: 2 months
- Full-Time Equivalent (FTE): 2.5 (1 full time employee, 3 part-time
- Total Costs: 30,000 USD

Future Plans

- Integration with other web2 social media platforms (Twitter, Google authentication, ..check for others).
- Integration with other identity and asset related web2 data sources (open banking, identity and AML checks).
- The team's long-term plan is to become the platform for providing properties of private web2 data for consumption by web3 applications.