29 MARCH 2022

ZERO KNOWLEDGE LEGAL WORKING GROUP INITIAL REPORT

EXECUTIVE SUMMARY

The Zero Knowledge Legal Working Group, made up of ten teams, was established to help understand the opportunities and questions held by projects looking to build with Zero Knowledge Proofs (ZKPs). This report aims to shed some initial light into how teams are thinking about using this technology and encourage more developers to use ZKPs in the blockchain industry. The report is broken down into three areas: The implementation of ZKPs for KYC (Know Your Customer), using ZKPs for Data Protection and where the burden of legal responsibility falls when developing with ZKPs.

Through our interviews, it was established that there is massive potential for implementing ZKPs for KYC purposes. However, there is a lot of uncertainty and ambiguity around how a ZKP based KYC application should be designed to ensure compliance with existing KYC requirements and how such technology could be incorporated into current KYC tools. Similarly for enhanced data protection applications such as selective disclosure, proof of certification and determining more information about an individual's internet identity, the use of ZKPs could present a big opportunity in minimising the amount of data stored on an individual, which is a component of GDPR. For developers and projects implementing ZKPs into their application or protocol the predominant legal concerns were around whether the implications of their application being used for illegal activities, despite having no control over this and if a centralised entity might remain legally responsible for a protocol after it has undergone decentralisation. In general, the rate of new legislation being drafted does not keep pace with the rate of innovation in the blockchain space needs, and so can stifle innovation. We hope the work from this group can help to tip this in the opposite direction.

This report is only a starting point. For this preliminary work to move forward and have a greater impact, more funding and time must be committed to this initiative beyond the foundations that have been laid herein.

GLOSSARY

AML	Anti-money Laundering
EU	European Union
FATF	Financial Action Task Force
GDPR	General Data Protection Regulation
KYC	Know Your Customer
L1	Layer 1
L2	Layer 2
MICA	Markets in Crypto Assets
PII	Personal Identifiable Information
VASP	Virtual Asset Service Provider
VC	Verifiable Credential
ZKP	Zero Knowledge Proof
ZKRP	Zero Knowledge Range Proof
ZKSM	Zero Knowledge Set Membership

CONTENTS

INTRODUCTION

Zero Knowledge Proofs (ZKPs) are a type of cryptographic proof that enables a prover and a verifier to confirm that the prover possesses certain information without revealing what this information is, hence verifying that a statement is true. A ZKP must consist of three elements:

- Soundness: the probability that a verifier can guess and trick the prover must be very low,;
- Completeness: when both prover and verifier act honestly the verifier is convinced by the prover that the statement is true
- Zero knowledge: no other information is conveyed to the verifier by the prover other than the knowledge that the statement is true.

MOTIVATION

ZKPs have the potential to transform privacy and scaling in the blockchain space. Their implementation has already been seen in scaling applications, particularly for layer 2 scaling solutions on the Ethereum network, implemented to power the high transaction throughput of decentralised exchanges where transaction fees have been dramatically reduced due to processing multiple transactions in a ZKP and appending to layer 1 with one gas fee paid. Examples of rollups include zksync, Aztec, Scroll and the Polygon Hermez network. Using ZKPs for L2 rollups offers the advantage of having data availability on chain, i.e. smart contract execution and transactions are verifiable on chain.

Other teams are building ZKP powered L1s, such as Mina, Penumbra, Aleo, and Anoma. In some of these cases, they may be also using ZKPs to provide selective disclosure or privacy to their users.

The ecosystem for implementing ZKPs is growing although it is still very early. To encourage more developers to build with ZKPs, clarifying the legal position of ZKPs will assist with risk mitigation for smaller projects, and in particular for teams just starting out without extensive capital or resources to fund legal advice. This is crucial for increasing adoption of ZKPs in the blockchain space.

RESEARCH QUESTIONS

This report aims to explore three themes around the opportunities and concerns linked to the use of ZKPs and privacy in blockchain networks and applications.

1. KYC (Know Your Customer) and Compliance
2. Data Protection
3. Legal Responsibility

WORKING GROUP MEMBER PROFILES

Aleo has developed a bespoke programming language, Leo alongside a development toolkit which enables developers to build privacy preserving applications by default. The integrated development environment (IDE) is tailored specifically for enabling zero knowledge proofs to be implemented within applications without requiring PhD level expertise in the subject area.

Anoma allows all crypto assets to share the same shielded pool — for example making a transaction involving DAI would be made indistinguishable from another one involving an NFT through implementing a multi-asset shielded pool (MASP). With the deployment of customized zero-knowledge circuits to enable different use cases, Anoma is able to facilitate interactions in the network with different levels of privacy guarantees (partial, full) depending on the requirements.

Aztec is a layer 2 protocol enabling Ethereum to scale whilst guaranteeing user privacy. Aztec enables identities, balances and transactions to remain private through the implementation of PLONK, a zk-SNARK construction. The Aztec rollup enables fast private transactions that save on gas fees.

c-Labs is part of the community building Celo. Celo is a mobile first application that makes it possible for anyone with a mobile phone to be able to use crypto based payments and use financial dApps.

rhino.fi (previously Deversifi) is a layer 2 exchange facilitating fast, private and gas free transactions. The zkrollup technology StarkWare (STARKS) is a cryptographic proof that permits thousands of transactions to be settled on the Ethereum blockchain in a single batch transaction, the enabling technology behind Deversifi's exchange.

Figment is a blockchain infrastructure and service provider that supports the web3 ecosystem with staking infrastructure, active on more than 35 mainnets, the Hubble Web 3 explorer and developer tools.

Gnosis produce interoperable products for the Ethereum ecosystem that enable users to create, through a conditional token framework powering prediction markets such as Omen, trade, with Cowswap and Gnosis Protocol V2 which leverage batch auctions to protect against MEV, and hold digital assets through the Gnosis Safe for use in decentralised finance.

Iden3 is an open-source set of tools for creating and managing self-sovereign identities on public blockchains: Identities that allow you to prove things about yourself while safeguarding your right to privacy.

Mina is a layer 1 protocol that utilises zk-SNARKs to verify the state of the blockchain without having to download the entire history. This enables users to interact with the blockchain as non-consensus nodes whilst only downloading approximately 22kb of data, essentially any user with an internet connection can use Mina.

Least Authority is committed to creating freedom compatible and privacy preserving technologies. They achieve this by providing a range of services including security audits, consulting, developing and contributing to open-source software projects and collaborating with non-profit foundations to provide privacy for human rights defenders.

ZKValidator is a mission driven validator aiming to raise the profile of privacy and zero knowledge proof technology adoption in the blockchain space through multiple initiatives including events, governance and funding. The validator is currently active on ten networks, including: Cosmos, Osmosis, Polkadot, Kusama, Moonriver, Celo, Mina and NEAR.

Qedit builds infrastructure for Web3 and the blockchain space to enhance scalability and privacy of decentralised applications. They do this through implementing zero knowledge proofs in the broad areas of business growth, data monetization and risk mitigation.

METHODOLOGY

The purpose of the working group is to gather questions and concerns regarding the implementation of ZKPs in relation to the member's projects. This information is to be presented in an open source format, to share any insights with the wider ZK and privacy community. There were two main avenues for data collection that were pursued after the first group meeting, these approaches were 1) asking group members to fill out forms, and 2) through structured interviews.

FORMS

During this initial phase of the project, two separate forms were sent to group members. The first form was sent to group members before the first working group meeting. The form contained the following questions:

- Have regulatory concerns prevented your project from developing in a specific direction? For example, have you stopped the ideation or development of a particular product or protocol because of these concerns?
- What legal concerns do you have in regards to ZK technology and privacy? E.g. compliance, KYC, etc. Have you started any work in regards to these concerns?
- Are you aware of the EU's proposed MICA (Markets in Crypto Assets) regulation?
- Do you feel MICA applies to your organisation?

The second form followed on from the discussion in the first working group meeting which helped to set the focus of the working group. The second form contained the following questions:

- Have you already received any professional legal advice relating to the use of ZKPs or privacy technology?
- If you decided against legal advice how did you work around this or resolve any concerns you may have had?
- Have you been put off seeking legal advice due to costs?
- What legal questions, concerns or challenges does your company have around the use of ZKPs for better information management in the KYC process?
- What legal questions, concerns or challenges does your company have around the use of ZKPs for data protection.

- What legal questions, concerns or challenges does your company have around the challenges of ZKPs and privacy preserving technologies and coins under the planned MICA regulation.
- What legal questions, concerns or challenges does your company have around the burden of legal responsibility when ZKPs and privacy technology is implemented.
- Of the four themes - KYC, data protections, civil liberties and restriction of ZK, burden of legal responsibility, which do you think is/ are most relevant for your organisation and should be prioritised by the working group?

Other than potential biases in the language of the questions, the main limitation of data collection with the forms was low participation. It was difficult to gather a lot of responses from members of the working group and often the responses were brief. This was discouraging, although during the working group meeting, it was observable that working group members did have a lot of insight and information to share. Because of this, an alternative approach was taken to gather data from group members through structured interviews.

Questions around civil liberties and the restriction of ZK and privacy technology in blockchain systems were asked in early meetings but in developing the project, we felt that this line of enquiry fell outside the scope of this first report.

STRUCTURED INTERVIEWS

Data collection through structured interviews was conducted with two interviewers. Each interview lasted 30 minutes, during the interview five questions were asked.

1. Have you already sought out legal advice regarding the use of ZKPs?

2. What legal questions, concerns or challenges does your company have around the first theme: KYC and the use of ZKPs for better information management in the KYC process.

3. What legal questions, concerns or challenges does your company have around the second theme: ZKPs for data protection

4. What legal questions, concerns or challenges does your company have around the third theme: Civil Liberties and restriction of ZK and privacy technology - under the planned Markets in Crypto Assets (MICA) regulation e.g. encrypted messages were initially banned in the US as they were considered weapons.

5. What legal questions, concerns or challenges does your company have around the fourth theme: Legal Responsibility - On which party does the regulatory and legal burden fall upon. E.g. Cryptographer, protocol designer, protocol implementor, protocol deployer, customer who uses the protocol (such as a DApp or exchange), user.

THE IMPLEMENTATION OF ZKPS FOR KYC

Using ZKPs to enable compliance with KYC, Know Your Customer, regulation presents itself as a great opportunity for ZKP implementation. This sentiment is felt by many members of the working group with Iden3 in particular actively working on a solution for a ZKP based KYC process (what was to become zkID). Beyond overcoming the technological requirements for a successful implementation, legal and regulatory barriers pose a challenge to innovators and potential users of such technology in the space. The concerns and uncertainties that surfaced during data collection can broadly be split into two categories:

1. Process Adoption and Standardisation
2. Meeting Regulatory Requirements / Proving Compliance

These issues will be discussed in turn.

PROCESS ADOPTION AND STANDARDISATION

Anti money laundering (AML) requirements necessitate that protocols or exchanges handling monetary instruments conduct due diligence on their clients. The requirement to complete KYC differs by jurisdiction, for instance crypto only trading in the EU does not currently require KYC whereas in the USA, crypto is considered in the same light as fiat currencies with regard to KYC requirements[1]. However, legislation is adapting and constantly evolving[2]. Nonetheless, to meet these KYC requirements, personal identifiable information, PII, is collected during the onboarding process. PII includes the name, date of birth, and address of the person in question and is verified by comparing with official documentation such as a driving license, identity card or passport. Different exchanges and protocols will have their own procedure which typically encompasses photographing official identity documents and verifying biometric data. The PII data is then encrypted and stored, enabling government bodies, such as law enforcement, to request access to the data if it is required.

---

[1] Getid. 2021, April 11, The 2021 Guide to AML and KYC for Crypto Exchanges & Wallets [Blog Post] Retrieved from https://getid.com/aml-kyc-crypto-exchanges-wallets/ on 25/01/22

[2] Poskriakov, R and Cavin, C, Blockchain & Cryptocurrency Laws and Regulations 2022 | 10 Cryptocurrency compliance and risks: A European KYC/AML perspective [Book Chapter] Retrieved from https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/10-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective on 25/01/22

However storing data for KYC in this centralised fashion can lead to multiple problems[3]:

- Data security - data breach through hacks and leaking of personal data.
- Excessive data stored - extra information other than what is required to be legally compliant. For instance, taking a photo of an identification card would also share someone's signature, place of birth or using a bank statement for a proof of address would compromise transaction data.
- Data protection concerns - once data is shared, what power does the person whose data is shared realistically have to protect their own data.

For more extensive adoption of a ZKP based KYC approach, buy-in from multiple parties, be it protocols or exchanges, will be required so a new standard approach can become the status quo.

MEETING REGULATORY REQUIREMENTS AND PROVING COMPLIANCE

Regulators are yet to see a successful implementation of ZKPs for KYC, as such regulation is not yet clear for this specific application. Regulators want to ensure the implementation of ZKPs complies with data protection requirements whilst proving that the identity of the client is known. Data protection requirements for within the EU are prescribed by GDPR and must be adhered to for a compliant implementation utilising ZKPs for KYC. Yet across different jurisdictions there are different regulatory requirements, and this creates more confusion for blockchain projects which operate worldwide. GDPR is broadly considered to be the strictest data protection policy, hence adhering to standards for GDPR and assuming this will comply with other jurisdictions is a logical strategy.

The matter of where the data for the KYC process is stored and who has access to it is also a major point of contention. Privacy preservation can also be viewed by regulators through the unfavourable perspective of enabling money laundering, fraud and tax avoidance rather than imparting the advantage of greater data protection for the average user. Existing guidance from FATF, updated in 2021, provides direction for service providers on standards for information sharing between virtual asset service providers, VASPs[4]. FATF guidance is motivated to combat money laundering and terrorist financing. This guidance stipulates that there should be co-operation between different supervisors and multilateral agreements for VASPs which are handling multilateral assets. For a decentralised exchange, such as rhino.fi,

[3] Pauwels, P, 2021, June, A solution concept for KYC without knowing your customer, leveraging self-sovereign identity and zero-knowledge proofs [Paper] Retrieved from https://eprint.iacr.org/2021/907.pdf on 25/01/22

[4] FATF, OECD, 2021 October, Virtual Assets and Virtual Asset Service Providers [Report], Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf on 25/01/22

where an external trigger, e.g. cyber security risk, could warrant information sharing, it is unclear whether a ZKP based KYC solution would be an acceptable solution for information sharing in these circumstances.

In general, members of the working group would benefit from clearer guidance on what a ZKP based KYC would need to look like to be a suitable, compliant solution. Due to unclear guidance, approaching the regulatory grey areas with a proof of concept seems to be the best solution, not to hinder innovation in the space and to provide a platform for future iterations.

CONCLUSIONS

There is a big opportunity for a ZKP based KYC solution but it would be beneficial to have clearer guidance on what would need to be done to prove compliance to regulations. Additionally, if regulators make clear guidelines, it would also be useful for these guidelines to be put into a format where standards for the KYC process could easily be adopted by multiple entities in the blockchain space.

USING ZKPS FOR DATA PROTECTION

ZKPs for compliance with KYC and Data Protection are topics that are intrinsically linked, but the focus on data protection broadly considers all data held that could be subject to data protection regulation rather than only the data held for compliance with KYC requirements. Some example use cases of ZKPs for data protection include any instances of selective disclosure, such as proving income is above a threshold level, use cases concerning health data, or proof of age above a certain limit. Similarly, ZKPs could be used for ensuring the privacy of verifiable credentials (VCs) - digital claims to prove something about a person or asset. These instances all have potential applications in regulatory matters and the use of ZKPs could ensure compliance with GDPR. In this section, we will examine how ZKPs could achieve compliance with GDPR, typically considered one of the most restrictive data protection policies and some potential data protection applications utilising ZKPs.

GDPR COMPLIANCE WITH ZKPS

Within the GDPR, article 25 is concerned with data minimisation and reducing the amount of data held on a specific party, only retaining what is absolutely necessary[5]. The use of ZKPs would present an opportunity here generally because they enable information to be verified without actually revealing the information, meaning the amount of data, or size of the data actually stored could be minimised. This is highly relevant for verifiable credentials and in practice this could be implemented by utilising zero knowledge range proofs (ZKRPs)[6]. ZKRPs verify that some data lies within a specified range, for instance there could be a clear need to prove that a user is an adult, therefore if their age was in the range of 18 - 120 it could be proven that they are an adult without storing their actual age data or birthdate. This technique is a subset of the zero knowledge set membership (ZKSM)[7] that verifies that some data in consideration, the commitment, is a part of a list of accepted responses. For instance, you may want to verify that a user's physical address is within a certain zone, so you could have a

[5] 018, May, Article 25 GDPR. Data protection by design and default [Legislation] Retrieved from https://gdpr-text.com/read/article-25/ on 25/01/22

[6] 2019, July, Morais E et al. A survey on zero knowledge range proofs and applications [Paper] Retrieved from https://link.springer.com/article/10.1007/s42452-019-0989-z on 25/01/22

[7] 2020, December, Voelkel J, Selectively Disclosed Verifiable Credentials [Blog Post] Retrieved from https://medium.com/51nodes/selectively-disclosed-verifiable-credentials-79a236b81ee2 on 25/01/22

list of acceptable postcodes. While ZKPs show promise with adhering to GDPR, it is unclear how regulators actually perceive this opportunity.

DATA PROTECTION APPLICATIONS WITH ZKPS

In this section, three example applications are considered and presented that would be possible with a ZKP based solution.

1. **Financial Selective Disclosure**

Using ZKPs to reveal some part of a financial profile, such as what tax bracket someone falls into, or proof that assets are under a certain threshold. When these accounts are on a public blockchain and there is an identity attached to said accounts, ZKPs could potentially be utilised to prove that account balances fall within a particular range, without revealing the account address or exact amounts. This could be useful for banks looking to confirm the wealth of someone taking a loan. Tax agencies could utilise ZKPs to check that the correct rate of tax is being paid. It would also be possible to prove that donations from government organisations are being used for their intended purpose whilst retaining privacy of the amount and addresses involved.

2. **Proof of Certification**

A ZKP could be used to prove that an individual owns a particular account that has possession of a specific token. These tokens could be representations of certificates or tests passed. An ideal form for these would NFTs, Non-Fungible Tokens. Even more appropriate for this use case, would be non-transferrable NFTs (or "Soulbound" NFTs). These are tokens that once minted or sent to an account, can no longer be moved. Thus they would permanently be attached to a specific address. Tools to prove the ownership of particular tokens privately using ZKPs are now being developed with research teams have already proposed ways to do this[8]. This would be an exciting use case for agencies and institutions who work with or rely on certifications.

3. **Internet Identity**

Here you actually use ZKPs to prove that an address belongs to an actual individual, and can help to prove certain characteristics about the individual without revealing additional information. The KYC case described above is one form of information that could be described, but the category is broader. Age, buying habits, browsing behaviour, and other

[8] 2007, May, Laurie B, Selective Disclosure [Paper] Retrieved from https://www.oecd.org/sti/ieconomy/38540177.pdf on 25/01/22

characteristics could be communicated, while cryptographically shielding any other information about this account's owner.

All of these applications present a clear opportunity for the utilisation of ZKPs in achieving the goal of more extensive data protection.

CONCLUSIONS

It is clear that there are opportunities for ZKPs to be used for a plethora of applications pertaining to the goal of data protection. Selective disclosure, proof of certification and internet identity are some of the possible applications and generally all of these could assist in minimising the amount of data an entity must hold on an individual, which is a core component of GDPR. From a regulatory perspective, there was some uncertainty as to whether the implementation of ZKPs for better data protection would be compliant under current GDPR rules.

THE BURDEN OF LEGAL RESPONSIBILITY

Developing applications and protocols encompassing ZKPs presents opportunities for scaling blockchain systems and for privacy. However, concern over what may happen to the developers once code is deployed and live can act as a deterrent to innovating within this space. Discussions around where the burden of legal responsibility falls broadly fell into considerations within two categories:

1. The impact of decentralisation on legal responsibility
2. The impact of protocols / applications being used for illegal activities

These two considerations will be elaborated upon in turn.

DECENTRALISATION AND LEGAL RESPONSIBILITY

Within the wider blockchain space, protocols originally founded by a foundation or organisation have often moved to become decentralised. The classic example of MakerDAO which was developed through the Maker Foundation has decentralised governance in phases through the introduction of the MKR governance tokens and the subsequent planned dissolution of the foundation[9]. Many additional foundations have followed suit, or are signalling their intention to decentralise. Some examples include Shapeshift[10] and the multitude of Cosmos Zones and Polkadot Parachains. However, teams implementing ZK technology into their protocols/ applications are concerned that even if the current governing state of a protocol is decentralised, because the prior state was governed in a centralised manner, this centralised entity, be it foundation or organisation, could be held legally responsible for the future use of this protocol or application.

[9] 2021 July, Dale B, MakerDAO Moves to Full Decentralization; Maker Foundation to Close in 'Months' [Blog Post] Retrieved from https://www.coindesk.com/tech/2021/07/20/makerdao-moves-to-full-decentralization-maker-foundation-to-close-in-months/ on 25/01/22

[10] 2021 July, Shapeshift Decentralizes [Blog Post] Retrieved from https://shapeshift.com/shapeshift-decentralize-airdrop on 25/01/22

ILLEGAL ACTIVITIES ON A PROTOCOL OR APPLICATION

Once a protocol or application is live on mainnet, what it is used for is outside the control of the developers. However, this is still a concern for protocol developers and a risk mitigating approach is often taken. In general, when funds are in custody of the protocol in some way, this concern is of greater bearing. In emerging markets where adoption of crypto can be high, concerns about how developed the regulation is can also create uncertainties.

CONCLUSIONS

Generally, the rate of new legislation being drafted for blockchain products is significantly slower than the rate of innovation in the space. This can create confusion and uncertainty around what is needed to be compliant and the question of where the burden of legal responsibility lies is no different. Of greater concern is when changes to legislation are applied retroactively. Developers and legislators must work together, not to stifle innovation.

FUTURE WORK

This work is very early and preliminary within the scope of understanding the regulatory requirements and burden upon projects utilising ZKPs. At this stage, only the legal questions, concerns and challenges common to multiple teams operating within the ZK space have been identified. Solutions or means to work around these challenges are yet to be presented in an open source manner and would be useful, particularly for smaller teams without ample resources to pay for extensive legal fees to see.

The project began as an initiative imagined by Zero Knowledge Validator. The working group was formed to discuss some of the general challenges around implementing ZK in the blockchain space. Many additional teams have inquired about joining since we started the initiative, but for the project to be taken further, we would need to build up a small team and hire a project leader who has skills and expertise in navigating through regulation relevant for the implementation of ZKPs. In the long term, it would make sense to include members who could make connections with policy makers to help inform regulation around ZKPs in an appropriate way.

Up until now, the ZKValidator has seeded this effort: paying for the legal work and committing employee time to the working group. However, to push this project forward, the project will require significant funding to pay for legal fees and expert advice. This can be generated in part through grants, or through the donations of working group partners.

If you would like to be a funder of this initiative, if you believe you could be project coordinator, or if your organisation may be able to offer in kind support, please reach out to us.