zkSafeZones - Blockchain & Zero-Knowledge for Civilian Protection in War Zones & Automated Legal Compliance

Illya Gerasymchuk

E-mail: contact@illya.sh | Homepage: https://illya.sh | https://zklocus.dev

Abstract

zkSafeZones introduces a pioneering approach to civilian safety in conflict zones through blockchain and zero-knowledge proofs. It extends the zkLocus framework on the Mina blockchain, innovating with an economic model centered around the $ZKL token. This model not only incentivizes the submission of geolocation data and legal evidence but also fosters a self-sustainable, decentralized legal system. By ensuring private, verifiable geolocation sharing, zkSafeZones significantly enhances civilian protection and adherence to international law. This comprehensive system integrates advanced technology for humanitarian aid, legal enforcement, and AI governance, marking a paradigm shift towards scalable, global solutions. With real-world applications aimed for integration with entities like the UN and the Red Cross, zkSafeZones aspires for widespread adoption, leveraging technology for enhanced civilian safety, legal compliance, and the creation of a decentralized ecosystem.

Keywords: zkLocus | Civilian Protection | Conflict Zones | Blockchain | Zero-Knowledge Proofs | Legal Enforcement | Mina Protocol | Geolocation | Privacy | zkSNARKs | recursive zkSNARKs

Introduction

zkSafeZones: Harnessing Technology for Humanitarian Protection in Modern Warfare

In the ever-evolving landscape of modern warfare, the protection of civilians remains a paramount yet challenging goal. The advent of sophisticated technologies offers new avenues to safeguard human lives, especially in conflict zones. This whitepaper introduces zkSafeZones - an initiative at the intersection of blockchain technology, zero-knowledge proofs, and international humanitarian efforts.

zkSafeZones leverages the power of the Mina blockchain and the zkLocus framework to create a secure, private, and transparent system for reporting civilian geolocations in areas affeceted by military conflicts. This initiative not only aims to reduce the risk of civilian casualties but also ensures compliance and transparency in adherence to international law.

As a part of our effort to intoroduce technology-enforced and abiding international law, and a system for the protection of civilians in military conflict zones, we have contacted the United Nations (UN) and the International Committee of the Red Cross (ICRC) with a proposal to implement zkSafeZones as a solution for civilian protection in conflict zones. We are currently awaiting a response from the UN and the ICRC, and will update this whitepaper with their response as soon as we receive it. As such, this whitepaper does not merely present a conceptual solution, but a practical proposal that is already in development.

This whitepaper outlines the vision, technology, and implementation of zkSafeZones, demonstrating its potential to revolutionize the landscape of law-abiding technology, reduction of civilian casualties in conflicts, as well as assisting directing and distributing humanitarian aid. It also explores the future development and scalability of zkSafeZones, envisioning its evolution as a versatile and effective tool for ensuring safety, compliance, and transparency in various domains.

The Foundations: zkLocus and Mina Blockchain

At the heart of zkSafeZones lies zkLocus - an application, framework and protocol designed for private, authenticated & programmable geolocation sharing, both off, and on-chain. Utilizing a protocol of cryptographic techniques, zkLocus enables individuals to attest to their presence in an arbitrary geographical area without necessarily disclosing their exact coordinates in a fully authenticated manner. zkLocus is architected using recursive zkSNARKs, and can be used offline, online, off-blockchain, on-blockchain and cross-chain.

zkLocus can be installed direclty from the Node Package Mananger (npm), and runs on any device that runs JavaScript. There is no strict requirement to support the JavaScript runtime, as the involved Zero-Knowledge proofs are recurisve zkSNARKs, which can be verified in a variety of computational environments. This includes smartphones, IoT devices, and web browsers. This enables zkLocus to offer a unique value proposition of being fully compatible with legacy systems, Web 2.0, Web 3.0 and in their intersection.

Complementing zkLocus is the Mina blockchain, renowned for its succinctness, scalability and decentralization. Akin to zkLocus, Mina's approach to verifiable computation model is based on recursive zkSNARKs, which allows the representation of the blockchain to remain constant-sized, regardless of the number of transactions. This enables every user to submit transactions to the netowork and have the security of a full node without the need to store the entire blockchain.

Moreover, the associated cryptographic computations do not require any specialized hardware, and can be performed on ubiquitous devices such as smartphones, IoT and personal computers. The lightweight nature of the Mina blockchain ensures that zkSafeZones can be used, accessed and verified by individuals and organizations worldwide, regardless of their technical and economical resources.

The synergy between zkLocus and the Mina blockchain makes zkSafeZones a solution which alignings technological innovation with the urgent need to protect civilians in military conflict zones. As we delve deeper into the intricacies of zkSafeZones, we will explore how this technology stands to revolutionize the approach to civilian safety in modern warfare while upholding the principles of international law. zkSafeZones is the first proposal of its kind, and is a practical testament to the use of blockchain technology and zero-knowledge proofs for humanitarian purposes.

The Promise of zkSafeZones in Conflict Resolution, Humanitarian Aid & Enforcement of The Law

zkSafeZones emerges not only as a technological innovation but also as a beacon of hope in the realm of conflict resolution, humanitarian aid and automated law enforcement. By enabling accurate and private geolocation reporting in warfare zones, it presents a unique solution to one of the most pressing challenges in modern conflict scenarios - the protection of civilian lives.

Bridging Technology with Humanitarian Needs

The application of zkSafeZones in conflict zones pioneers at demonstrating the potential of blockchain and zero-knowledge proofs in advancing humanitarian objectives. By enabling secure and anonymous reporting of civilian locations, zkSafeZones aims to significantly mitigate the risk of civilian casualties. Additionally, zkSafeZones can provide legal evidence of military organizations disregarding or intentionally targeting civilians, if such incidents occur. This produced legal evidence can demonstrate both, lawful and unlawful actions, as well as be used to automate the enforcement of the law. These features are achieved through the use of zero-knowledge proofs, which allow for the verification of civilian presence in a specific area without disclosing their exact coordinates. This analysis can be performed individually, in a cohort, or a mixture of both.

To achive its goals, zkSafeZones combines the verifiable computational model offered by recursive zkSNARKs, with the authenticated, integirty-assured, destributed, programmable and succint state transition and data storage model offered by the Mina blockchain. This combination allows zkSafeZones to leverage the strongest points of each technology, while mitigating their respective weaknesses, thus enabling its unique value proposition. The result is a secure, private, and transparent system for geolocation reporting in conflict zones, aligning with international law and humanitarian needs. It enables individuals in high-risk areas to share their authenticated geolocation without compromising their security, safety and privacy, while maintaining full transparency and enabling compliance enforcement.

A New Era of Compliance with International Law

zkSafeZones pioneers a protocol and framework for the automated, distributed, permissionless, transparent and decentralized enforcement of the law. This whitepaper forcuses on the international law, particularly in conflict zones, however its applications extend to all legal domains.

By harnessing the security properties of the blockchain with the privacy-preserving and verifiable computation capabilities of zero-knowledge proofs, it creates a robust platform for legal compliance and transparency. This system not only empowers civilians in conflict zones but also provides international bodies with reliable, verifiable data to monitor and enforce legal standards in real-time.

Automating Law Enforcement Through zkSafeZones, the potential for automated enforcement of international laws becomes tangible. The system's ability to provide authenticated evidence of civilian presence in conflict areas paves the way for automatic legal responses to violations. By integrating smart contract technology, zkSafeZones can trigger predefined legal actions upon the verification of specific conditions, such as unauthorized military activities in civilian-dense areas.

Enhancing Transparency and Accountability zkSafeZones enables a new realm of transparency in conflict zones. By creating and storing a tamper-proof record of civilian locations and military activity, it ensures that all parties are held accountable for their actions. This level of transparency is pivotal for international legal bodies and humanitarian organizations in decision-making, policy formation, and in taking swift action to protect civilians.

Collaborative Legal Frameworks The implementation of zkSafeZones encourages collaboration between technology, developers, enthusiasts, legal experts, and international bodies. It facilitates the creation of a new legal framework where technology and law intersect, ensuring that humanitarian principles are upheld in the digital age. By involving entities like the UN and ICRC, zkSafeZones ensures that its development and application align with international standards and ethical practices.

zkSafeZones enables anyone and everyone to participate in the enforcement of the law and the protection of civilians in conflict zones. The system is designed with programmable value incentives via the $ZKL token, which can be used as a reward for desirable actions. Examples of desirable actions include the submission of a zkLocus geolocation proof for another individual, and submission of a proof of violation of international law, such as a proof of military activity in a civilian-dense area. The latter can be used to automate the enforcement of the law, by triggering a smart contract which automatically enforces a predefined legal action, such as locking a preditermined amount of collateral for further review.

The implementation proposed in this whietpaper, extends zkLocus, by enabling the attachment of a “bounty” for the submission of its geolocation proofs on-chain. This “bounty” is a value reward attributed to the submitter of the proof onto the Mina blockchain. The “bounty” can be claimed by anyone who submits the proof to the Mina blockchain.

This creates a permissionless, transparent and decentralized system for the enforcement of the law, where anyone can participate in the enforcement of the law, and anyone can claim the “bounty” for submitting a proof. This system is designed to be self-sustainable, and self-enforcing, as the “bounty” is funded by the $ZKL token, which is a programmable value token, which can be used to reward desirable actions, such as the submission of a proof of violation of international law, or the submission of a proof for another individual/entity or group of individuals/entities in a conflict zone.

In summary, zkSafeZones represents a disruptive advancement in the enforcement of international law in conflict zones. Its innovative use of blockchain and zero-knowledge proofs offers an unprecedented level of compliance, transparency, privacy, and legal automation, marking a pivotal shift in how technology can be used for humanitarian protection and legal enforcement on a global scale.d

Existing Solutions and the Innovations of zk-SafeZones

Ensuring the safety of civilians in military conflict areas, and enforcing the adeherence to international law are key challenges in the realm of humanitarianism, geopolitics and international relations. This section explores the existing solutions, and outlines the innovative approach and features provided by zk-SafeZones, demonstrating its potential to revolutionize the landscape of civilian protection and law enforcement in conflict zones.

Existing approaches have involved collaborative international efforts, legal and moral frameworks, and technological innovations. These strategies range from nation-to-nation cooperation and military training to the integration of emerging technologies like AI and blockchain.

While effective in some aspects, current solutions often lack in providing real-time, privacy-centric, economically viable and participatory mechanisms for civilians in conflict zones. This is where zkSafeZones innovatively provides its value. It uniquely combines blockchain technology with zero-knowledge proofs, creating a system that is not only secure and private but also decentralized and transparent. zkSafeZones allows civilians to actively participate in their safety by verifiably and privately reporting their geolocation, or deferring that to antoher party - features which are not present in existing solutions. Additionally, the use of smart contracts for legal compliance in zkSafeZones offers automated, guaranteed, and data-driven enforcement of international laws, distinguishing it from traditional governance methods. Its global accessibility and scalability further set it apart, making it a versatile and effective tool for various environments and regions, including those with limited technological infrastructure, or the absence of internet connectivity.

Therefore, zkSafeZones stands as a novel solution, addressing the limitations of existing approaches and offering an innovative, self-sustainable, and programmable system for civilian protection and law enforcement in conflict zones. The following sections provide an overview of the current approaches and the unique features of zkSafeZones.

Overview of Current Approaches

In the realm of conflict zones, various strategies and technologies have been employed to minimize civilian casualties and enforce international law. These include collaborations among nations, integration of AI and blockchain technologies, and adherence to legal and moral obligations in military operations.

Collaborative Efforts and Training Programs

The U.S. government collaborates with allies and partner nations to minimize civilian casualties during military operations. This involves integrating civilian protection into arms transfers and foreign military sales. The focus is on training partners and providing advisory support with an emphasis on mitigating civilian harm. This initiative includes expanding the scope of what partners can offer, from new curriculum for civilian harm mitigation training to the development of advisory materials and services, and technical solutions to help partners conduct operations more effectively and responsibly. Source: (U.S. Department of Defense, 2020)

Legal and Moral Obligations

A strong commitment to minimizing civilian casualties and adhering to international humanitarian law principles is enculturated and internalized at all levels of the U.S. military command. This includes educational training for commanders in the moral and legal obligations to mitigate civilian harm. Source: (U.S. Department of Defense, 2020)

Use Of Emerging Technologies

There are several technological solutions that have been concepted to mitigate civilian harm in conflict zones. These include:

- **Artificial Intelligence (AI)**: AI can be used to mitigate harm to civilians by identifying specific problems leading to civilian harm. For instance, AI applications can alert the presence of transient civilians, detect changes from collateral damage estimates, and alert potential miscorrelations in military operations. AI can also recognize protected symbols, such as the red cross or red crescent, and alert operators or the chain of command.
- **Blockchain Technology**: Blockchain is used in systems like the Human Security Information System (HSIS), developed by USAID, to improve the knowledge of the civilian environment in military operations. This system provides a secure means to report and update civilian information, thereby strengthening the mitigation of civilian harm (CNA, n.d.).

zkSafeZones: A New Paradigm In Civilian Protection and Legal Enforcement

While the existing solutions and proposals have made contributions to reducing civilian casualties in conflict areas, and enhancing the adeherence and enforcement to the law, zkSafeZones presents a disruptive, first of its kind, paradigm, by providing a basis for a fully automated, programmable, permissionless, transparent, decentralized and self-sustainable system for the enforcement of the law, and the protection of civilians in conflict zones.

The approach proposed here is unique and differs from existing solutions in several key ways:

1. **Technology Integration**: zkSafeZones integrates blockchain technology with zero-knowledge proofs, a combination not widely used in current military or humanitarian operations. This integration provides a new level of security, privacy, and transparency.

2. **Privacy and Security with Zero-Knowledge Proofs**: Unlike traditional methods, zkSafeZones uses zero-knowledge proofs to enable individuals to verify their location without revealing exact coordinates. This ensures privacy and security, which is not a primary feature of the technologies like AI and blockchain currently used in existing solutions.

3. **Decentralized and Immutable Record Keeping**: The Mina blockchain's use in zkSafeZones offers a decentralized and immutable record of civilian locations, enhancing transparency and accountability in ways that traditional systems and current emerging technologies do not focus on.

This blockchain application is distinct from the current use of blockchain in the HSIS system, which primarily focuses on improving knowledge of the civilian environment. zkLocus and its developments as a part of zkSafeZones can also be direcly integrated into the HSIS system, to enhance its capabilities and use-cases.

4. **Enhanced Civilian Protection in Conflict Zones**: zkSafeZones is specifically designed to minimize civilian casualties in conflict zones by providing accurate geolocation data. While existing solutions like the U.S. military's efforts and AI applications focus on minimizing harm, they do not offer a dedicated system for civilians to actively participate in their safety through technology, nor the ability to automate the enforcement of international & humanitarian law.

5. **Automated Enforcement of International Law**: zkSafeZones' use of smart contracts for legal compliance is a novel approach. It allows for the automated enforcement of laws, such as the international law, based on verifiable data, a feature not present in current systems, where legal enforcement relies more on traditional governance and less on automated, data-driven processes.

6. **Global Accessibility and Scalability**: The public, permissionless, decentralized, succint and lightweight nature of the Mina blockchain ensures global accessibility and scalability of zkSafeZones. This feature is crucial for widespread adoption and effectiveness, especially in regions with limited technological infrastructure, which is a challenge for some of the existing technologies that require more robust infrastructure.

7. **Flexibility and Offline Capability**: zkSafeZones operates seamlessly online and offline, on and off the blockchain, across Web 2.0 and legacy systems, thanks to its recursive zkSNARKs architecture. This enables infinite proof compression and roll-up, allowing civilians in areas with no internet access to generate and share geolocation proofs via bluetooth or mesh networks. Once connectivity is available, these proofs can be batch submitted to the blockchain, incentivized by $ZKL token bounties.

8. **Bounty-Driven Proof Submission**: zkSafeZones introduces a unique value incentive model where entities can associate a bounty, in the form of $ZKL tokens, with a geolocation proof for submission on-chain. This model enables one entity to generate a proof with zkLocus and incentivize another entity to submit it to the blockchain, thereby fostering a collaborative ecosystem for data sharing and verification.

9. **Self-Sustainable Legal System**: The platform establishes a self-enforceable legal system, leveraging $ZKL tokens and smart contracts on the Mina blockchain. This system incentivizes third-party participation in law enforcement, such as international law, creating a decentralized framework for legal compliance and civilian protection.

10. **Economic Incentive Model for Civilian Protection and Legal Enforcement**: zkSafeZones's economic model, powered by $ZKL tokens, facilitates the financing of both civilian protection and law enforcement. Organizations like the UN or Red Cross, as well as individuals, can set up funds to incentivize the submission of civilian geolocation proofs in conflict zones. This system ensures that even individuals without internet access can incentivize others to submit proofs on their behalf, enhancing the reach and effectiveness of civilian protection efforts.

In summary, zkSafeZones's disruptive approach, characterized by its unique technology integration, privacy protection, decentralized architecture, and innovative economic incentives, enables a new paradigm for civilian safety in conflict zones and lawful enforcement. This novel platform, protocol and framework not only addresses the limitations of current solutions but also introduces a robust, scalable, and incentivized system for global adoption.

Problem Statement and Background

Addressing the Complexities of Modern Warfare and Civilian Safety

In the landscape of modern warfare, the safety of civilians and the enforcement of international law present profound challenges. Conflicts increasingly unfold in urban settings, heightening the risk of civilian casualties. The intricacy of these environments, where distinguishing between combatants and non-combatants is often challenging, compounds the issue, making ethical and effective decision-making by military forces more complex.

Modern Warfare's Urban Shift

The trend towards urbanized warfare places civilians at greater risk than ever before. Populated areas become theatres of conflict, leading to unintended casualties and humanitarian crises. This shift necessitates innovative solutions that can adapt to the unique demands of urban conflict zones, ensuring civilian safety while maintaining military effectiveness.

International Law and Civilian Protection

The role of international law is pivotal in safeguarding civilians. Laws of armed conflict emphasize sparing non-combatants from harm. However, enforcing these laws is hampered by the lack of real-time, verifiable data on civilian presence, creating a gap between legal standards and their practical application.

Existing Solutions and Their Limitations

Current methods for protecting civilians, while diverse and multi-faceted, often fall short. These include international collaborations, technological innovations, and adherence to legal and moral frameworks in military operations. Yet, they frequently lack the ability to provide real-time, participatory, and privacy-centric solutions for civilians in conflict zones.

AI-Powered Warfare and Legal Enforcement

As technology advances, so does the nature of warfare. The emergence of AI-powered warfare presents new challenges and complexities. AI-driven systems are increasingly being integrated into military operations, offering capabilities such as autonomous decision-making, predictive analytics, and enhanced precision. While a lot of progress has been done on AI-powered weapons, little has been done in enforcing the law in these systems, and providing a legally-binding way demonstrate compliance or non-compliance with the law in these systems.

The autonomy of AI-powered technology, especially the one that is deployed in drones and other unmanned vehicles, requires a reliable, timestamped, and verifiable data source on civilian presence. This is where zkSafeZones and its extensions to the functionality of zkLocus offer a unique value proposition. Designed for easy integration into drones and AI systems, the proposal described in this whitepaper, enables for a secure and private geolocation system that can supply accurate and verifiable data on-demand. This system can be used online, offline, on the blockchain, off the blockchain, and in any combination of these. This is made possible by the recursive zkSNARKs architecture, which enables a portable and flexible verifiable computation model, whose usage is feasable in a variety of computational environments, including smartphones, IoT devices, and web browsers.

In the context of contemporary, automated and AI-powered warfare, accurate and verifiable geolocation data is crucial for avoiding civilian casualties, by allowing to distinguish between combatants and non-combatants, and accouting for the principle of proportionality in International Humanitarian Law (IHL). The use of zkSafeZones and its extensions to zkLocus, can provide a reliable, verifiable and secure data source for AI-powered systems, enabling them to operate within the bounds of international law, and avoid civilian casualties.

The principle of proportionality prohibits attacks against military objectives, which are "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated." Besides the aforementioned use-cases, the framework proposed in this whitepaper provides cryptographcially & legally-binding means to demonstrate compliance or non-compliance with the principle of proportionality, by providing a secure, private, verifiable and immutable data source for civilian presence in conflict zones. This data source can be used to demonstrate compliance or non-compliance with the principle of proportionality, by providing a timestamped and verifiable record of civilian presence in conflict zones. The combination of this data, the data of actions taken by military forces in these zones, and smart contracts can be used to automate the enforcement of the law, by triggering a smart contract which automatically enforces a predefined legal action, such as locking a preditermined amount of collateral for further review.

Therefore, the rise of AI-powered warfare underscores the need for solutions like zkLocus and zkSafeZones. By providing a public, decentralized geolocation sharing system, they can ensure that AI systems operate within the bounds of international law, protecting civilian lives in the process.

Overcoming Connectivity Challenges A key feature of zkSafeZones is its ability to function both online and offline, crucial in conflict zones where internet access is unreliable. Civilians can share their geolocation proofs, even in the absence of active internet connections, using technologies like Bluetooth in a mesh-style network.

Unique Features of zkSafeZones

1. **Decentralized Mempools**: Facilitating private geolocation sharing, allowing any party to become a mempool to roll-up proofs and submit them collectively.
2. **Smart Contract-Based Reporting**: Enabling real-time tracking of entity locations, crucial for transparency and accountability.
3. **Programmable Incentives**: Utilizing $ZKL tokens to incentivize the submission of geolocation proofs, fostering a self-sustaining ecosystem for data sharing.

Evolving zkLocus for zkSafeZones

zkSafeZones extends zkLocus to create a public geolocation system tailored for conflict zones. This extension includes features like offline chains for data submission, smart contract integration for tracking entity locations, and mechanisms for adding or blacklisting entities.

A Self-Sustainable Legal System zkSafeZones proposes a self-sustainable and enforceable legal system, using $ZKL tokens to incentivize third-party participation in law enforcement. This decentralized approach enables a new form of transparent and participatory legal compliance.

Broader Impact and Applications Beyond military conflict zones, zkSafeZones's technology can be applied in various domains, including commercial applications like drone regulation, delivery verification, and creating logs of entity trustworthiness.

The Vision of zkSafeZones

zkSafeZones addresses these challenges in practice, by providing an implementation that leverages the Mina blockchain and the zkLocus framework. Its goal is to establish a public, decentralized geolocation system for entities to report their locations for compliance and transparency in international law.

Conclusion

In summary, zkSafeZones represents a significant leap forward in addressing the challenges of civilian safety in conflict zones. Its innovative use of blockchain and zero-knowledge proofs, coupled with its flexible, decentralized, and incentivized framework, positions it as a powerful tool for revolutionizing civilian protection and legal enforcement in the modern, urbanized landscape of warfare.

Legal Snapshot

Legal Purpose and IHL Principles Protection

zkSafeZones, utilizing zkLocus technology, is fundamentally aligned with the principles of International Humanitarian Law, aimed at enhancing the protection of civilians during armed conflicts. The technology supports the Principle of Distinction, a keystone of IHL, by providing accurate geolocation data for the purpose of differentiating between military targets and civilian areas. This capability is critical in minimizing civilian casualties and damages to civilian properties. Furthermore, zkSafeZones contributes significantly to the Principles of Proportionality and Necessity. By offering precise, verifiable location data, it aids in the assessment and planning of military operations, ensuring they are necessary, target only legitimate military objectives, and do not result in disproportionate harm to civilians. Additionally, zkSafeZones embodies the Principle of Humanity. By its nature, it promotes human dignity and alleviates human suffering by reducing the risk of harm to civilian populations in conflict zones.

Implementation in IHL and Increased Adherence

The implementation of zkSafeZones within the framework of IHL could potentially lead to greater adherence to these principles by involved countries and armed groups. The system's ability to provide secure, private, and transparent reporting of civilian geolocations offers a mechanism for monitoring and enforcing compliance with IHL. This technology can serve as a tool for international organizations and states to ensure that actions in conflict zones adhere to the legal standards set by IHL. The transparency and accountability facilitated by zkSafeZones can act as a deterrent to violations of IHL, as the technology makes it more challenging for parties in a conflict to deny targeting civilian areas or to claim ignorance about the location of such areas.

Legal Advantages Over Current Solutions

Compared to existing solutions, zkSafeZones offers several legal advantages. Its use of zero- knowledge proofs ensures the privacy and security of the data, crucial in conflict zones where information can be exploited for military gain. This aspect of zkSafeZones is particularly valuable in upholding the principles of IHL while ensuring that the technology itself does not become a tool in the conflict. The precision and reliability of the data provided by zkSafeZones also mean that decisions made based on this information are more likely to be in compliance with IHL, reducing the risk of legal repercussions for wrongful attacks on civilian populations.

In the context of zkSafeZone's compliance with international data protection standards, particularly those set by the United Nations and the Red Cross, our approach is centered around a framework that respects and incorporates these global principles. This compliance is achieved through a multi-faceted strategy that ensures the protection of personal data in humanitarian actions, aligning with the highest standards of data security and privacy. At the center of zkSafeZone's compliance with international humanitarian data protection standards is our adherence to the principles outlined in the "Handbook on Data Protection in Humanitarian Action" published by the International Committee of the Red Cross (ICRC). This handbook provides guidelines tailored to data protection in humanitarian scenarios, emphasizing on the safeguarding of individual's personal data as an integral part of protecting their lives, integrity, and dignity. Our technology and operational protocols are designed to ensure the integrity, confidentiality, and availability of personal data, in line with the ICRC's emphasis on protecting individual's rights, freedoms, and dignity. Moreover, zkSafeZones integrates the ICRC Rules on Personal Data Protection into its core operations. These rules, cater to the evolving landscape of data protection, accounting for new technologies and the interconnected nature of data processing in today's world. The ICRC's rules are specifically tailored to address the challenges of managing personal data in challenging environments, a main aspect of zkSafeZone's operations in conflict and disaster zones. In practice, zkSafeZones achieves compliance through the following measures:

- Data Protection by Design and Default: From the inception of our technology, data protection is ingrained in the design. We ensure that personal data is processed with the utmost security and only used for its intended humanitarian purposes.
- Regular Compliance Monitoring and Assessment: zkSafeZones will undergo regular assessments to ensure that our data processing activities align with international standards. This includes adapting to new developments in data protection laws and guidelines set by bodies like the UN and the Red Cross.
- Expert Consultation: We will engage regularly with data protection authorities and experts, especially those specializing in humanitarian data protection. This ensures that our practices are in line with the latest standards and recommendations in the field.
- Staff Training and Awareness: Our team will receive continuous training on the specific requirements of data protection in humanitarian contexts. This ensures that all members are aware of and adhere to the guidelines and principles set by international organizations like the UN and the Red Cross.

It is imperative to acknowledge the importance of conducting a Data Protection Impact Assessment (DPIA). Given the nature of zkSafeZones operations, which involve the processing of sensitive geolocation data, a DPIA becomes not just a compliance requirement but also a fundamental aspect of our commitment to data protection. The necessity for a DPIA in our operations is primarily due to the potential high risk to the rights and freedoms of individuals inherent in geolocation data processing. This type of data is sensitive and, if misused or inadequately protected, can lead to significant privacy intrusions. The DPIA will allow us to systematically evaluate these risks and implement measures to mitigate them effectively. It will also ensure that zkSafeZones adheres to the principles of data protection by design and by default, as mandated by GDPR.Conducting a DPIA aligns with our commitment to uphold the highest standards of data privacy and security. It demonstrates to our stakeholders, including users, regulators, and partners, that we are proactive in identifying and addressing any privacy risks associated with our data processing activities. This not only enhances our compliance profile but also reinforces trust in our technology and practices.

zkLocus Framework

Transforming Geolocation with Privacy and Authentication

zkLocus stands as a transformative framework in the realm of geolocation services. It addresses critical privacy and data integrity issues in geolocation sharing through its innovative use of recursive zkSNARKs. This section delves into the architecture, features, and functionalities of zkLocus, demonstrating its pivotal role in enhancing geolocation privacy and verification in the digital age.

Core Principles of zkLocus

zkLocus introduces a novel paradigm in geolocation services, enabling authenticated, private, and programmable geolocation both off and on-chain. This is accomplished through the innovative use of recursive zkSNARKs, a form of cryptographic proofs that allow a user to authenticate their presence within a specific geographical area without disclosing exact coordinates. The privacy and data authenticity offered by zkLocus is a significant step forward in resolving the dual challenge of privacy and trust in digital geolocation.

Key Features of zkLocus

1. **On-Chain Geolocation**: zkLocus brings geolocation data onto the blockchain, ensuring authenticity and integrity while preserving user privacy.
2. **Native Bridging Capabilities**: It enables verifiable and private geolocation on-chain without relying on external oracles or bridges.
3. **Cross-Chain Functionality**: Designed with flexibility, zkLocus is compatible with multiple blockchain ecosystems, including Ethereum and Cardano.
4. **Privacy Preservation**: Users can share their location or validate the location of others without exposing their exact coordinates.
5. **Programmable Geolocation**: zkLocus proofs on the blockchain can be programmed with arbitrary logic, introducing the concept of programmable geolocation.

The Role of Recursive zkSNARKs

zkLocus leverages recursive zkSNARKs to maintain user privacy and data authenticity. These cryptographic proofs enable the verification of a user's presence within a specific area while preserving the confidentiality of their exact location. This approach is particularly beneficial in applications requiring both data integrity and privacy, such as supply chain management, DeFi, and legal compliance.

Broad Applications and Impact

zkLocus, with its distinct features and robust protocol, has wide-ranging implications across various domains. Its ability to provide secure, private, and verifiable geolocation data opens up new possibilities in several industries, transforming how geolocation information is utilized and authenticated in the digital world.

In summary, zkLocus stands as a beacon of innovation in geolocation services, offering a comprehensive solution to the challenges of privacy invasion and data integrity. By leveraging recursive zkSNARKs, zkLocus ensures user privacy and data authenticity, providing a secure, private, and verifiable method of geolocation sharing. Its impact extends across various domains, demonstrating its potential to revolutionize geolocation privacy and verification.

Mina Blockchain Integration

Leveraging the Power of the World's Lightest Blockchain

The integration of zkSafeZones with the Mina blockchain represents a significant advancement in utilizing blockchain technology for humanitarian purposes. Mina's unique architecture and capabilities make it an ideal platform for implementing the zkSafeZones initiative.

Distinct Features of Mina Blockchain

1. **Succinct Blockchain**: Mina is renowned for its constant-sized blockchain, regardless of transaction volume. This succinctness is achieved through the use of recursive zkSNARKs, similar to zkLocus, making the blockchain incredibly lightweight and accessible.
2. **Full Node Accessibility**: Every user on the Mina network can act as a full node with minimal hardware requirements. This democratizes access to the blockchain, ensuring a high degree of decentralization and security.
3. **Efficient Verification**: Due to its succinct nature, the Mina blockchain allows for rapid verification of transactions and data, crucial for the timely reporting and verification of geolocation data in conflict zones.

Role in zkSafeZones

The Mina blockchain's integration into the zkSafeZones framework enhances the system's capabilities in several key areas:

- **Decentralized Data Storage**: Mina's blockchain serves as a secure and immutable repository for storing geolocation data, ensuring transparency and tamper-proof record-keeping.
- **Rapid Verification**: Quick and efficient verification of geolocation proofs is vital in conflict zones. Mina's architecture enables fast and reliable verification processes, a critical factor in the timely protection of civilians.
- **Global Accessibility**: The lightweight nature of the Mina blockchain ensures that zkSafeZones can be accessed and verified by individuals and organizations worldwide, regardless of their technical resources.

In summary, the Mina blockchain's integration with zkSafeZones is a strategic choice that leverages its unique features of succinctness, accessibility, and efficient verification. This integration is pivotal in realizing the vision of zkSafeZones to provide a secure, private, and transparent system for geolocation reporting in conflict zones, aligning with international law and humanitarian needs.

zkSafeZones: Extending zkLocus

Innovating for Enhanced Civilian Protection in Conflict Zones

zkSafeZones represents a significant extension of the zkLocus framework, tailored specifically for use in conflict zones. This section explores the new features and functionalities that zkSafeZones introduces to zkLocus, enhancing its application for the safety of civilians in war-torn areas.

New Functionalities in zkSafeZones

1. **Offline Geolocation Proof Submission**: Recognizing the challenges of internet connectivity in conflict zones, zkSafeZones introduces an innovative feature for offline geolocation proof submission. This ensures continuous and uninterrupted reporting of civilian locations, even in the absence of an active internet connection.
2. **Decentralized Mempools**: To address the scalability and efficiency of geolocation data submission, zkSafeZones incorporates decentralized mempools. These allow for the aggregation of multiple proofs before they are batched and submitted to the blockchain, reducing transaction costs and network congestion.
3. **Incentivization with $ZKL Token**: zkSafeZones introduces an incentivization model using the $ZKL token. This model rewards entities for submitting geolocation proofs, encouraging active participation and timely data provision.

Enhancing Modular Design for Future Scalability

Each of these new features is designed as an independent module that can be integrated into the zkLocus framework. This modular approach ensures that zkSafeZones is not only a solution for immediate humanitarian needs but also a scalable and adaptable system for future applications.

Integration with Existing zkLocus Capabilities

zkSafeZones builds upon the existing capabilities of zkLocus, such as private and authenticated geolocation sharing, and enhances them with its unique features. This integration ensures that zkSafeZones retains the core strengths of zkLocus while expanding its functionality to meet the specific needs of conflict zone applications.

In summary, zkSafeZones extends the zkLocus framework with critical features for conflict zone applications, focusing on offline functionality, decentralized data processing, and incentivization. These enhancements position zkSafeZones as a potent tool for protecting civilians in conflict zones, showcasing the potential of blockchain and zero-knowledge proof technologies in humanitarian applications.

Technology and Implementation

Integrating Advanced Technologies for Real-time Civilian Safety

zkSafeZones is not just a conceptual framework but a practical solution, leveraging advanced technologies for real-time implementation. This section outlines the technological backbone of zkSafeZones and its implementation process.

Technical Architecture of zkSafeZones

- **Combining Zero-Knowledge Proofs with Blockchain**: zkSafeZones utilizes zero-knowledge proofs for privacy-preserving geolocation reporting, integrated with the Mina blockchain for decentralized data storage and verification.
- **Offline Data Collection and Submission**: Leveraging advanced cryptographic techniques, zkSafeZones enables the collection and submission of geolocation data even in offline scenarios, ensuring continuous civilian protection.
- **Decentralized Data Aggregation**: The system employs decentralized mempools for efficient data aggregation and submission, optimizing network resources and reducing transaction costs.

Implementation Process

- **Integration with Existing Systems**: zkSafeZones is designed for seamless integration with existing infrastructures, including both blockchain-based and traditional systems, ensuring broad applicability and ease of adoption.
- **Security Measures**: Robust security protocols are in place to protect data integrity and privacy, ensuring the system's resilience against potential threats and vulnerabilities.
- **User Accessibility**: Special attention is given to making zkSafeZones accessible and user-friendly, considering the diverse range of users, from civilians in conflict zones to international monitoring bodies.

Privacy and Security Considerations

Inherent in zkSafeZones' design is a strong emphasis on privacy and security. The use of zero-knowledge proofs ensures that while geolocation data is verifiable, the privacy of individuals is strictly maintained. Additionally, the blockchain's immutable nature guarantees that once submitted, the data cannot be altered, providing a reliable source of truth for monitoring and compliance purposes.

In conclusion, the technology and implementation of zkSafeZones represent a synergistic combination of blockchain and cryptographic technologies, tailored to meet the pressing needs of civilian safety in conflict zones. This innovative approach not only enhances the effectiveness of humanitarian efforts but also sets a new standard for the application of technology in upholding international law and human rights.

Architecture and Design

zkSafeZones is implemented by both, extending the functionality of zkLocus, and using that functionality to achieve its goals. The goals of zkSafeZones can be summarized as follows:

1. Provide a ready-to-use application, framework and protocol to be used for the purpuses of minimizing civilian casualties, protecting civilians and infrastructure in conflict zones, and enforcing the law in these zones.

2. Provide the first implementation of legal digital evidence regarding geolocation of digital assets, such an entity or an object, with arbitrary metadata, such as the timestamp. An example use-case is to prove the presence or the absece of an individual in a specific area, at a specific time interval. The evidence contains a cryptogprahic proof of the verifiable computaional model based on Zero-Knowledge pririmitives and recursive zkSNARKs.

Such an evidence, or proof is authenticated, integrity-assured and transparent by design, and can be used in a the “traditional” court of law in existing legal systems across the world, in the digital realm of the law that is currently being pioneered by its first applications like zkSafeZones is doing, or in any other legal context.

3. Enable the creation of a self-sustainable, programmable, permissionless, transparent, decentralized and automated legal digital evidence sharing and a legal system for the enforcement of the law in the digital realm, by leveraging the aforementioned features of the Mina blockchain, and its architecture based on recursive zkSNARKs, which natively integrates with zkLocus, and its extensions as a part of zkSafeZones.

4. Enable programmable value incentives for the submission of zkLocus proofs on-chain, by allowing each proof to have a “bounty” associated with its submission. This “bounty” is a value reward attributed to the submitter of the proof onto the Mina blockchain. The “bounty” can be claimed by anyone who submits the proof to the Mina blockchain. The “bounty” is funded by the $ZKL token, which is the native token of the zkLocus framework, and its extensions as a part of zkSafeZones. A “bounty” can be attached to the proof even in an off-chain, offline scenario.

5. Create a Decentralized Finance (DeFi) ecosystem on the Mina blockchain for zkLocus and its extensions as a part of zkSafeZones. At core of this DeFi ecosystem is the $ZKL token, which is a programmable value token that can be used to reward desirable actions. Examples of desirable actions include:

   - Submission of a timestamped proof for another verified individual/entity or group of individuals/entities in a military conflict zone. This can be used to provide a cryptographically verifiable proof of civilian presence in a conflict zone, which can be used to minimize civilian casualties in these zones, by enabling the distinction between combatants and non-combatants, and by enabling the enforcement of the principle of proportionality in International Humanitarian Law (IHL).
   - Fully-private geolocation sharing on the Mina blockchain, which enables any digital entity to have their proof submitted by another entity, in exchange for a certain amount of $ZKL token. This enables the sharing of one’s location without exposing their geolocation, IP address, Mina account address, or any other personally identifiable information (PII). The work presented in this whitepaper will enable such functionality for any zkLocus proof. In the context of civilian protection, this can be used to enable the sharing of one’s location in a conflict zone, without exposing any information regarding their digital footprint, such as IP address and mobile device type, while having their identity fully attested.

- Collective funding of geolocation proof submissions for individuals and affected areas. This is enabled by the support for external funding of proof submissions, which is embedded into the architecture of smart contracts developed as a part of this proposal. Such a feat allows for humanitarian organizations, like the UN, or the Red Cross, to fund the submission of geolocation proofs for individuals in conflict zones, or for areas affected by natural disasters, such as earthquakes, floods, etc. The same is true for any other entity, such as a government, or a private organization, or an individual, who wishes to fund the submission of geolocation proofs for affected individuals, collectives of individuals or areas. This enables everyone and anyone to collectively participate in the protection of civilians in conflict zones, evidence gathering, and the automated enforcement of the law in the digital realm.
- Collective gathering of select legal evidence. The collective funding model described above enables for a programmable legal evidence gathering system, where a value incentive is provided in exchange for a desired piece of legal evidence. Examples of such evidence include proofs of civilian presence in a specific area, at a specific time interval.

6. Dynamic addition and blacklisting of verified entities.

Implementation

zkSafeZones is implemented by extending the functionality of zkLocus, and then using that functionality to implement the goals of zkSafeZones. As such, zkSafeZones is a framework, a protocol, and a concrete appplication which achieves the goals mentioned above. The end most basic delivrables of this proposal are:

1. An application, in the form of a fully functional, ready to use, Minimum Valuable Product (MVP), with a user interface, in the form of a web application, all of the required backend components and smart contract functionality. The application will be hosted online and publically accessible.
2. Extensions to the zkLocus, focusing on the integration and functionality of zkLocus on the Mina blockchain. This will include all of the necessary smart contracts and their user-friendly public API abstraction. This will enable anyone to easily create appplications which use any of the individual pieces of functionality and features covered in this whitepaper. This includes the ability to include monetary incentives for the submission of zkLocus proofs on-chain.
3. DeFi ecosystem for zkLocus, which enables a decentralized business model. The $ZKL token, it's use-cases and its tokenomics will enable a self-sustainable business model for zkLocus, fully on the Mina blockchain.

4. Generic, reusable components, zkApp design patterns and protocols to enable the use of features described in this proposal for zkApps. This includes the ability to attach a "bounty" to any O1JS proof that is submitted to the Mina blockchain, the public funding models that can be used in the context of DAOs, etc.

Technical Details

This section covers the technical implementation details of zkSafeZones, and its extensions to zkLocus.

The main architectural components and additions are as follows:

- $ZKL token, implemented through a set of smart contracts on the Mina blockchain.
- Proof-of-storage.
- Monetary incentives for the submission of zkLocus proofs on-chain, in the form of $ZKL token "bounties." These monetary intives can be generated offline, without an active internet connection, and be claimed once they're submitted on-chain. This functionality is implemented through a set of smart contracts which contain the logic for the creation, claiming and programmability of these "bounties."
- Identity association for zkLocus proofs. This extends zkLocus into a new realm, by allowing the association of a digital identity to a zkLocus proof. This identity is independent of the account from which the the proof is submitted. The architecture will be extended to support easy integration with any digitial identity system, including the support for oracle-based authentication. The latter will allow the the system to be easily used with any existing infrastructure, inlcuding legacy.
- Grouping of identities. This will enable the creation of groups of identities, which enables cohort analysis and management of groups of individuals and their geolocations. This is a desirable use-cases not only for zkSafeZones, but for any solution and use-case which requires the management of groups of individuals and their geolocations.
- Programmable funding models for the submission of proofs onto the Mina blockchain. This will provide a set of smart contracts and generic components which can be used to enable the programmability of value incentive models for the submission of proofs onto the Mina blockchain.

Each and every component can be further refined into a generic, independent protocol.

$ZKL Token

The token will be implemented through a set of smart contracts, using a standard for its independent usage. The initial interface will be based on the ERC-20 token standard, but innoviative solutions enabled by the Mina Protocol model will be explored and added as well.

The $ZKL will be designed with principled aimed to maximise its liquidity, by enabling its usage in various environments. This includes derivatives of $ZKL, and even multiple interopable versions of these direvatives. One solution being explored, is a $ZKL derivative that is collateralized by Mina protocol's native cryptocurrency $MINA. This will include a smart contract which can mint $ZKL from $MINA, and burn $ZKL to mint $MINA, thus enabling a fully decentralized, and collateralized liquidity pool for $ZKL. This will enable a a liquidity pool for $ZKL, and enable its seamless integration with $MINA.

The tokens will be implemented the native token functionality that is present on Mina, and the related functionality present in the O1JS framework.

Monetary Incentives For The Submission Of Proofs On-Chain

The functionality to attach the monetary incentives for the submission of any zkLocus proof-on chain will be implemented. This protocol can also be generalized for any other proof to be submitted to Mina. This will be implemented through a combination of Zero-Knowledge Circuits and smart contracts.

On the side of Zero-Knowledge circuits, the ability to "wrap" zkLocus proofs with a value incentive or "bounty" for its submission into a smart contract on-chain will be added. This will be implemented leveraging recursive zkSNARKs, and the cryptographic signatures. More specifically, a set of ZkPrograms/Zero-Knowledge circuits will be created which accepte zkLocus proofs as private input, alongiside the signature authorizing this "bounty," as well as a unique identifier for this bounty, in the form of a None (Field). This unique identifier for each bounty is important to keep a track of which bounty is funded, which one is claimed, and which one is not claimed.

On the smart contract side, all of the necessary code for the creation, verification, and payout for bounties will be implemented. Each bounty is identified by a unique key, in the form of a Field number. A bounty can be funded and claimed. Each bounty can only be claimed once. All of the data related to funded and the claimed bounties is stored off-chain and a merkle root commitment is stored on-chain. It is possible to require a Proof-of-Storage for every bounty funding or claiming action, thus ensuring that the associated data has been saved. The support for the arbitrary integration of Proof-of-Storage mechanisms will be included, but a concrete implementation will be provided as well. This is described below.

In order to fund a bounty with a specific ID, it is necessary to provide the following as an input:

- Merkle Tree Witness
- Bounty ID + additional data
- $ZKL funds for the bounty, which will be locked in the smart contract until the bounty is claimed
- Proof-of-Storage for the bounty funding action

The smart contract will verify the provided data, and update the Merkle Tree Root for the commitment to the association between a Bounty ID and the associated bounty.

To claim a bounty with a specific ID, is to provide a zkLocus proof wrapped with a cryptographic claim on that bounty. That claim is verified, and if its's valid, the bounty has not been claimed, and the proof is qualified for a bounty, and the bounty is attributed to the submitter (claimer) of the proof. As such, a nullifier-based mechanism will be included for the bounty functionality. It's also possible to fix the claimer of the proof in the bounty claim itself, thus transferring the bounty funds not to the claimer, but to that fixed/hardocoded address.

Each smart contract will be intialized with a tree with a pre-determined amount of leaves, thus setting a limit for the maximum number of available bounties for an identity. To mitigate this limitation, self-replication of the bounty smart contracts will be included, thus enabling the creation of a new smart contract once the maximum number of bounties is reached. This will enable an interaction way that is transparent to the user, where they interact with the system as if it was a single smart contract. For this reason, the bounty ID will be the digest (Poseidon hash) of the bounty ID, and the address of the current smart contract. As such, globalBountyID = hash(localBountyID, smart contract addr)

Identity Association For zkLocus Proofs

As a part of the functionality of zkSafeZones pretaining to submission of geolcoation proofs by civilians, it is necessary to embed the concept of digital identity into the zkLocus framework and protoocol. This will be implemented through a set of Zero-Knowledge circuits, which will enable the association of a digital identity to a zkLocus proof. The support for arbitrary digitial identity sources included, allowing any solution to be used with zkLocus. An approach based on utilizing an integration oracle will be inlcuded. We are also considering a digitial identity solution that is a part of another zkCohort 3 proposal.

In terms of technical details, this will be implemented leveraging recursive zkSNARKs, by wrapping/attaching ditital identity data to zkLocus proofs. This will be implemented in a manner similar to which the arbitrary Metadata association functionality that is already present in zkLocus

Grouping Of Identities

The ability to group identities will be implemented. This will enable the creation of groups of identities, which enables cohort analysis and management of groups of individuals and their geolocations. This is a desirable use-cases not only for zkSafeZones, but for any solution and use-case which requires the management of groups of individuals and their geolocations.

This will be implemented by a set of smart contracts, that will allow for the submisison and managemenet of geolocation data for a group of identities, and the following associated functionality:

- Authorization/whitelisting of entities which can submit geolocation proofs. It will be possible to authorize only a subset of entities to submit geolocation proofs to a smart contract. In the context of zkSafeZones, this means verifying the identity of civilians, and allowing only verified civilians to submit their geolocation proofs. This functionality is fully dynamic, and this set can be updated at any time. A commitment to the set of authorized entities will be stored on-chain in the form of a merkle tree root. It's possible to require a Proof-Of-Storage.
- Blacklisting of entities. It will be possible to blacklist entities, including currently authorized entities, thus preventing them from submitting geolocation proofs. This functionality is fully dynamic, and this set can be updated at any time. A commitment to the set of blacklisted entities will be stored on-chain in the form of a merkle tree root. It's possible to require a Proof-Of-Storage.
- Decentralized addition of entities, without a centralized entity. The architecture outlined here also allows for the creation of the ablity to whiteliset new entities by having a certain amount/percentage of authorized entity to "vouch" for a new entity. The transparent and traceable nature of all actions, allows to easily identify collusions chains of bad actors and take down large chains at once, in a transparent manner

Programmable Funding Models For The Submission Of Proofs Onto The Mina Blockchain

Besides the ability to include monteray incentives for the submission of proofs on-chain, it's also possible to program those incentives. With this it's possible to create monetary incentives only for proofs meeting certain criteria, such as geolocation proofs recorded at a certain time interval, or in a certain geographical area. This can be used to incentivise the gathering of legal evidence, such as the presence of civilians in a specific area, at a specific time interval.

This will be implemented through a set of logic in the smart contracts with generic logic. For example, to require proofs in a certain geographical area, the public output of zkLocus proofs can be exracted in the smart contracts, and asserted to be equal to the desired geographical area.

Proof-Of-Storage

In order to ensure that all of the data comitted to the Merkle Trees on-chain is actually stored, it's possible to require a Proof-Of-Storage for every action that updates the Merkle Tree Root. The implemented architecture will support arbitrary sources of storage proofs, thus allowing for easy integration with any verifiable off-chain storage model. While there are existing solutions in the Mina ecosystem, they are not actively maintained, and it would intorduce a big risk for this proposal. For this reason, we will provide the means to easily integrate with any existing solution, and provide a concrete implementation as well. The concrete implementation will support the the proof of storage from arbitrary integraiton oracles.

This functionality will be implemented by enabling the attachment/wrapping of zkLocus proofs with the proof of storage, using a mechanism similar to the attachment of arbitrary metadata. The associated smart contracts will verify those proofs before accepting the merkle tree updates.

Zones Compression and Database-Free Design

zkSafeZones is designed to operate in extreme environments, where network connectivty and computational resources are scarce. For this reason, it important to minimize the amount of data that is necessary to process and send over network. A part of this is already addressed by the architecture of zkLocus, which enables for infinite compression, by leveraging its architecture based on recursive ZK-SNARKs. However, in the most dynamic implementation of zkSafeZones, it's necessary to communicate the geolocation data associated with each geolcoation proof. At the very minimum, this would be two 64-bit numbers, representing either the coordinates or the polygon. Given the range of all possible values, the requirement for storing this data in a dedicated storage system is necessary.

Based on our research and during the process of integration of zkLocus with third-parties, a design based on storage-free solution, or its compressed form is a strong value-proposition. In the context of confict zones, some of the regions are extremely limited in their network coverage, which makes it either fully inacessebile or extremely slow. Given the importance of submission of geolocation data on chain being as fast as possible, a solution that does not require a dedicated storage system expands its aplicability to the most extreme environments.

Moreover, during our integration of zkLocus with Decentralised.trade (https://decentralised.trade), the need for a limited set of pre-defined geolocation areas was expressed. These areas are specific geographical areas of interest, such as ones deliniating the borders of a specific facilty.

Given the reduced amount of data associatd with these proofs in their current state, and the possiblity for its furhter compression, we do not consider this to be a limitation, neither a practical one, nor a theoretical one. In this section, we will describe the mechanism by which zkSafeZones can operate without the requirement for off-chain storage.

Despite that, based on the potential application environments that we identified during our research, as well as the practical business needs, in this section, we will devise a solution that enables zkSafeZones and zkLocus geolocation proofs to be used without the need for a dedicated storage system, thus not requiring off-chain storage for geolocation data, and limiting the blockchain storage to just a few bytes.

Removing The Need For Storage

zkSafeZones can be used to submtion geolocation proofs for arbitrary geolocation areas. However, in several practical applications it is sufficient to to limit the set of possible geolocation areas to a few pre-defined areas. In the case of application of zkSafeZones in conflict zones, these areas of interest bould be the borders of specific facilities, such as hospitals, schools, and other areas with civilian infrastructure. In the case of business applications for decentralized trade, these areas could represent warehouses, or other areas of delivery of goods.

This represents an opportunity for greatly compressing the amount of geolocation data that has to be stored, including reducing the need for storing any data at all. This is achieved by defining a set of geolocation areas, and then assigning an ID to each one of these areas. This ID can be an integer, as small as 1 bit. In this process, the set of possible geolocation areas of zones is reduced to a small number, thus we call this process "Zones Compression."

Zones Compression in zkSafeZones

It's possible to remove the need for geolocation data storage in zkSafeZones and zkLocus by limiting the set of possible geolocation areas to a few pre-defined areas. Each area is assigned a unique integer value, which is used to identify the area. The geolocation proofs are then submitted with the ID of the area, instead of the actual geolocation data. Once this proof is submitted, the smart contracts updates the merkle root, which now includes an additional leaf, in form of `digital identity: geolocation area ID`. Given that the list of authorized identities is known, and it's possible to identify the identity for whom the proof is being submitted, the `geolocation area ID` can only be a value from a small set of possible values. This makes it possible to brute-force the entire set of possible values, and thus to identify the actual geolocation area. In this way, the need for storing the geolocation data during proof submission is removed, and the blockchain storage is limited to just a few bytes.

For example, if the set of possible geolocation areas to report is limited to 5, then for each geolocation data point, it's only needed to attempt 5 values at most. Such a reduced computation complexity is manageable even in resource-constrained devices.

Ensuring A Manageable Complexity With A DeFi Business Model

In order to ensure that at any point the amount of data to bruteforce is manageable, it's possible to associate monetary value incentives for the update of the data represented by the merkle tree root on-chain. In practice, this entails allowing any entity to identiy bruteforce the numeric ID of the geolocation data commited to on-chain, and then claim a $ZKL bounty for the update of geolocation data to the data availability layer.

This is akin to how the Proof-of-Work (PoW) mechanism in Bitcoin works, where the miners are incentivised to update the blockchain with the new block, by the reward of the newly minted Bitcoin. In the case of Bitcoin, the bruteorcing operation is used to demonstrate Proof-of-Work, while in zkSafeZones and zkLocus it's used to demonstrate the correctness of updated geolocation. Such an approach enables a fully self-sustainable, and decentralized system, which uses economic incentives and cooperation for its operation.

Such an architectural approach, voids the need for storing the geolocation data off-chain before submitting that data on-chain, while including a fully decentralized and self-sustainable business model. This is a strong value proposition for the most extreme environments, such as conflict zones, where the network connectivity is limited, and the computational resources are scarce, as well as adaptable to specific solutions.

Use Cases and Applications

Broadening the Horizon: Diverse Applications of zkSafeZones

zkSafeZones, with its innovative blend of blockchain and cryptographic technologies, has applications that extend beyond the primary goal of civilian safety in conflict zones. This section explores various scenarios where zkSafeZones can be effectively utilized.

Humanitarian Aid and Conflict Resolution

- **Civilian Protection**: In war zones, zkSafeZones can be a lifeline for civilians, providing a secure method to report their locations, thereby facilitating targeted aid and reducing collateral damage during military operations.

Legal Compliance and Transparency

- **International Law Enforcement**: By creating transparent and immutable records of civilian locations, zkSafeZones aids international organizations in monitoring and enforcing compliance with humanitarian laws.

Commercial and Civilian Applications

- **Delivery Verification**: In logistics, zkSafeZones can automate and authenticate delivery processes, ensuring goods reach their intended destinations while maintaining privacy and data integrity.
- **Legal Proof for Drone Operations**: Civilian drone operators can use zkSafeZones to prove compliance with no-fly zone regulations, enhancing privacy and legal compliance.

Future Potential

- **Integration in Military Equipment**: As a defensive measure, countries could integrate zkSafeZones to demonstrate compliance with international laws, proving that military actions did not occur in civilian-dense areas.
- **Smart Contract Enforcement**: In a broader legal context, zkSafeZones could facilitate the creation of smart contracts that automatically enforce international agreements based on verified geolocation data.

In conclusion, the use cases and applications of zkSafeZones are vast and varied, demonstrating its versatility as a tool for not just conflict zones but also for legal, commercial, and civilian uses. The technology paves the way for new possibilities in ensuring safety, compliance, and transparency in a range of scenarios.

Future Development and Scalability

Envisioning the Evolution of zkSafeZones

As a dynamic and forward-looking initiative, zkSafeZones is not only focused on immediate applications but also on its future potential and scalability. This section outlines the roadmap for zkSafeZones' development, highlighting its adaptability and potential for widespread application.

Planned Enhancements

- **Generalization of Features**: Future versions of zkSafeZones will focus on generalizing its unique features, such as offline geolocation proof submission and decentralized mempools, for broader applications beyond conflict zones.
- **Cross-Chain Compatibility**: Efforts will be made to enhance zkSafeZones' compatibility with various blockchain platforms, increasing its versatility and potential for integration into diverse ecosystems.

Scalability and Adaptability

- **Modular Design**: The modular architecture of zkSafeZones ensures that it can be easily scaled and adapted to various needs, from small-scale deployments in specific areas to large-scale implementations across different sectors.
- **Community Involvement and Open Source Development**: Leveraging the power of open source development and community involvement, zkSafeZones aims to continuously evolve, integrating new ideas and technologies as they emerge.

Potential Integration with Other Technologies

- **Integration with IoT and AI**: The potential integration of zkSafeZones with IoT devices and AI technologies could offer advanced solutions for real-time monitoring and decision-making in various scenarios, from urban planning to environmental monitoring.

In summary, the future development and scalability of zkSafeZones are grounded in its flexible, modular design and commitment to continuous improvement and adaptation. Its evolution will be marked by broader applications, cross-chain compatibility, and integration with emerging technologies, solidifying its role as a versatile and effective tool for ensuring safety, compliance, and transparency across various domains.

Conclusion

Charting a New Path in Humanitarian Technology

zkSafeZones represents a groundbreaking fusion of blockchain technology and zero-knowledge proofs, charting a new path in the use of technology for humanitarian purposes. This initiative not only showcases the potential of these technologies in conflict zones but also sets a precedent for their broader application in various sectors.

Reinforcing Humanitarian Efforts

- **Empowering Civilians**: zkSafeZones empowers civilians in conflict zones by giving them a secure and private platform to report their locations, thereby contributing to their safety and protection.
- **Aiding Compliance with International Law**: The initiative aids in enforcing compliance with international law, providing transparent and immutable records of civilian locations in conflict zones.

A Vision for the Future

- **Expanding Applications**: The potential applications of zkSafeZones extend beyond conflict zones, encompassing legal, commercial, and civilian uses, demonstrating its versatility as a tool for ensuring safety, compliance, and transparency.
- **Open Collaboration**: The future development of zkSafeZones will be marked by open collaboration and continuous innovation, adapting to emerging technologies and evolving needs.

In closing, zkSafeZones stands as a testament to the power of combining advanced technologies for the greater good. It not only addresses the immediate challenge of civilian protection in conflict zones but also opens the door to a future where technology plays a central role in upholding human rights and international law.

References and Appendices

Note for the reader: This sections is a work-in-progress (WIP). All of the referrences can be found within the text of the whitepaper, in the form of hyperlinks. The appendices will be added in the future.

Documenting the Foundations and Further Reading

To provide a comprehensive understanding and to support further research, this section includes references and appendices related to zkSafeZones and its underlying technologies.

References

- A curated list of academic papers, technical documents, and other relevant materials that have been referenced throughout this whitepaper.
- Legal texts and international law documents pertinent to the application of zkSafeZones in conflict zones.

Appendices

- Appendices will be added here

Note For The Reader

This whitepaper is a work-in-progress (WIP). Contributions are welcomed. Contact: contact@zklocus.dev | Homepage: https://zklocus.dev/ | Twitter/X: https://x.com/zkLocus