WHITEPAPER

ZKTsunami

11:11PM

Abstract

Zcash was the first to implement and apply ZK-SNARK in the decentralized cryptocurrency, include a section explaining what is zk snarkbut the trusted setup step of ZK SNARK presents a security risk. The relatively costly proof generation further reduces the likelihood of its being adopted in practice.

ZKTsunami implements and integrates the state-of-the-art setup-free zero-knowledge proof protocol to enable trustless anonymous payment for smart contract platforms. Our proposed ZK-AnonSNARK scheme also attains the optimal balance between performance and security, i.e., almost constant proof size and efficient proof generation and verification. This will anonymize any cryptocurrency including Bitcoin and Ethereum.

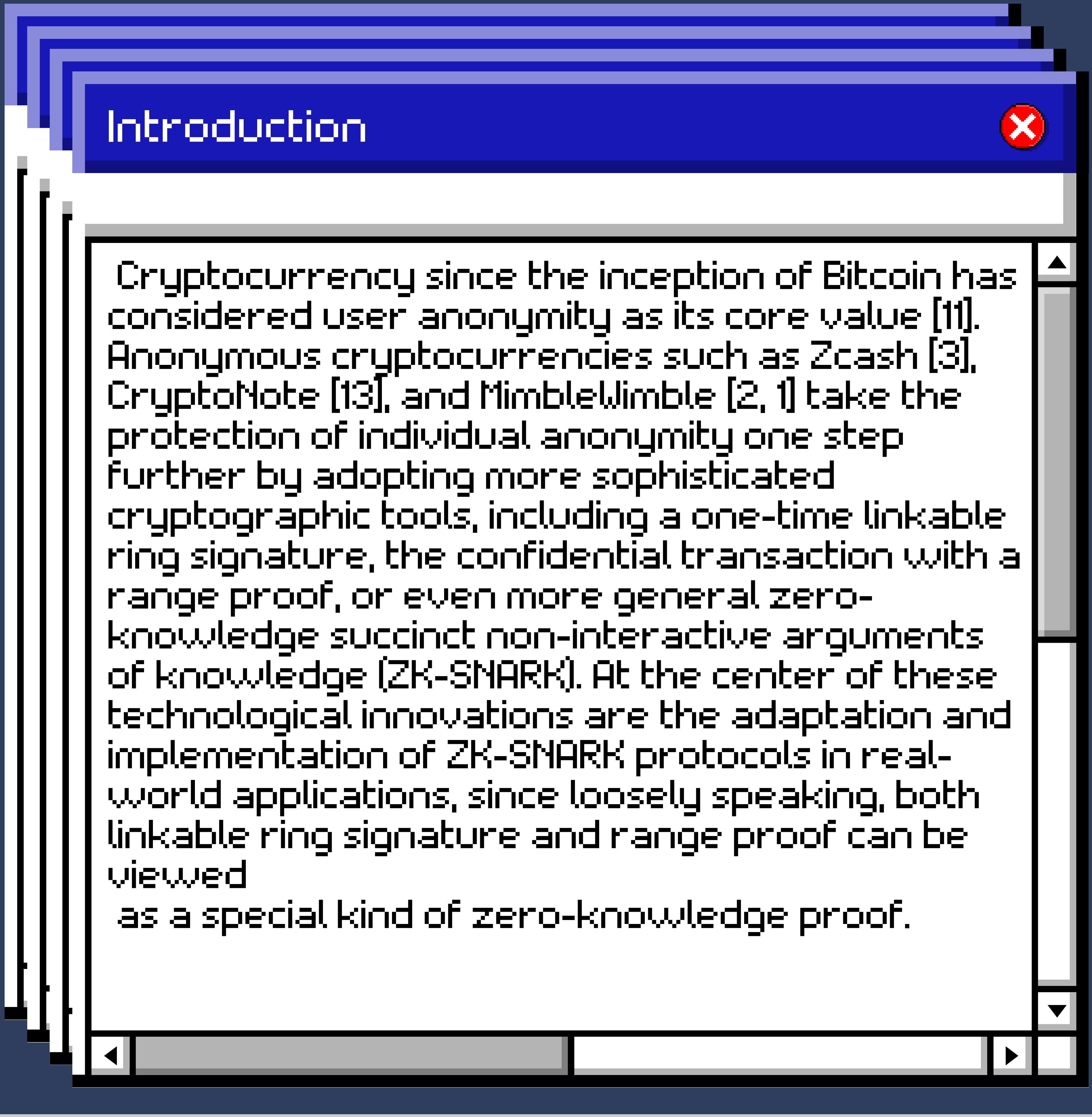
ZKTsunami

Start

ZKTsunami: Hide Beneath the Waves

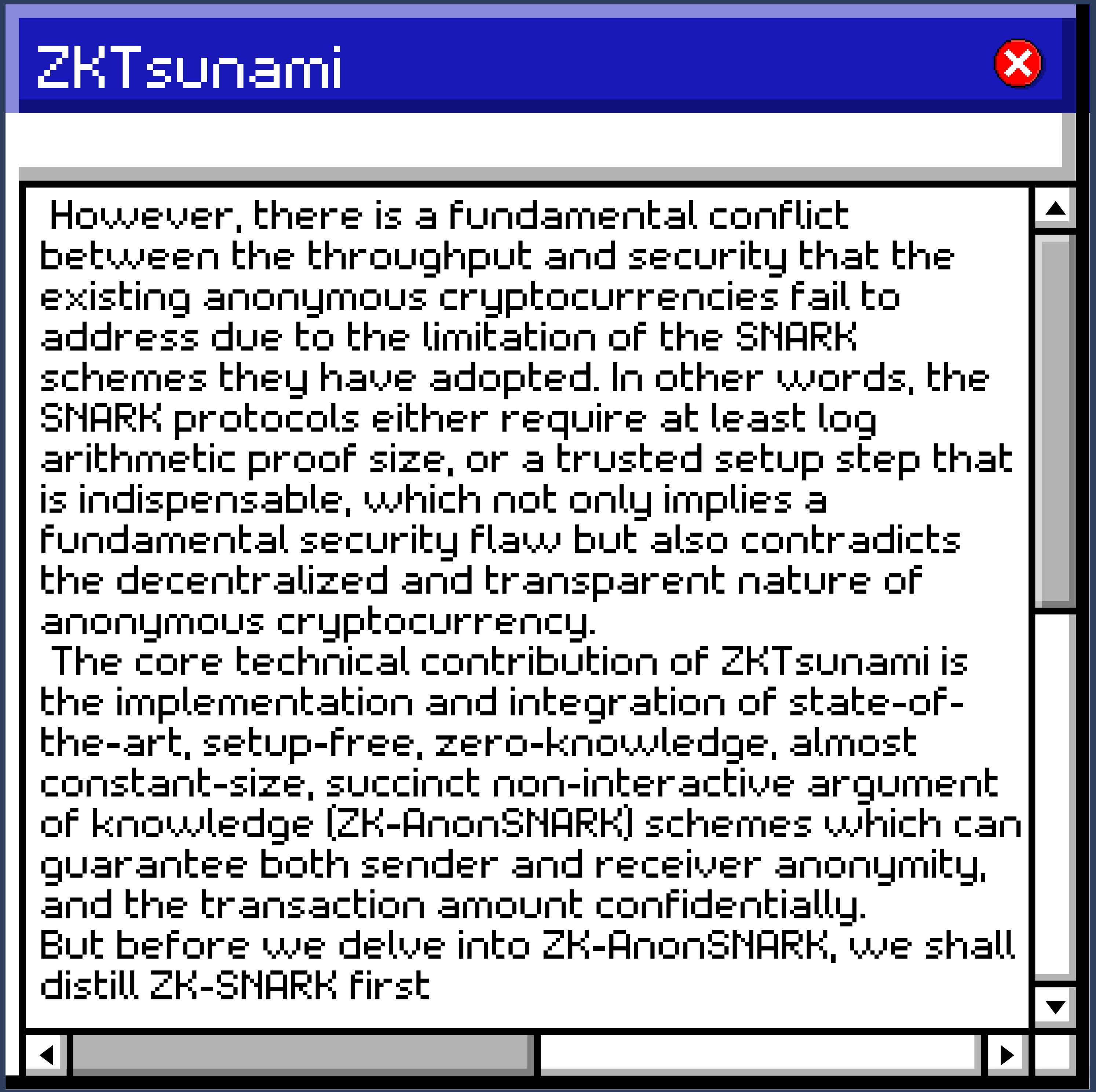
Introduction

ZKTsunami



Introduction

Cryptocurrency since the inception of Bitcoin has considered user anonymity as its core value [11]. Anonymous cryptocurrencies such as Zcash [3], CryptoNote [13], and MimbleWimble [2, 1] take the protection of individual anonymity one step further by adopting more sophisticated cryptographic tools, including a one-time linkable ring signature, the confidential transaction with a range proof, or even more general zero-knowledge succinct non-interactive arguments of knowledge (ZK-SNARK). At the center of these technological innovations are the adaptation and implementation of ZK-SNARK protocols in real-world applications, since loosely speaking, both linkable ring signature and range proof can be viewed as a special kind of zero-knowledge proof.



ZKTsunami

However, there is a fundamental conflict between the throughput and security that the existing anonymous cryptocurrencies fail to address due to the limitation of the SNARK schemes they have adopted. In other words, the SNARK protocols either require at least log arithmetic proof size, or a trusted setup step that is indispensable, which not only implies a fundamental security flaw but also contradicts the decentralized and transparent nature of anonymous cryptocurrency.

The core technical contribution of ZKTsunami is the implementation and integration of state-of-the-art, setup-free, zero-knowledge, almost constant-size, succinct non-interactive argument of knowledge (ZK-AnonSNARK) schemes which can guarantee both sender and receiver anonymity, and the transaction amount confidentially.

But before we delve into ZK-AnonSNARK, we shall distill ZK-SNARK first

Start

ZKTsunami

Benefits of ZK Snarks

One of the main benefits of ZK Snarks is their ability to provide privacy in transactions. Both parties must reveal their identities to complete a transaction in traditional transactions.

However, with ZK Snarks, both parties can remain anonymous while still completing the transaction. ZK Snarks can also be used to ensure that a computation was performed correctly without revealing any of the inputs or outputs of the computation.

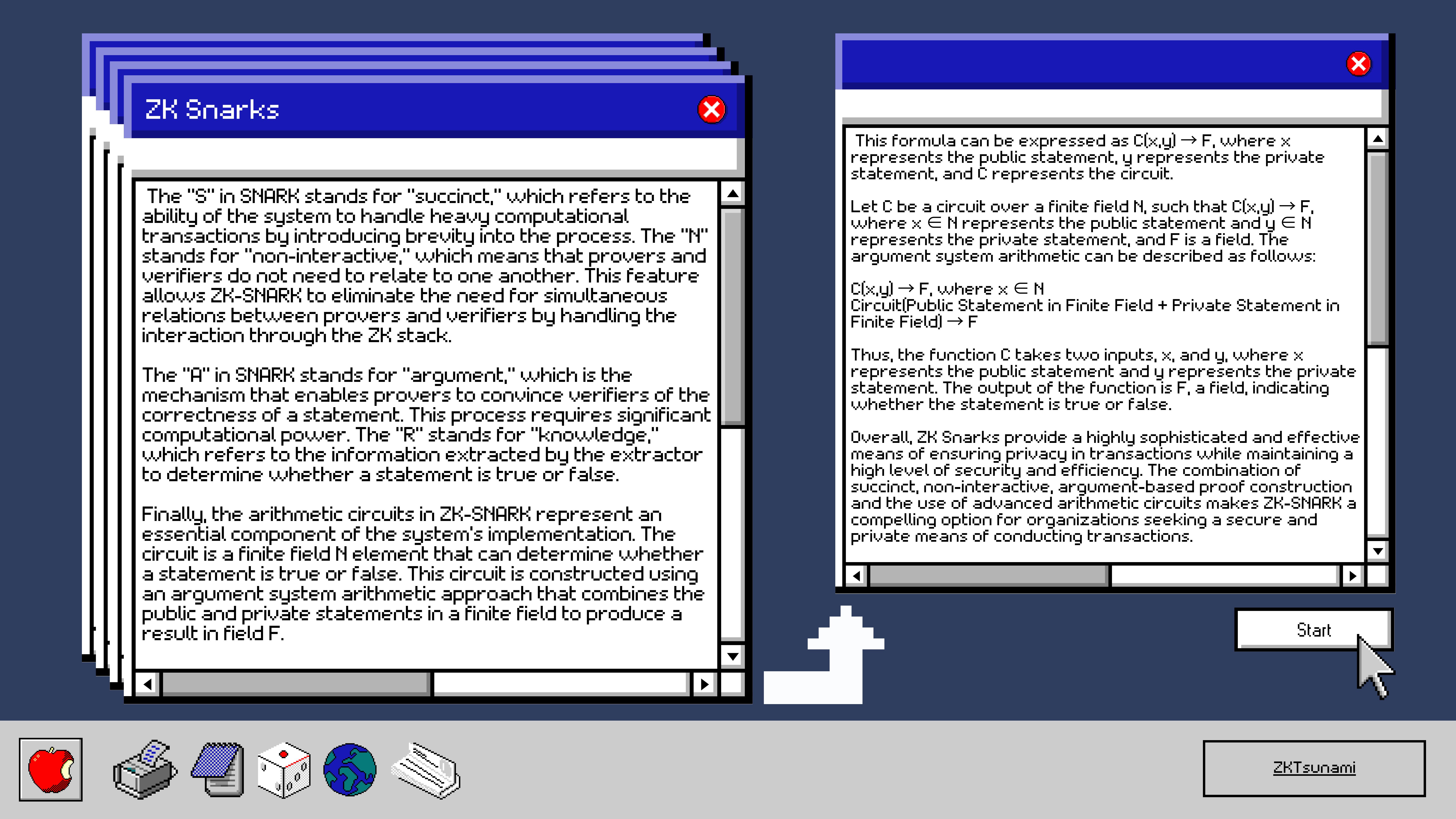
This technology is versatile and can be used in various applications such as cryptocurrencies, voting systems, and identity verification systems.

ZK Snarks Explained

ZK Snarks represent a sophisticated type of zero-knowledge proof system that enables the creation of concise and efficient proofs that third parties can easily verify. Essentially, ZK Snarks take a complex computation and transform it into proof that can be quickly and securely verified by a third party. This process provides a high degree of privacy for transactions, allowing both parties to maintain anonymity while completing their transactions.

While there are different methods for implementing ZK, SNARK (Succinct Non-Interactive Argument of Knowledge) is one of the most advanced techniques. What makes ZK-SNARK unique is its ability to provide a succinct, non-interactive, and argument-based approach to proof construction.

Start



ZK Snarks

The "S" in SNARK stands for "succinct," which refers to the ability of the system to handle heavy computational transactions by introducing brevity into the process. The "N" stands for "non-interactive," which means that provers and verifiers do not need to relate to one another. This feature allows ZK-SNARK to eliminate the need for simultaneous relations between provers and verifiers by handling the interaction through the ZK stack.

The "A" in SNARK stands for "argument," which is the mechanism that enables provers to convince verifiers of the correctness of a statement. This process requires significant computational power. The "R" stands for "knowledge," which refers to the information extracted by the extractor to determine whether a statement is true or false.

Finally, the arithmetic circuits in ZK-SNARK represent an essential component of the system's implementation. The circuit is a finite field N element that can determine whether a statement is true or false. This circuit is constructed using an argument system arithmetic approach that combines the public and private statements in a finite field to produce a result in field F.

This formula can be expressed as $C(x,y) \rightarrow F$, where x represents the public statement, y represents the private statement, and C represents the circuit.

Let C be a circuit over a finite field N, such that $C(x,y) \rightarrow F$, where $x \in N$ represents the public statement and $y \in N$ represents the private statement, and F is a field. The argument system arithmetic can be described as follows:

$C(x,y) \rightarrow F$, where $x \in N$
Circuit(Public Statement in Finite Field + Private Statement in Finite Field) → F

Thus, the function C takes two inputs, x, and y, where x represents the public statement and y represents the private statement. The output of the function is F, a field, indicating whether the statement is true or false.

Overall, ZK Snarks provide a highly sophisticated and effective means of ensuring privacy in transactions while maintaining a high level of security and efficiency. The combination of succinct, non-interactive, argument-based proof construction and the use of advanced arithmetic circuits makes ZK-SNARK a compelling option for organizations seeking a secure and private means of conducting transactions.

ZK Snarks in Identity Verification Systems

1

ZK Snarks can be used in identity verification systems to verify the identity of a user without requiring the user to reveal their personal information. This technology can help protect user privacy while ensuring the integrity of the verification process. With ZK Snarks, users can prove their identity without revealing sensitive information.

For example, the uPort platform uses ZK Snarks to verify user identities on the Ethereum blockchain, ensuring that personal information is kept private while providing a high level of security and accuracy in identity verification.

ZK Snarks in Cryptocurrencies

2

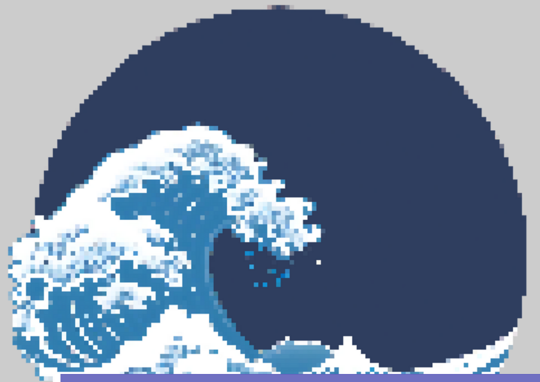
ZK Snarks can be used in cryptocurrencies to provide transaction privacy without sacrificing network security. This technology can be used to conceal the sender and receiver's identity while ensuring the transaction's integrity.

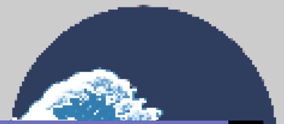
For example, the cryptocurrency Zcash uses ZK Snarks to enable anonymous transactions, allowing users to send and receive funds without revealing their identities or transaction details to others on the network. This approach provides a high level of privacy for users while still maintaining the integrity and security of the transaction system.

ZK Snarks in Voting Systems

3

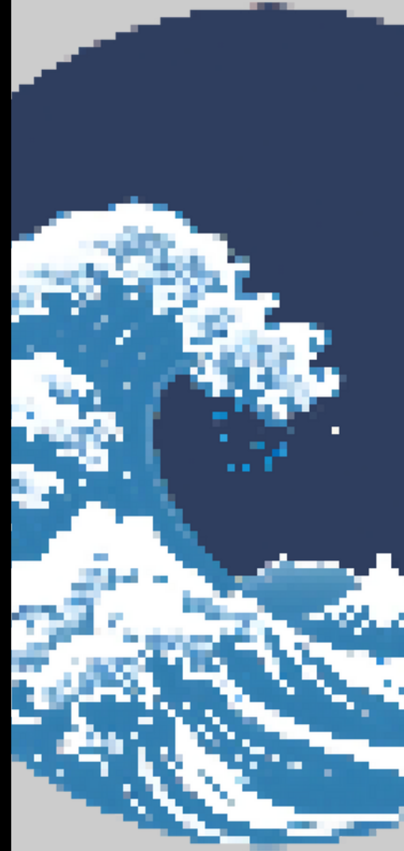
Voting systems can also benefit from ZK Snarks. ZK Snarks can be used to ensure that a vote was counted correctly without revealing the voter's identity. This technology can help prevent voter fraud and ensure the integrity of the voting system. With ZK Snarks, voters can vote anonymously without fear of revealing their identity.



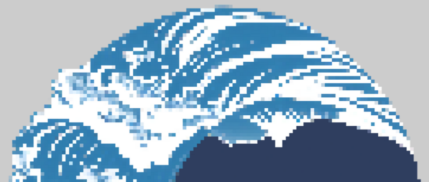


Limitations

1. Trusted Setup: ZK Snarks require a trusted setup, which can be a security concern. During the setup, a set of parameters are generated to generate the proofs.
If these parameters are compromised, the system's security can also be compromised. While there are methods to mitigate this risk, such as multi-party computation, the trusted setup remains a potential vulnerability.
2. High Computational Requirements: ZK Snarks require significant computational power to generate the proofs, making them expensive and slow to use. This computational requirement makes it challenging to use ZK Snarks in real-time applications and can limit their scalability.



ZKTsunami



Setup-free ZK-AnonSNARK

1

The maximum throughput of a blockchain protocol is mainly determined by the maximum block size and average transaction size, which is further determined by the size of SNARK when it comes to a privacy-preserving blockchain protocol. There are mainly two types of ZK-SNARK schemes:

– Zcash has a constant SNARK size but requires a trusted setup step, the compromise of which will allow the attacker to print infinite amounts of Zcash out of thin air without the possibility of being detected [12, 4].

– Setup-free cryptocurrencies such as Monero, Grin, and Beam do not scale well due to their asymptotically larger SNARK size. Their proof size remains logarithmic even after adopting the very elegant Bulletproof technique [6].

ZK-AnonSNARK Schemes

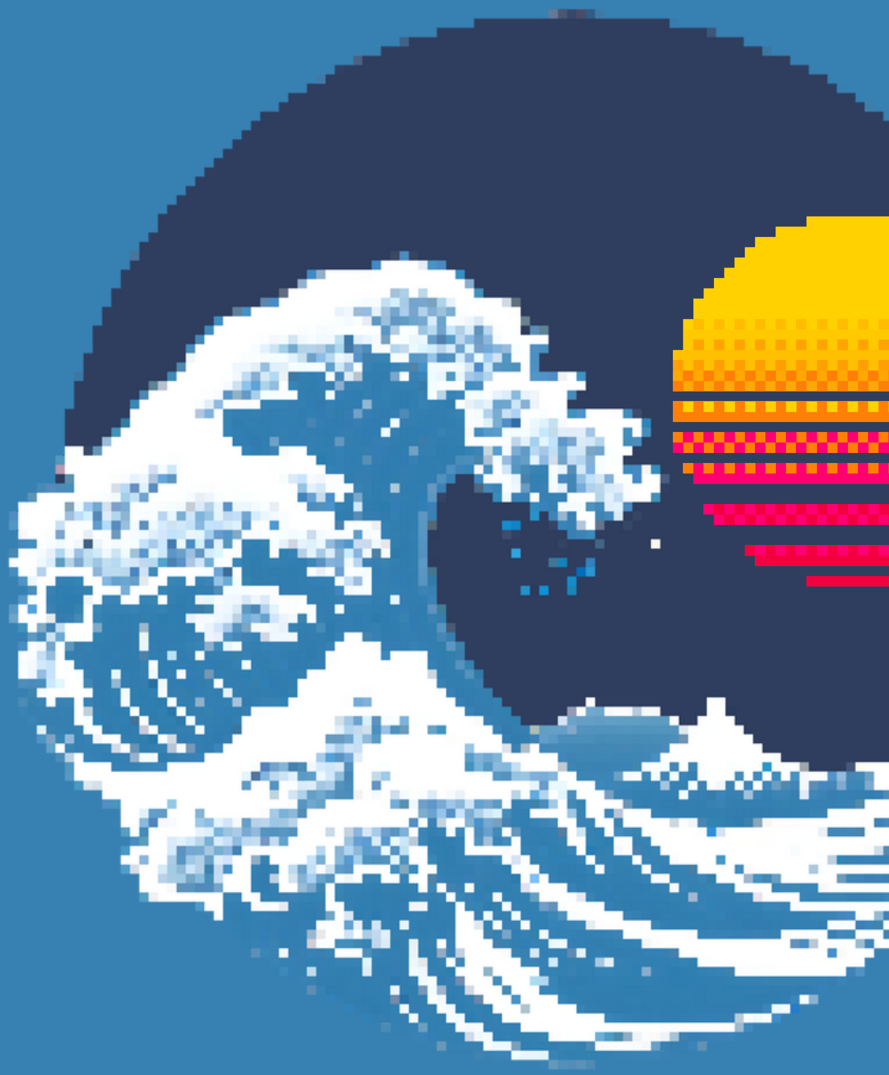
ZK-AnonSNARK schemes realize the setup-free almost constant-size SNARK for the first time. It has the advantages of both categories with none of their downsides. We can literally "eat the cake and have it". Under the discrete logarithm assumption, our recent work [7] obtains the most compact and efficient range proof among all existing candidates (with or without a trusted setup). Our proofs are 12% to 20% shorter than the state-of-the-art Bulletproof [6] for standard choices of range size and security parameter and are more efficient (both for the prover and the verifier) by more than an order of magnitude.

2

Start

Comparison of different types of SNARK schemes :

ZK-SNARK (Zcash,SERO)	TRUSTED SETUP ☒	CONSTANT SIZE PROOF ✓
Bulletproof (MimbleWimble,Beam,Grin)	SETUP FREE ✓	LOGARITHMIC SIZE PROOF ☒
ZK-AnonSNARK ZKTsunami	SETUP FREE ✓	(ALMOST) CONSTANT SIZE PROOF ✓



ZKTsunami

How ZkTsunami Is Better Than Other Competitors

ZK-AnonSNARK

ZkTsunami is a revolutionary anonymous crypto protocol that is disrupting the market by exhibiting a significant increase in trading volume. This surge in demand is attributed to the protocol's ability to provide better anonymity than its competitors. This technical whitepaper aims to investigate and compare ZkTsunami against other anonymous crypto protocols, such as ZCash, Dash, Grin, and Beam, using research, facts, and results.

Start

ZCash

ZCash, a pioneer in anonymous crypto protocols, leverages the ZK-SNARK tech stack. However, this tech stack has some flaws, such as the requirement for a trusted setup, which goes against the anonymous nature of blockchain technology. Consequently, ZCash's anonymity is only partial, and the protocol cannot provide its users with complete privacy.

ZkTsunami

In contrast to its competitors, ZkTsunami implements an end-to-end ZK-AnonSNARK architecture, which supports high-level transactional privacy. The protocol provides complete anonymity without requiring a trusted setup, ensuring that the user's privacy is secure. This architecture offers a significant improvement over the current market options, making ZkTsunami the best choice for anonymous crypto transactions.

ZkTsunami is a game-changer in the anonymous crypto protocol market. Its battle-tested end-to-end ZK-AnonSNARK architecture provides complete anonymity without any limitations, making it superior to its competitors. With its geometrically increasing trading volume, ZkTsunami is poised to become the leading anonymous crypto protocol in the market.

Grin and Beam

Grin and Beam are two anonymous crypto protocols that have some limitations. Firstly, they do not support smart contracts, which limits the developers' ability to utilize anonymity for transactions within a CA. Secondly, their account cancellation mode of operation, which requires the repetitive creation of new accounts, is inconvenient from a user experience point of view.

Dash

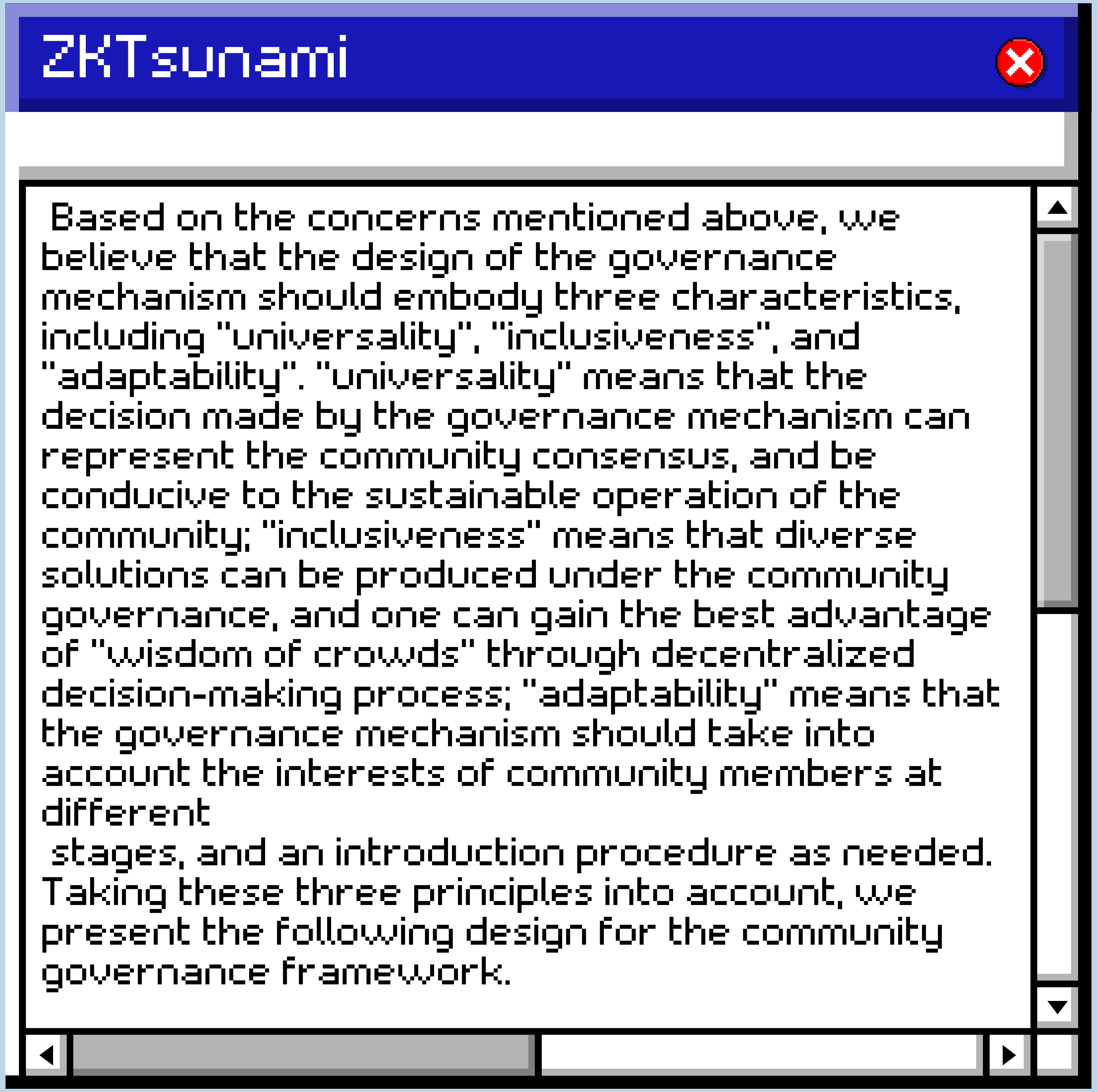
Dash uses the CoinJoin tech stack, which is a crypto-mixing protocol natively built for Bitcoin-based transactions. However, Dash taps into infrastructure rather than implementing a crypto-mixing protocol itself. Additionally, the protocol is currently rebranding and shifting focus towards adoption, which has reduced its privacy-centric tenet.

Governance

1

After research on the existing POS consensus mechanism and the behavior patterns of delegators and validators, the design of the governance mechanism should address these concerns:

1. How to increase the voter turnout rate while keeping the system decentralized?
2. How to keep a balance between the number of votes and the professionalism of decision-making?
3. How to bootstrap the community and introduce the governance structure?



Based on the concerns mentioned above, we believe that the design of the governance mechanism should embody three characteristics, including "universality", "inclusiveness", and "adaptability". "universality" means that the decision made by the governance mechanism can represent the community consensus, and be conducive to the sustainable operation of the community; "inclusiveness" means that diverse solutions can be produced under the community governance, and one can gain the best advantage of "wisdom of crowds" through decentralized decision-making process; "adaptability" means that the governance mechanism should take into account the interests of community members at different stages, and an introduction procedure as needed. Taking these three principles into account, we present the following design for the community governance framework.

2

Start

How to participate

1. Become a community member by holding ZKT token(s). A ZKT token is not only a certificate of community participation, but also a stake in ZKTsunami protocol, and it will play a central role in community governance.

2. Quantifying contribution based on gas. is the basic unit to measure contribution in the ZKTsunami ecosystem, and is calculated according to the quantity and holding period of ZKT token. This means that the more ZKT tokens and the longer the holding period, the lower the transactional costs will be.

Ecosystem roles and their behavior patterns :

ZKT holder
Definition: a holder of the ZKT token who uses some or all of the tokens to secure the ZKTsunami ecosystem.

Behavior pattern: vote on proposals or hold a ZKT token.

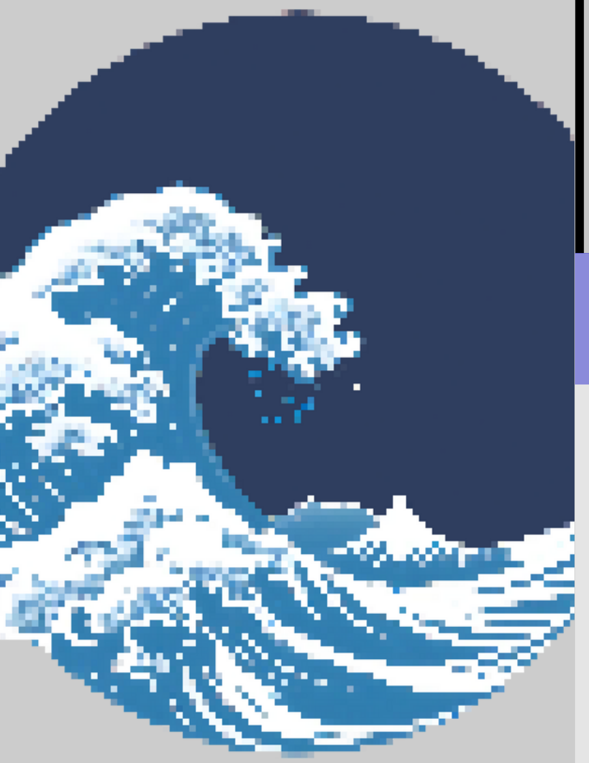
Possible activities :

1. A ZKT holder can vest their tokens to obtain staking interest;

2. If a ZKT holder does not vote on a proposal, they will pay the opportunity cost of losing staking interest;

3. A holder will pay for a different commission rate, depending on how many tokens they hold.

ZKTsunami

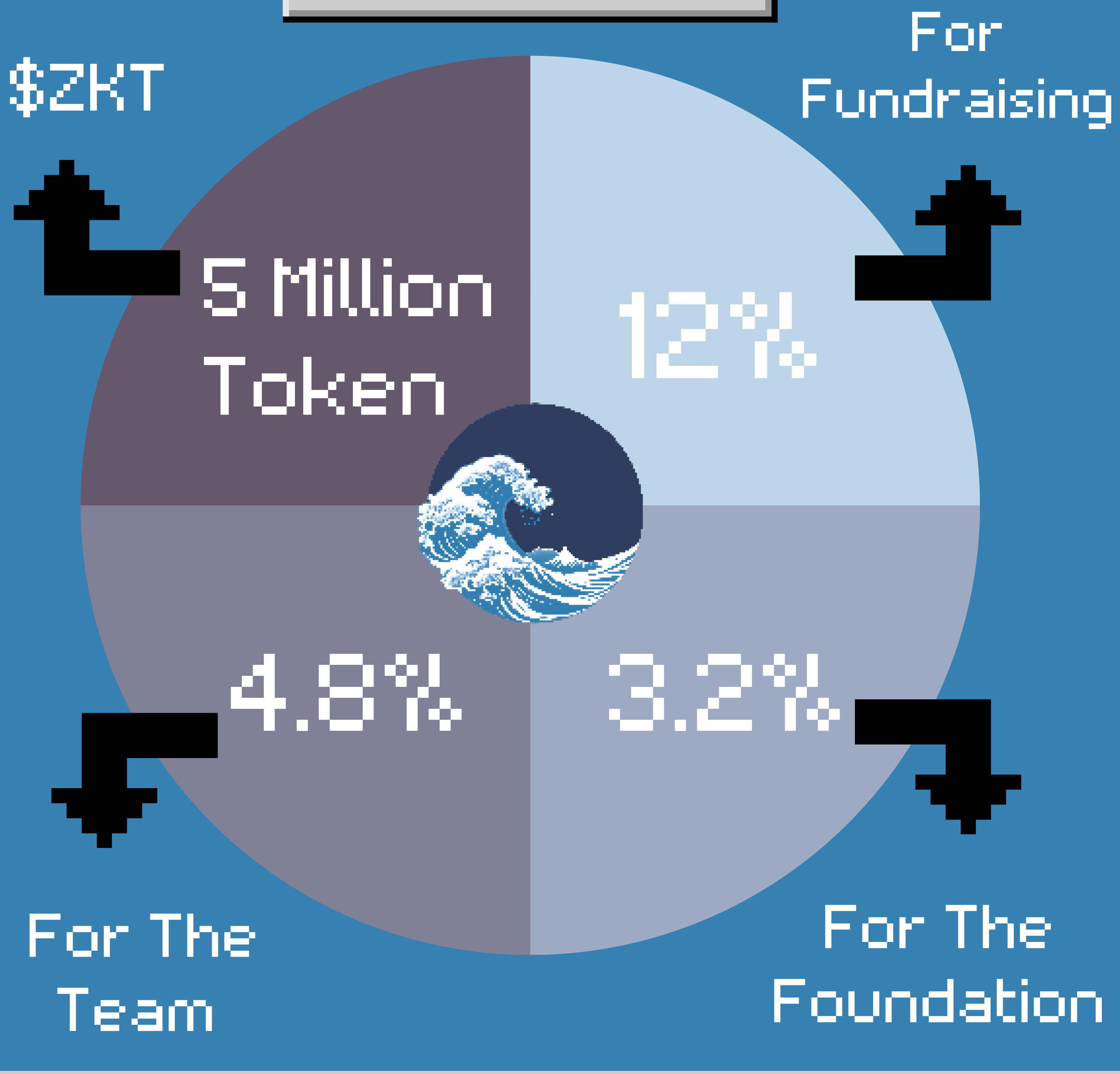


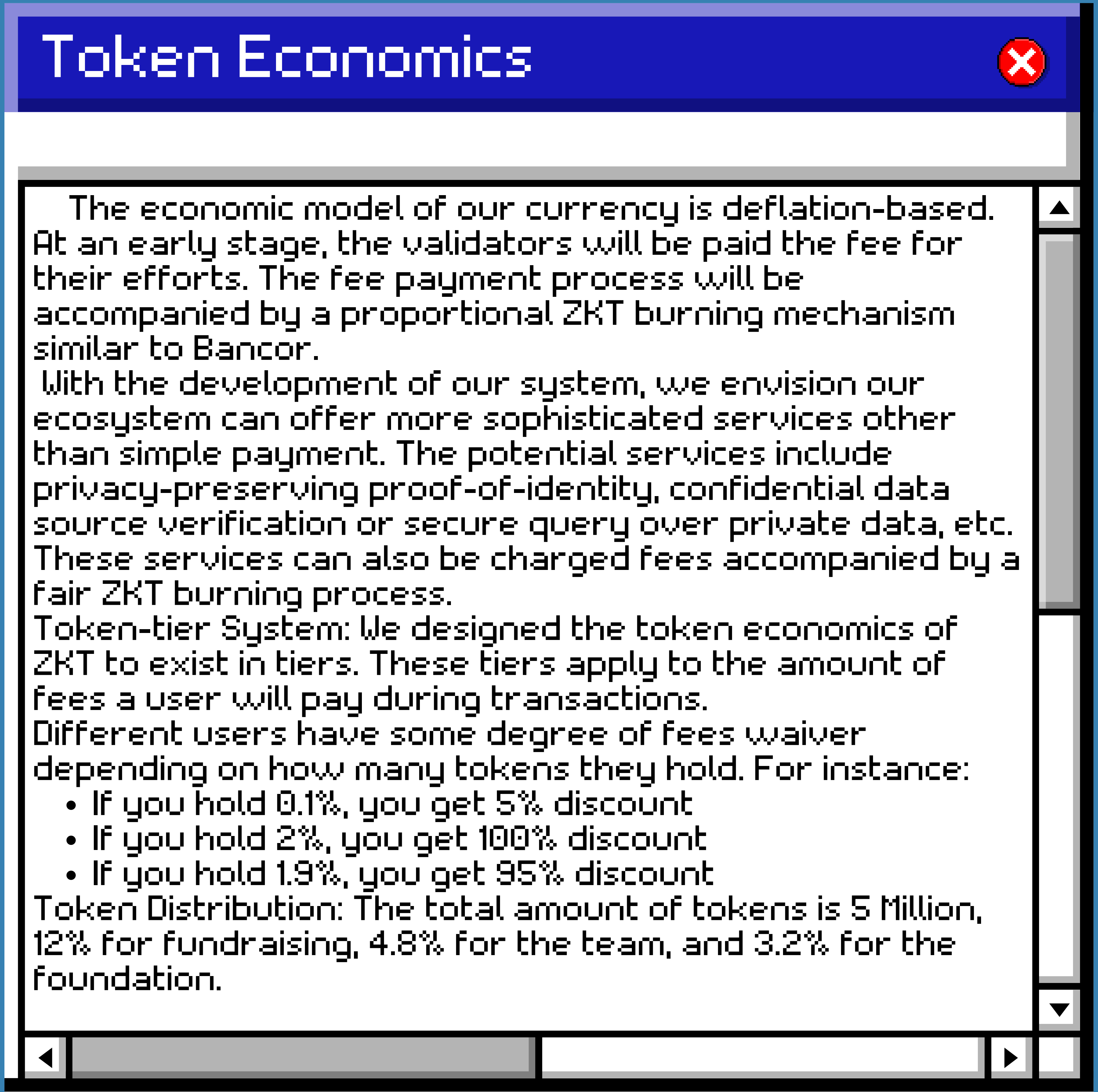
Foundation

Definition: a service organization that does not participate in voting Responsibilities:

1. The development progress;
2. Organize a voting process;
3. Financial management;
4. And other specific matters.

Token Distribution




Token Economics

The economic model of our currency is deflation-based. At an early stage, the validators will be paid the fee for their efforts. The fee payment process will be accompanied by a proportional ZKT burning mechanism similar to Bancor.

With the development of our system, we envision our ecosystem can offer more sophisticated services other than simple payment. The potential services include privacy-preserving proof-of-identity, confidential data source verification or secure query over private data, etc. These services can also be charged fees accompanied by a fair ZKT burning process.

Token-tier System: We designed the token economics of ZKT to exist in tiers. These tiers apply to the amount of fees a user will pay during transactions.

Different users have some degree of fees waiver depending on how many tokens they hold. For instance:

- If you hold 0.1%, you get 5% discount
- If you hold 2%, you get 100% discount
- If you hold 1.9%, you get 95% discount

Token Distribution: The total amount of tokens is 5 Million, 12% for fundraising, 4.8% for the team, and 3.2% for the foundation.

ZKTsunami

Potential Use Cases

1

Private Payment for Defi

With our anonymous payment module for smart contract platforms and anonymous BTC cross-chain transfer module, one could easily build sophisticated Defi functionality such as decentralized exchange, or lending and load. To put the cherry on top of the cake, we will guarantee all the money transfer in these fancy Defi functionality is privacy-preserving, meaning both the sender and receiver identity of a transaction is anonymized while the transaction amount is confidential. The plug-and-play nature of the technical modules provided by the ZKT ecosystem will guarantee the minimum efforts of developing the privacy-preserving Defi. ZKTsunami will be the top choice of Defi projects when they try to ensure maximum liquidity while still preserving their clients' financial privacy.

Proof of Identity

Zero-knowledge proof of identity is another application case of ZK-AnonSNARK. When a registered user visits a website, his identity is revealed when using the conventional password-based authentication approach. On the other hand, he could run the zero-knowledge proof of identity protocol to authenticate themselves to the website without revealing exactly who they are. This serves to protect the user's browsing privacy.

2

Start

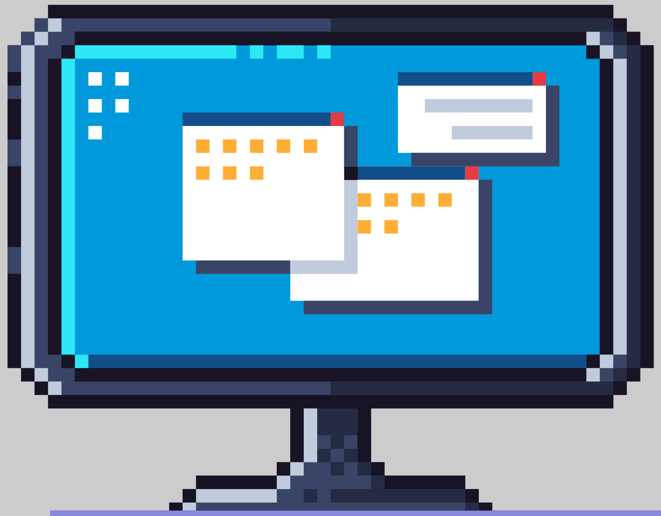
Data Protection and Monetization

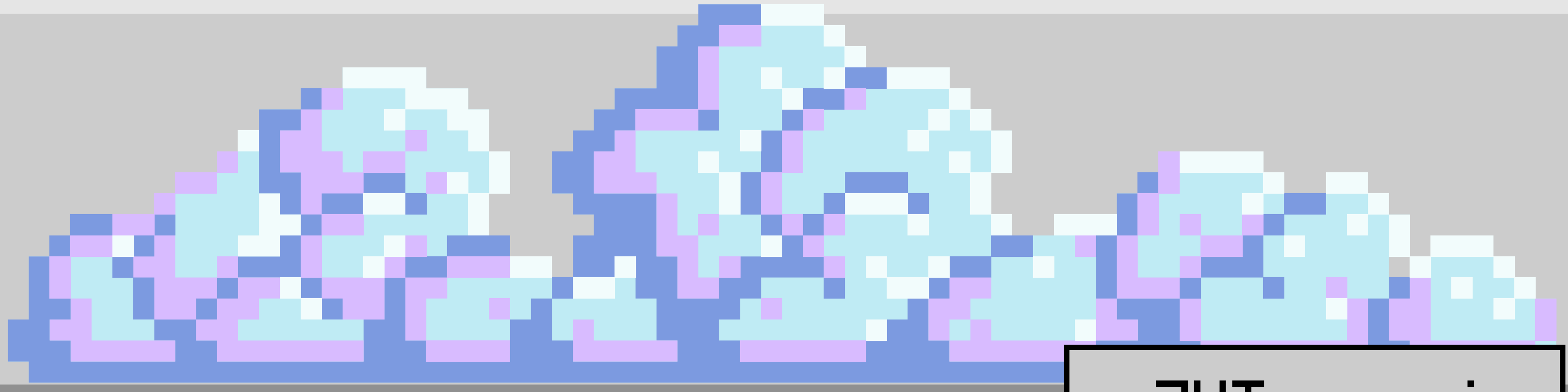
Start

ZK-AnonSNARK

ZK-AnonSNARK can also be deployed to protect one's digital property in a fair data monetization process. Imagine a hacker found a vital bug in a software and they try to sell their knowledge of the bug to the software vendor. But the hacker does not want to reveal this knowledge before they receive the bounty. From the software vendor's perspective, it cannot release the bounty without evidence showing that the hacker has successfully found a bug. In this case, the vendor and attacker could run a zero-knowledge test so that the attacker could indeed present proof showing there is a bug in the software without revealing exactly what the bug is. Using the same principle, the general zero-knowledge AnonSNARK could be used to prove the validity of any data in a privacy-preserving manner in any data monetization deal.

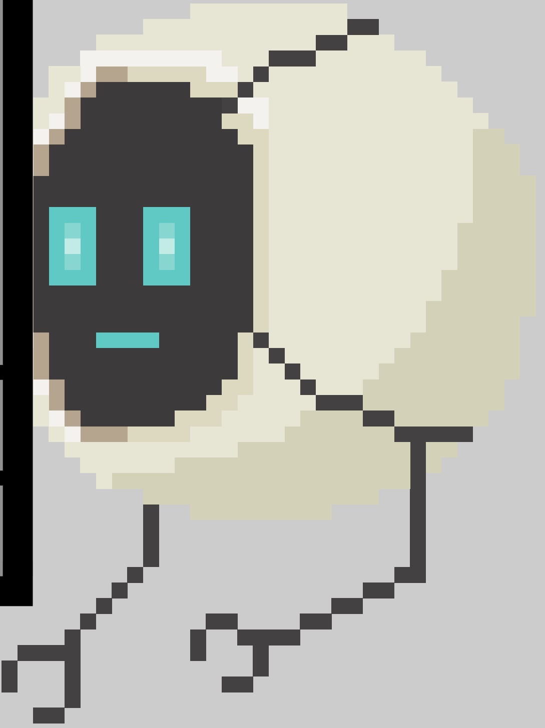
The amazing power of zero-knowledge AnonSNARK can even shine in a centralized setting. For instance, companies like Uber or DiDi have long been accused of manipulating the ridesharing price. However, the price variation could just be the natural result of the algorithm they use in some cases. Nonetheless, it might be difficult for those companies to exonerate themselves since the algorithm, especially the algorithm's parameters, is their core trade secret. In this case, it is possible to apply the general zero-knowledge AnonSNARK to efficiently prove their innocence while protecting their intellectual property. The same principle applies whenever there is a conflict between algorithmic transparency and confidentiality. Zero-knowledge AnonSNARK can always be applied to realize control information leakage such that exactly the amount of balance can be achieved. For instance, the federal reserve could use our zero-knowledge AnonSNARK to prove they are not reckless in terms of their currency policy, while not leaking any classified information.





Conclusion

ZKTsunami provides an interoperable ecosystem for the anonymous digital assets derived from our ecosystem based on our design and implementation of advanced ZK-AnonSNARK technology.



References

1. Beam project. https://github.com/BeamMW/beam.
2. Grin project. https://github.com/mimblewimble/grin.
3. Zcash project. https://github.com/zcash/zcash.
4. Daniel Benarroch. Diving into the zk-snarks setup phase.
5. Benedikt B ¨unz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh. Zether: To wards privacy in a smart contract world.
6. Benedikt B ¨unz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE Symposium on Security and Privacy (SP), pages 315–334. IEEE, 2018.
7. Geoffroy Couteau, Michael Kloo?, Huang Lin, and Michael Reichle. Efficient range proofs with transparent setup from bounded integer commitments. Cryptology ePrint Archive, Report 2021/540, 2021. https://eprint.iacr.org/2021/540.
8. Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability.
9. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. 12. Greg Slepak. How to compromise zcash and take over the world. 13. Nicolas van Saberhagen. Cryptonote v 2.0. https://cryptonote.org/whitepaper.pdf, 2013.

ZKTsunami