Zero Knowledge Proof: A Introductory Guide

This article offers an introduction to the concept of Zero Knowledge Proof (ZKP). Also, you will find different types of ZKP, and use cases and implementation strategies for ZKP.

With people's information being controlled continuously and the lack of privacy, now, demands a new era. Blockchain holding the torch of a decentralized system is making changes, but it's not

Many of you must have heard about zero knowledge proof example but don't really know the concept behind it. Zero knowledge encryption is a new protocol that allows adding a higher level of

---

> **Enroll Now:** Zero Knowledge Proofs (ZKP) Masterclass

Table of Content

Chapter-1: Different Ways to Chain in the Blockchain

Typically, blockchain is merely a shared database, where you are keeping a score of who owns how much cryptocurrency or other digital assets. However different blockchain works a bit differe

For example, you'll see metadata in bitcoin and other contractual logics in Ethereum. In any case, blockchains, mainly private blockchains offer two severe use cases.

- Owning external assets, which is represented by tokens on the network. A user can also transfer external assets using the tokens.
- Increased privacy and application are more related to general applications of data management.

Not saying, that every private blockchain offers these two use cases. But typically, private blockchains can be more suitable for companies, which needs additional confidentiality and privacy.

Regarding storing general data, blockchain does indeed do a lot of services. First, it needs to prove where the data is coming from, then timestamp it and then making it immutable so that no one

However, the blockchain doesn't have anything to say about the information itself. So, every app can decide what the data can actually represent or if it's actually valid or not. Any bad data coul

So, if blockchains want to transfer any kind of assets, it needs to offer internal rules on the process of validating those transactions. This is something that the blockchain lacks from the start — o

---

> Don't know the fundamentals of blockchain technology? Read this detailed guide on introduction to blockchain features.

Can Blockchain Maintain the Privacy Needed?

For example, maybe you want to send $50 to your friend Kevin. But before your transaction gets approved the network needs to know whether you really have $50 in your possession. Althou needs to know that you own $50.

This helps to maintain the validity of your assets along with Kevin's when he receives the money. However, you are sacrificing your privacy for the sake of this validating process.

But there's a catch. In blockchain, you won't have a regular identification name such as Kevin. Instead, you'll get addresses for transactions and all these addresses a stream of strings that has no

Even though this information is accurate, still this necessarily doesn't change the scenario. Why? Well, you can still find many ways to figure out connections between two users and figure out th

The Issue with Current Scenario

At first, if a user wants to transact or send assets on the chain, then he/she needs to know the address. So, when you send the money, you can see which address it's going to. On the other hand, if

If a user knows any information about another user from the real world, then he can easily track and figure out what address the other is using. Obviously, they can search through the chain and f

Yes, it's time-consuming, but it's not impossible to know. That's why having addresses instead of names doesn't help preserve the privacy of the network.

Can Only Encryption be Enough?

The concept of privacy and sensitive information is closely related to encryption. If you are thinking about storing only general data on the blockchain, then we can definitely do that. In this case

As none of them don't have anything to do with the data type, therefore, you would still be able to use the distributed ledger to store any data that is only readable. But you would still need to r before.

However, you can't use this type of encryption for transactions that signify any transfer of tokenized assets. If you and Kevin encrypt your transactions, nobody on the chain can ever safely use tl

The asset in question would lose its value on the ledger, so encryption can't be the answer.

Enroll Now: Ethereum Development Fundamentals

A Conflict between Liquidity and Privacy

Now you can see that, if we want to use blockchain for financial purposes, then you will always face a conflict between these two. Many startups are facing this problem now when they are deali

Even though there have been many pilot projects simulating the process on the blockchain, in real life, it's not the same. The process requires too much activity and thus reveals that two addresse

This is how information gets leaked, and it's one of the major issues, but there aren't any specific rules on the network still now.

Now many startups settle all their scores off-chain rather than on-chain where they can encrypt and get the privacy. But blockchain has so much to offer, and on-chain settlements with privacy co

Among all these conflicts, we finally have the solution we have been looking for – The Zero Knowledge Proof.

Also Read: Example Of A Good Zero Knowledge Proof

Chapter-2: What is Zero knowledge Proof?

The concept behind zero-knowledge proof is unique indeed. A zero-knowledge proof is a unique method where a user can prove to another user that he/she knows an absolute value, without actu

Here, the prover could prove that he knows the value z to the verifier without giving him any information other than the fact that he knows the value z.

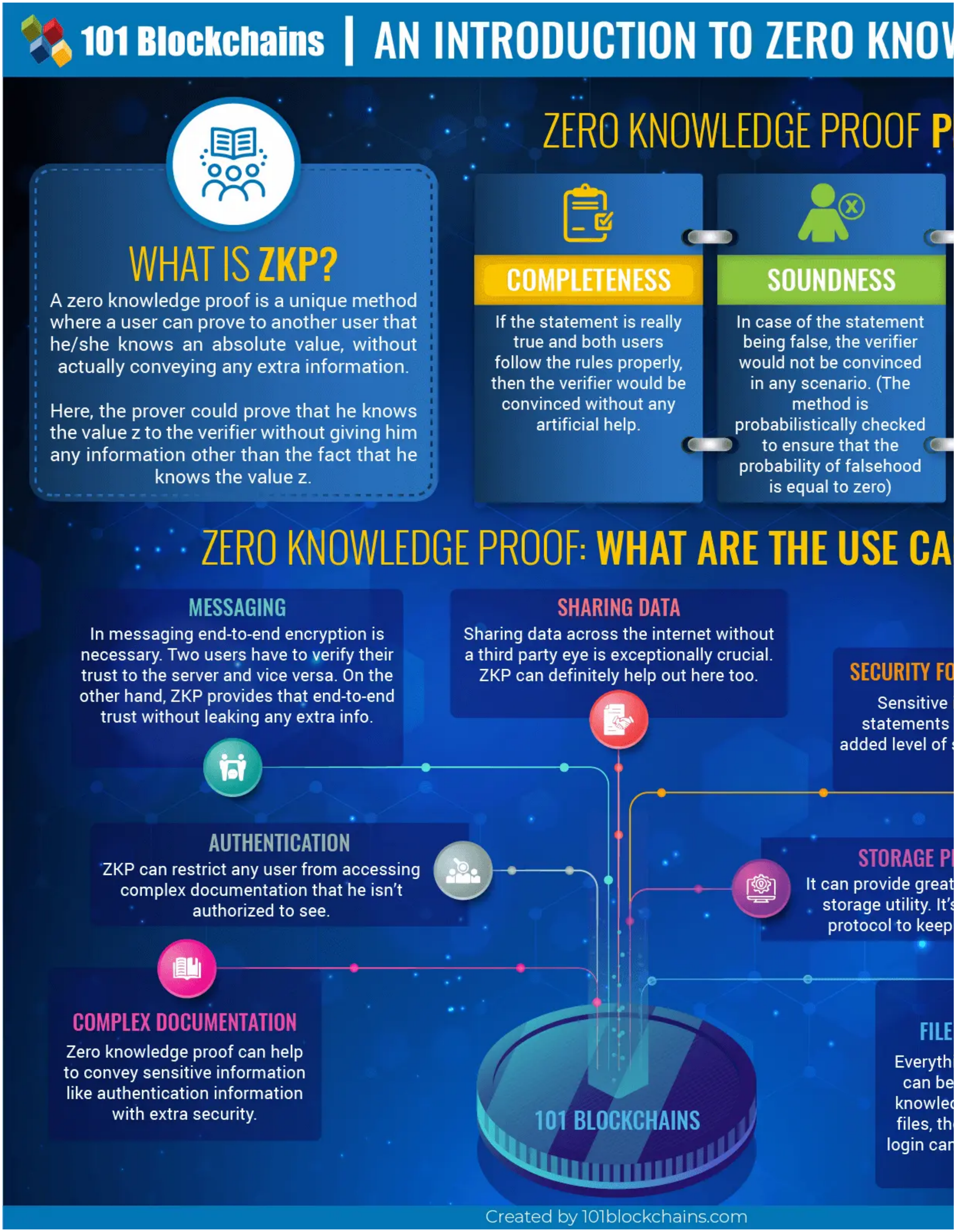
The main essence behind this concept is to prove possession of knowledge without revealing it. The primary challenge here is to show that you know a value z without saying what z is or any otl

Seems tough? Well, it's not that difficult.

If a user wants to prove a statement, then he would be required to know the secret information. This way the verifier would not be able to relay the information to others without actually knowing

Thus, the statement will always need to include that the prover knows the knowledge, but not the information itself. Meaning, you can't say the value of z but can state that you know z. Here, z c

This is the core strategy of zero knowledge proof applications. Otherwise, they won't be zero knowledge proof applications. That's why experts consider zero knowledge proof applications to be



101 Blockchains | AN INTRODUCTION TO ZERO KNOW

WHAT IS ZKP?

A zero knowledge proof is a unique method where a user can prove to another user that he/she knows an absolute value, without actually conveying any extra information.

Here, the prover could prove that he knows the value z to the verifier without giving him any information other than the fact that he knows the value z.

ZERO KNOWLEDGE PROOF P

COMPLETENESS

If the statement is really true and both users follow the rules properly, then the verifier would be convinced without any artificial help.

SOUNDNESS

In case of the statement being false, the verifier would not be convinced in any scenario. (The method is probabilistically checked to ensure that the probability of falsehood is equal to zero)

ZERO KNOWLEDGE PROOF: WHAT ARE THE USE CA

MESSAGING

In messaging end-to-end encryption is necessary. Two users have to verify their trust to the server and vice versa. On the other hand, ZKP provides that end-to-end trust without leaking any extra info.

SHARING DATA

Sharing data across the internet without a third party eye is exceptionally crucial. ZKP can definitely help out here too.

SECURITY FO

Sensitive statements added level of

AUTHENTICATION

ZKP can restrict any user from accessing complex documentation that he isn't authorized to see.

STORAGE PI

It can provide great storage utility. It's protocol to keep

COMPLEX DOCUMENTATION

Zero knowledge proof can help to convey sensitive information like authentication information with extra security.

FILE

Everyth can be knowle files, th login can

Created by 101blockchains.com

```
Please include attribution to 101blockchains.com with this graphic. <a href='https://101blockchains.com/blockchain-infographics/'> <img src='https://101blockchains.com/wp-c
```

Zero Knowledge Proof Properties

A zero-knowledge proof needs to have three different properties to be fully described. They are:

- **Completeness:** If the statement is really true and both users follow the rules properly, then the verifier would be convinced without any artificial help.
- **Soundness:** In case of the statement being false, the verifier would not be convinced in any scenario. (The method is probabilistically checked to ensure that the probability of falsehood is
- **Zero-knowledge:** The verifier in every case would not know any more information.

Researchers are further investigating the process to be more accurate and make sure it requires fewer interactions between two peers. Mainly the goal is to eliminate the amount of communicatio

Zero knowledge proof applications have been gaining popularity from quite some time now. But it’s not a new concept out on the blue. It’s been here for more than 20 years. Researchers have im

Now, proving a statement is super easy and highly efficient. It can now go directly with the blockchain system.

Chapter-3: How does Zero Knowledge Proof Work?

Zero knowledge proof applications seem like a unique protocol. However, many of you must be wondering how you prove your statement without actually relaying the information. Well, let me

Lets’ start.

First Example: Ali Baba Cave

This is one of the favorite scenarios to properly investigate how the zero knowledge proof authentication works. Here the prover is known as Peggy, and the verifier is Victor.

So, to keep things on the same level as zero knowledge proof authentication, the prover would know a value z, and the verifier would know that the prover knows the value z.

The example starts like this, imagine that Peggy somehow knows a secret word that can open a magic door inside the Ali Baba cave. The cave looks like a ring with the door blocks the pathway

Now, Victor wants to make sure that Peggy is telling the truth. Meaning, she knows the secret word. But Peggy is a private person and is unwilling to say the magic word to Victor. So, how can V

A Different Scheme

Victor comes up with a plan to solve the situation. He marks the entrance path A and exit path B. However, as they meet at the same position, path A and B are just left and right path. During thi

Peggy now has the option to take path A or B, but whatever she takes Victor can’t know that. After Peggy chooses a path, she goes in, and Victor enters the cave. He then shouts the path name w

Well, if she actually knows the secret word, it’ll be really easy. She can use that word to open the door and return to Victor. Or she can also return the same path if necessary.

Suppose, Peggy doesn’t really know the word. In that case, she would only be able to return to Victor, if Victor shouts the name of the path, she chooses at first. As the selection process is rand
15 time or 25 times, then Peggy would not be able to make a lucky guess to fool him.

Anticipating Victors move will become next to zero and Peggy would get caught.

But even after repeating this process so many times, Peggy manages to come back wherever Victor wants her to be; then Victor can safely assess that she does know the secret word.

What Happens with A Third-Party View?

Typically, if a third-party is watching this situation, then Victor would have to have a hidden camera to record the transaction. However, the camera would only be able to record what Victor i
Appearing at A when he shouts A.

This recording could be straightforward to fake for two people if they agree on this from beforehand. That’s why no third party would be convinced with this record that Peggy actually knows th

So, how do they prove the integrity of the experiment?

If Victor flips a coin and then chooses the path based on that, the zero knowledge proof authentication will lose its property. But the coin flip would be convincing enough for any third-party obs

This way Victor would be able to prove the integrity of the experiment without knowing the word. But it won’t be entirely zero knowledge proof.

In digital cryptography, Victor can flip coin using a random number generator that has some fixed patterns like the coin. But if Victor’s coin behaves like a number generator, then he and Peggy

Thus, even with a number generator, it won’t be as much as efficient as the simple coin flip.

Only Single Trial

Did you notice that Peggy could easily prove that she knows the word without saying the word in the first try? In that case, Peggy and Victor need to go inside the cave at the same time. Victor w

But this kind of proof would convince anyone. So, Peggy doesn’t want anyone else to know about it, she can’t say that she conspired with Victor. Because she doesn’t even know who knows abo

Second Example: A Color-Blind Friend and Two Balls

This type of experiment for zero knowledge proof authentication would require two same sized balls but with different colors. The experiment is really popular. Mike Hearn and Konstantinos Ch

It goes like this — imagine you have a color-blind friend and two balls. The balls need to be red and green and of the same size. Your friend thinks they are the same thing and is doubting your s

So, you need to prove that they have different colors without telling him which is which.

You give the balls to your friend, and he keeps them hidden behind his back. After that, he brings out a ball randomly and lets you see it. He then puts that ball back and then randomly chooses th

You get to see the ball this time too. After that, he would ask you whether he switched the ball or not. He will be repeating this process for some time to be sure.

Now that you are not color blind, you can definitely tell that if he switched the ball or not. If the balls were of the same color, your probability for answering correctly would be 50%. So, after rep

The probability of anticipation would become zero, and you would achieve the three zero knowledge properties.

But make sure that your friend doesn't know which one is green and which one is red. This way you will be able to preserve the third property "zero knowledge."

Chapter-4: Interactive Zero Knowledge Proof

Zero knowledge encryption can be of two kinds –

- Interactive zero knowledge proof.
- Non-interactive zero knowledge proof.

Let's see what they are.

The Fundamentals of Interactive Zero Knowledge Proof

This type of zero knowledge proof authentication would require interactions between peers or any computer systems. By interacting, the prover can prove the knowledge, and the validator can va

This is the most typical scenario of zero knowledge proof blockchain. Here, you would be proving without disclosing the understanding. But you are also revealing it to the user you're interactin

Although it's one of the best privacy protocols, still it requires a lot of efforts when you want to prove it to more than one people. This is because you would have to repeat the same process over

This protocol would need any kind of interactive response from the verifier to execute. Or else, the prover can never prove it on their own. The interactive input could be a form of challen knowledge.

In other cases, the verifier could record the process and then play it for other so that they can also see it. But whether other people would actually be convinced or not depends solely on them. Th

This is why interactive zero knowledge proof blockchain is more efficient for few participants rather than a large group.

Chapter-5: Non-Interactive Zero Knowledge Proof

Non-interactive zero knowledge proof blockchain is here to verify one's statement to a larger group of people. You don't always have to go for the non-interactive zero knowledge proof blockcha

But when you can't find anyone, then non-interactive zero knowledge proof blockchain is the way to go.

The Sudoku Challenge with Cards

Sudoku is one of the most difficult games but with simple rules. All of the rows, sectors, and columns need to have the number 1-9 only once.

In this case, imagine you know the solution of this puzzle, which may take days for even computers. So, if you want to sell the solution how the verifier will know that you are not tricking him?

Let's see how you can do it.

A Way to Solve

You would need 27 cards where they are numbered from 1-9. So, 27 cards would contain the number 1 and then another 27 the number 2. In total, you would need 243 cards.

Now you would have to put three cards in a corresponding box with the solution. Meaning if the correct number for that box is five, you will put three number 5 cards in that box.

In a Sudoku table, you see some answers are always visible. In these boxes, you will place the card face up. On boxes that don't have the answer, you will place the cards upside down.

Now you need to prove that you have placed all cards in the right position without revealing it. You have to:

Take the topmost card from each column until you have nine piles. Repeat the same thing for rows and sector.

Then you would need to shuffle every pile and then turn over to reveal the numbers.

You know the basic rule, all numbers from 1-9 have to appear once in every row, sector, and column. So, if all of your pile has the number 1-9 appearing only once then the verifier would know t

Non-interactive can be the best way to prove your statement to a lot of people without increasing resources and costing.

Read Now: Benefits of Blockchain Technology

Chapter-6: Zero Knowledge Proof Explained – zk-SNARKS Explained

You must have heard about zk-SNARKS by now. Ever wonder what it actually is? Well, zk-SNARKS explained is a technology that uses the non-interactive zero knowledge proof example conc

It's actually an acronym for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge.

This technology consists of three different algorithms:

- **Key Generator:** The key generator sets up a parameter to generate a key pair. Here, a trusted source could generate a private or public key pair and then destroy the private part. Afte verifying.
- **Prover:** The prover has to take the proving key and some public input to proof his knowledge. Here, he will be witnesses privately and then satisfy the context to prove his point.
- **Verifier:** The verification would need the verification key to make sure the statement is true or false. He has to take in the public input and the proof to evaluate whether it's true or false.

Other than these three the zk-SNARKS also need to maintain –

- **Zero-knowledge:** The verifier would not learn anything other than the fact that the statement is true. Succinct: Whatever the challenge maybe it needs to be really small so that one can pro
- **Non-Interactive:** The user would only be sent the stamen to the verifier and nothing else. Verifier won't be able to interact further with the prover.
- **Argument:** The proof would hold the soundness of zero knowledge encryption and would be bound by polynomial-time.
- **Of Knowledge:** Prover and Verifier can't execute the process without a trusted witness.

Chapter-7: Enterprises Utilizing Zero Knowledge Encryption

Now that you know all about zero knowledge proof let's take a look at some of the famous enterprises that use this protocol.

Notable Projects

- **Zcash**

Most of the blockchain platform exposes the transactions between two peers. Not only it's one of the disadvantages of the blockchain, but it's also disrupting its growth. Zcash, on the other hand,

It's open-source and permissionless blockchain platform that utilizes the essence of zero knowledge proof. The transaction process is shielded. So, it will find the value, the sender and recipient o

It's also famous for introducing zk-SNARKS and after that many have followed its path.

Read More: What is Zcash?

- **ING**

The ING is a Netherlands based bank who has started their new zero knowledge blockchain. Although they launched a bit of a modified version of zero knowledge system is called zero knowled

It's directly related to the financial sector such as mortgage value. You will be able to prove that you have the salary to get a mortgage without revealing your salary.

Currently, it's open source, but it does through a considerable challenge to other financial blockchains.

- **PIVX**

This company wants to change the typical ways that the world works. In a system where everything is controlled and managed by others, PIVX intends to introduce a safe haven for your fina example.

Here, the only thing that would be public is the confirmation of sent money. Meaning, you would see that someone sent money, but the address or amount of timing would be hidden. PIVX ensur

- **Zcoin**

The company utilizes Zerocoin protocol for providing extra security and completely anonymous transaction. The Zerocoin protocol obviously follows the zero knowledge proof example concept

Here, with the use of Zcoin, you will be able to preserve your identity to the fullest and what you are spending on the network. It's a great way to protect fungibility.

But don't confuse them with Zcash. They have different protocols and definitely not forks of each other.

Want to become a blockchain professional? Enroll Now: Certified Enterprise Blockchain Professional (CEBP)

Notable Vendors

- **StarkWare**

StarkWare is another great company that utilizes the zero knowledge proof example for technology to the fullest. But they seem to twist up the typical SNARKs protocol. Instead of SNARKs, th

StarkWare aims to improve the privacy and scalability problem of blockchain with a transparent transaction method. They are currently developing the hardware and software support to ensure a

This new technology will get rid of the hidden inflation problem, which will remove the trusted setup. zkSTARK is the acronym for Zero Knowledge Scalable Transparent ARgument of Knowle

This new STARK technology could be the next stage of SNARKs.

- **QED-it**

This is one of the startups that utilizes zero knowledge proof to provide security. QED-it is an Israeli based company that is capable of handling confidential data without the third party eye. You

Some of their popular customers include BNP Paribas and Deloitte. The main goal is to provide privacy to enterprises. Last two years, they improved their project, developing brand new SNARK

Some of their use cases are a real-time risk assessment, supply chain, asset management, predictive maintenance, and many more.

Chapter-8: Where Can You Use ZKP?

ZKP or zero knowledge proof use cases need to be able to work with cryptography and trustable devices. Compared to other devices mobile seems to be the correct choice here. They offer a safe

But the main question is where can you utilize zero knowledge proof use cases?

- **Messaging**

In messaging end-to-end encryption is necessary. So that, no one can read your private messages without the client itself. Two users have to verify their trust to the server and vice versa. On the c would be able to hack their way to your message anymore.

This is one of the zero knowledge proof use cases.

- **Authentication**

Zero knowledge proof can help to convey sensitive information like authentication information with extra security. Here, ZKP can maintain a secure channel for the user to use his/her authentica

- **Sharing Data**

Sharing data across the internet without a third-party eye is exceptionally crucial. When you share something on the network no matter how protective they claim to be, there are always some risl

Someone could always hack in or intercept in between sharing information — this is where ZKP can definitely help out.

This is another great one of the zero knowledge proofs use cases.

- **Security for Sensitive Information (Credit Card Info)**

Sensitive information such as bank statements or credit card info needs an added level of protection. The bank preserves the credit card history. However, when you request the information from

Even though banks go through a secure line, still one's credit card history is a lot more sensitive than average data. In this case, not just encrypting the whole information as one but blocks, the ba

Because banks would only manipulate the necessary blocks without touching other blocks, your history will get the right amount of security layer. And ZKP can provide that.

- **Complex Documentation**

ZKP can restrict any user from accessing complex documentation that he isn't authorized to see. As ZKP is able to encrypt the data in chunks, you will only have to manipulate certain blocks to g

This way, unauthorized people won't be able to see your documents.

- **Storage Protection**

It can provide greater protection for your storage utility. ZKP is equipped with the protocol to keep the hackers away. With this, not only your storage unit but the information within it will also b

- **File System Control**

Everything within a file system can be protected by the zero-knowledge proof protocol. The files, the users and even every login can have different layers of security. So, it can be a great use case

All of these zero knowledge proof use cases can be used in real life scenario.

Read more: How Zero Knowledge Proofs Are Changing Blockchain?

Chapter-9: Implementing Zero Knowledge Proofs Architecture

Before you want zero knowledge proof implementation, you need to know about what it relies on.

Key Wrapping Process

ZKP splits a single stream of data into small blocks. Each of these blocks is encrypted separately. In zero knowledge proof implementation, the key to encrypt will be on the user only, and with th

Managing Privileges

The keys will be stored in containers. But if a user wants to change the storage key, then he would have to compare his ownership tag. If they match, then he will be able to change it, and if they

Controlling Requests

You should make sure that no one can just add up texts within your zero knowledge proof implementation. As the users will only be able to access it in the blockchain network, you need to conv

This way no one would be able to bypass your security measures.

Mitigate All Attacks

The blockchain is not a perfect network. Even if it lowers the amount of attack, it doesn't fully get rid of it. So, when you integrate ZKP in a system, couple it with other measures. This way implementation does require these methods to work correctly.

Is Zero Knowledge System Important?

Zero knowledge proof explained by far has been proving itself to be capable of handling enterprise level businesses. Not everyone is a fan of the public ledger system where everyone can s addresses too.

Also, when it comes to storing additional sensitive information blockchain isn't the best idea. Enterprises deal with a lot of private info, and the existing privacy protocol isn't enough.

Zero knowledge proofs explained only can improve blockchain, but it can also get rid of all the negative issues. Many enterprises aren't interested in blockchain even though; it's a beautiful inve

So, the answer would be yes, zero knowledge system is undoubtedly an important factor regarding blockchain.

Enterprise courses can offer you better context to ZKP. Enroll in our blockchain courses and take your blockchain career to the next level.

Chapter-10: Conclusion

Blockchain comes with its own set of merits and demerits. Even though at first it seemed quite promising, but it does indeed have a lot of baggage. These faults are slowing the growth of this wo

However, with the introduction of zero knowledge system – the knight in shining armor, things have started to change. Now blockchain can be the super protective platform everyone hoped for.

If you are interested in more fundamental block concepts like ZKP, this free fundamental enterprise blockchain course will come in handy.

About Author

Hasib Anwar

An engineer, a gadget-freak, and a perfection fanatic – the ideal combination of a tech-nerd! This Enterprise Blockchain Analyst seems to have an unfathomable interest in blockchains, w

Search

-

Categories

Analyst Corner	(36)
Blockchain Surveys	(8)
Community Spotlights	(10)
Comparisons	(46)
Featured	(8)
Guides	(471)
Newbies	(36)
News	(68)
Opinions	(84)
Profiles	(9)
Reviews	(222)
Startups	(3)
Uncategorized	(5)

-

Featured Posts

Top 20 Promising Blockchain Projects in 2022

6 Key Blockchain Features You Need to Know Now

List of 10 Most Expensive NFTs Ever Sold

List of Top 50 Companies Using Blockchain Technology

How to Become Certified Expert in Blockchain?

-

Recent Posts

Optimistic Rollups Vs Zero-Knowledge Rollups

[Top Ethereum Bridges You Should Know]

[A Beginner’s Guide to Vyper]

[How to Become a Web3 Developer]

[Everything You Need to Know About the Roblox Metaverse]

Subscribe Now

Your email address

Your first name

□ *I agree to the Privacy Policy and Terms of use.*

SUBSCRIBE NOW

Related Post

Guides

Top Ethereum Bridges You Should Know

James Howell

August 24