

# zk-SNARK

Distributed Lab

Sep 5, 2024



- 1 What the zk-SNARK is?

# What the zk-SNARK is?

# What the zk-SNARK is?

## Definition

**zk-SNARK** – Zero-Knowledge Succinct Non-interactive ARgument of Knowledge.

# What the zk-SNARK is?

## Definition

**zk-SNARK** – Zero-Knowledge Succinct Non-interactive ARgument of Knowledge.

- **Argument of Knowledge** - a proof that the prover know data that resolves a certain problem, and this knowledge can be verified.

# What the zk-SNARK is?

## Definition

**zk-SNARK** – Zero-Knowledge Succinct Non-interactive ARgument of Knowledge.

- **Argument of Knowledge** - a proof that the prover know data that resolves a certain problem, and this knowledge can be verified.
- **Succinct** - the proof size is relatively small and does not depend on the size of the data or statement.

# What the zk-SNARK is?

## Definition

**zk-SNARK** – Zero-Knowledge Succinct Non-interactive ARgument of Knowledge.

- **Argument of Knowledge** - a proof that the prover know data that resolves a certain problem, and this knowledge can be verified.
- **Succinct** - the proof size is relatively small and does not depend on the size of the data or statement.
- **Non-interactive** - to produce the proof, the prover does not need any interaction with the verifier.

# What the zk-SNARK is?

## Definition

**zk-SNARK** – Zero-Knowledge Succinct Non-interactive ARgument of Knowledge.

- **Argument of Knowledge** - a proof that the prover know data that resolves a certain problem, and this knowledge can be verified.
- **Succinct** - the proof size is relatively small and does not depend on the size of the data or statement.
- **Non-interactive** - to produce the proof, the prover does not need any interaction with the verifier.
- **Zero-Knowledge** - the verifier learns nothing about the data used to produce the proof, despite knowing that this data resolves the given problem and that the prover possesses it.



# Still didn't get who is Snark...

Well... Let's take a look at some example.

# Still didn't get who is Snark...

Well... Let's take a look at some example.



Imagine you're part of a treasure hunt...

# Still didn't get who is Snark...

Well... Let's take a look at some example.



Imagine you're part of a treasure hunt...

...and you've found a hidden treasure chest...



# Still didn't get who is Snark...

Well... Let's take a look at some example.



Imagine you're part of a treasure hunt...

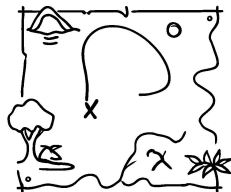
...and you've found a hidden treasure chest...



...but how to prove that without revealing the chest location?

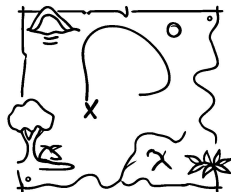
# Still didn't get who is Snark...

**The Problem:** you have found a hidden treasure chest, and you want to prove to the organizer that you know its location without actually revealing that.



# Still didn't get who is Snark...

**The Problem:** you have found a hidden treasure chest, and you want to prove to the organizer that you know its location without actually revealing that.



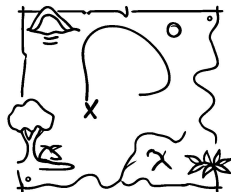
We can retrieve some information from that:

## Question #81673

What is a secret data? Who is a prover and who is a verifier?

# Still didn't get who is Snark...

**The Problem:** you have found a hidden treasure chest, and you want to prove to the organizer that you know its location without actually revealing that.



We can retrieve some information from that:

## Question #81673

What is a secret data? Who is a prover and who is a verifier?

**The Secret Data:** the exact treasure location.

**The Prover:** you.

**The Verifier:** the treasure hunt organizer.

# Ohh... Got it!

Here is how we can apply the zk-SNARK to our problem:

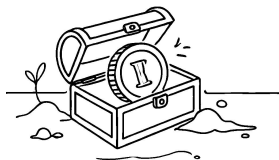
- Argument of Knowledge: You need to create a proof that demonstrates you know the chest is.
- Succinct: The proof you provide is very small and concise. It doesn't matter how large the treasure map is or how many steps it took you to find the chest.
- Non-interactive: You don't need to have a back-and-forth conversation with the organizer to create this proof.
- Zero-Knowledge: The proof doesn't reveal any information about the actual location of the treasure chest.



# Ohh... Got it!

Here is how we can apply the zk-SNARK to our problem:

- Argument of Knowledge: You need to create a proof that demonstrates you know the chest is.
- Succinct: The proof you provide is very small and concise. It doesn't matter how large the treasure map is or how many steps it took you to find the chest.
- Non-interactive: You don't need to have a back-and-forth conversation with the organizer to create this proof.
- Zero-Knowledge: The proof doesn't reveal any information about the actual location of the treasure chest.



Well... The golden coin where the pirates' sign is engraved is our zk-SNARK proof!