WHAT IS ZERO KNOWLEDGE ??

Zero-knowledge proof is a cryptographic concept that allows one party to prove knowledge of a specific piece of information to another party without revealing any details about the information itself.

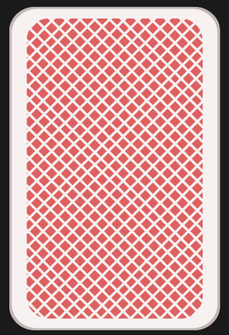
Prover

Secret

Verifier

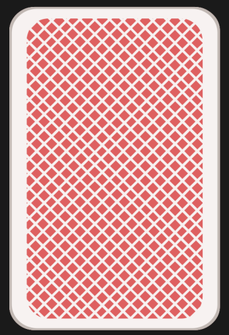
Deck of cards

Deck of cards



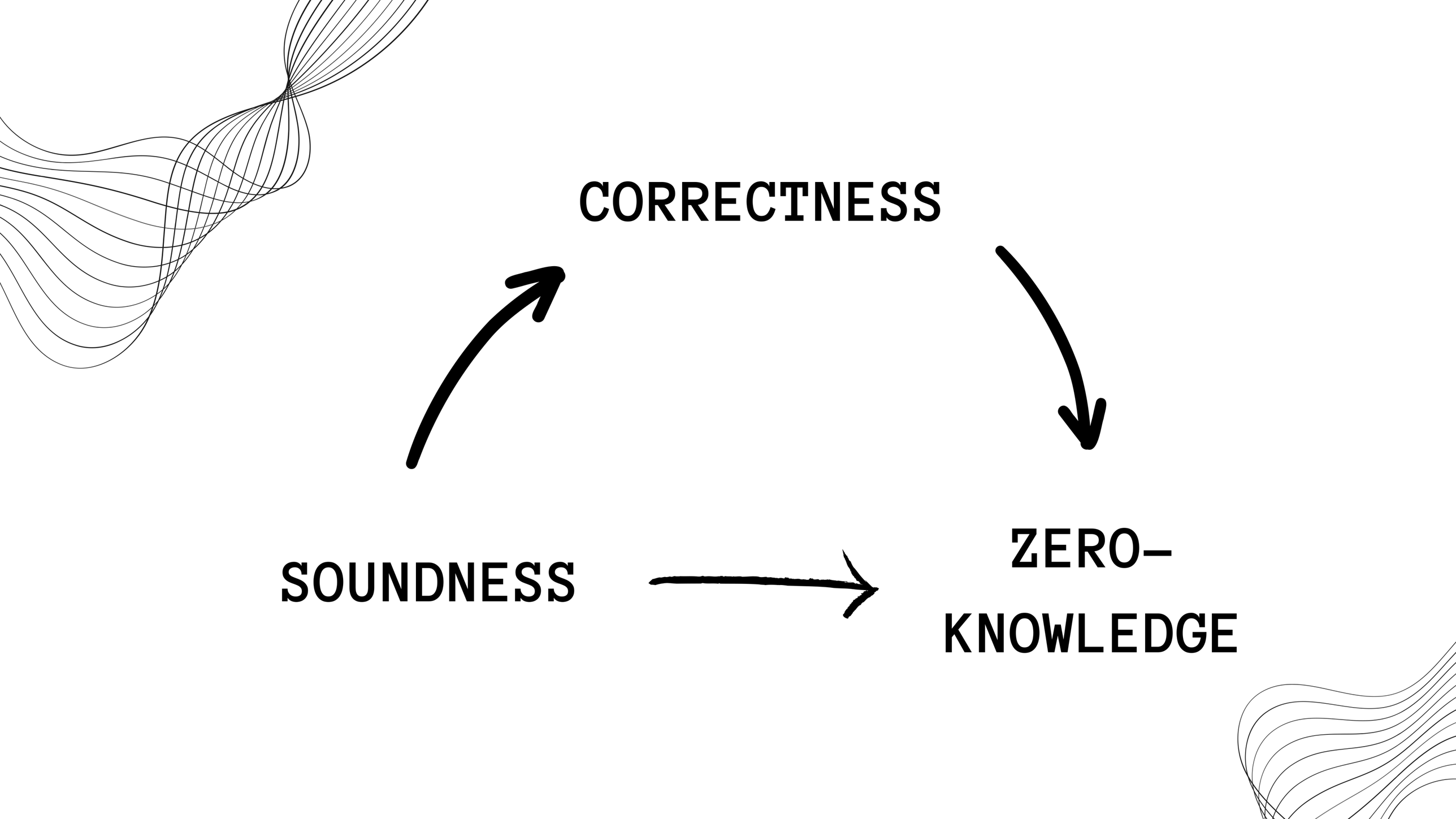
I Withdrew a card and claim it’s RED

Deck of cards

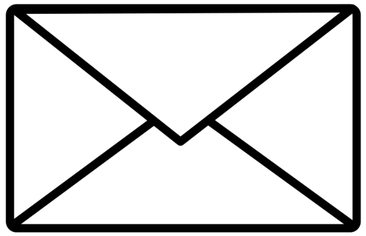


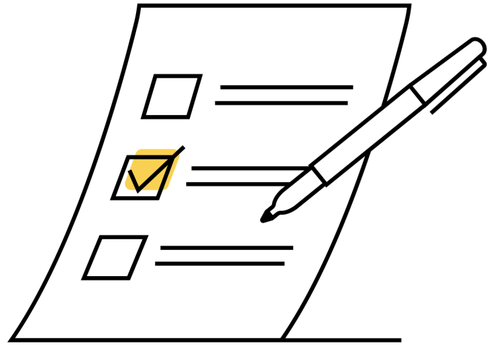
I Withdrew a card and claim it’s RED

Showing you 26 black cards


CORRECTNESS
SOUNDNESS
ZERO-
KNOWLEDGE

EVOTING EXAMPLE





0 or 1

EVOTING EXAMPLE

Protocol 1 : Sum of the votes is 1

EVOTING EXAMPLE

Protocol 1 : Sum of the votes is 1

Protocol 2 : The votes are in binary digits

EVOTING EXAMPLE

Protocol 1 : Sum of the votes is 1

Protocol 2 : The votes are in binary digits

Protocol 3 : Know the content inside the vote

COLOR BLIND ACTIVITY

PROBABILITY OF LUCKY GUESSES

After 1st switch :
1 : 2

After 2nd switch :
1 : 4

After 3rd switch :
1 : 8

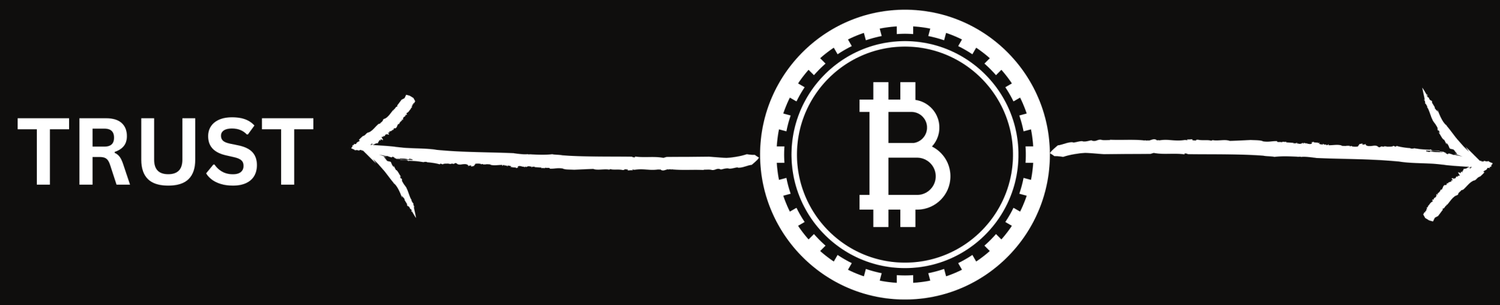
After 4th switch :
1 : 16

After 5th switch :
1 : 32

After 6tth switch :
1 : 64

After 7th switch :
1 : 128

The probability of lying is less then one



Zero-Konwledge Proof

Applications of Zero-Knowledge Proofs

Privacy-Focused Cryptocurrencies:

- *Zero-knowledge proofs are utilized in cryptocurrencies like Zcash to enhance transaction privacy.*

Authentication Protocols:

- *Secure authentication processes can employ zero-knowledge proofs to verify identity without revealing passwords.*

VARIANTS OF ZERO-KNOWLEDGE PROOFS

Zero-Knowledge Proof of Knowledge (ZKPoK):

Zero-Knowledge Proof of Existence (ZKPoE):

Zero-Knowledge Proof of Possession (ZKPoP):

THANKYOU