Authenticated Input: A Challenge For Bridges

Christian Lewe

2026-07-22

Alpen Labs

The Problem

Bridge Withdrawal

Alice (Bridge)

Bob

Bridge Withdrawal

Alice (Bridge)

Bob

Bridge Withdrawal

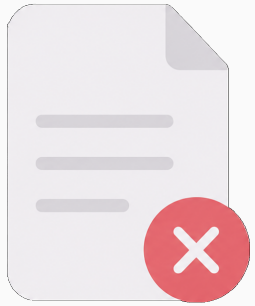
Alice (Bridge)

Bob

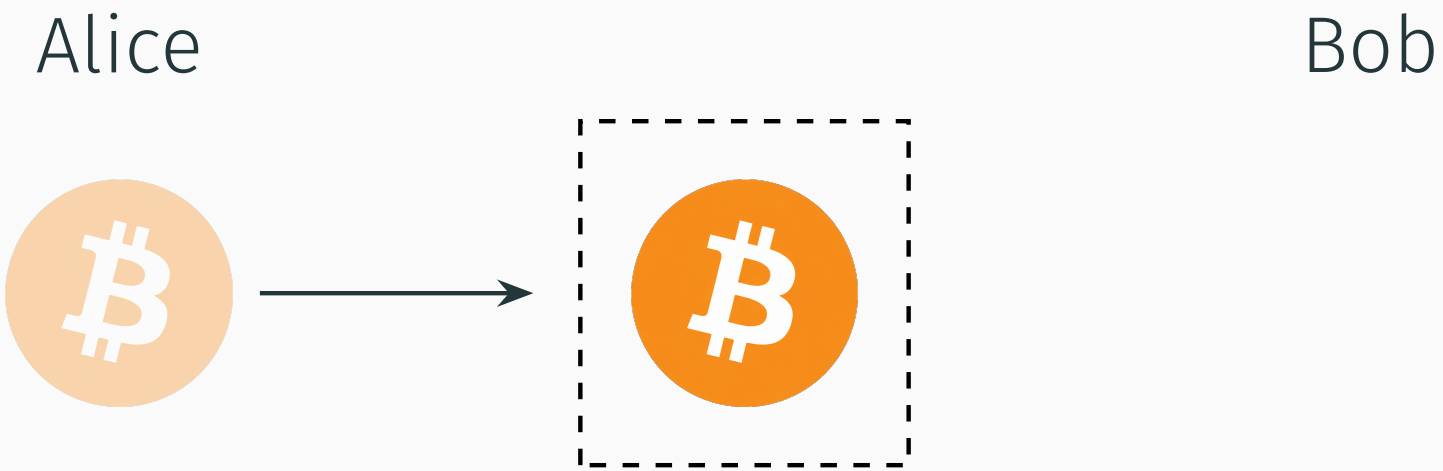
Bridge Withdrawal

Alice (Bridge)

Bob



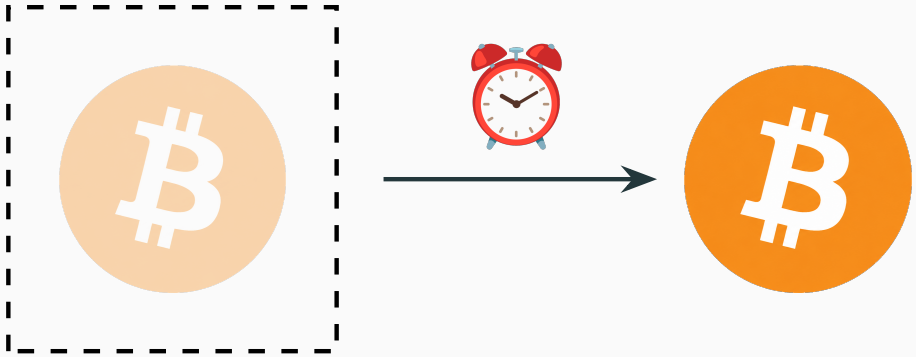
Optimistic Verification



Optimistic Verification

Alice

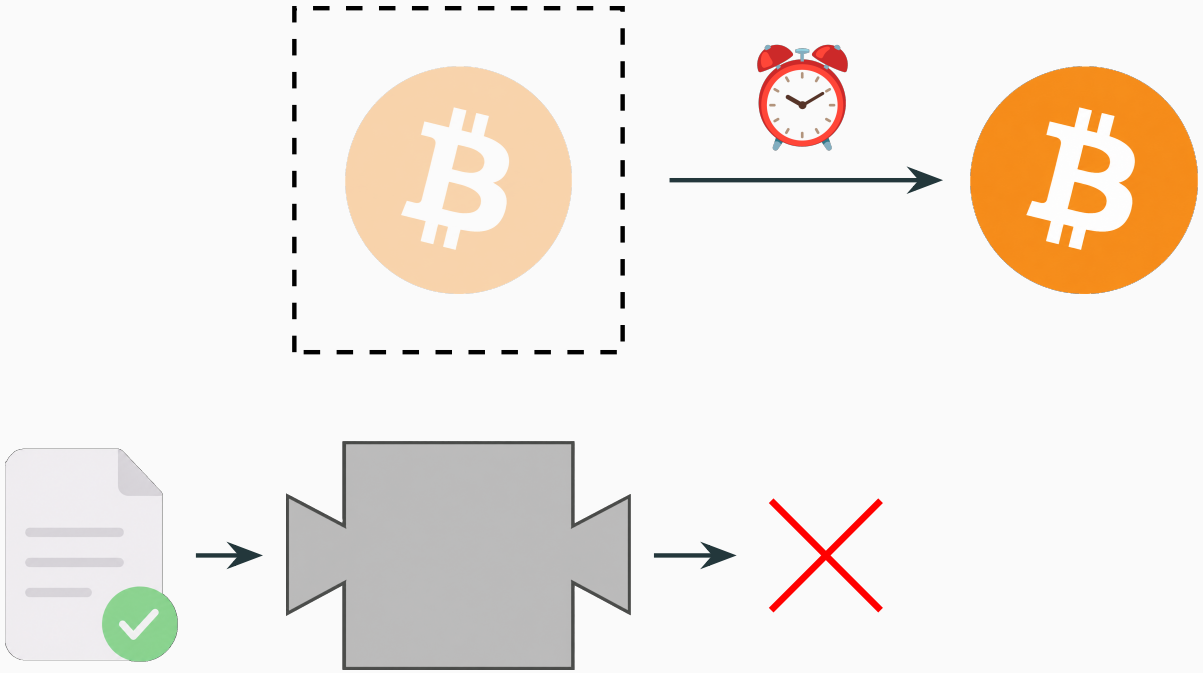
Bob



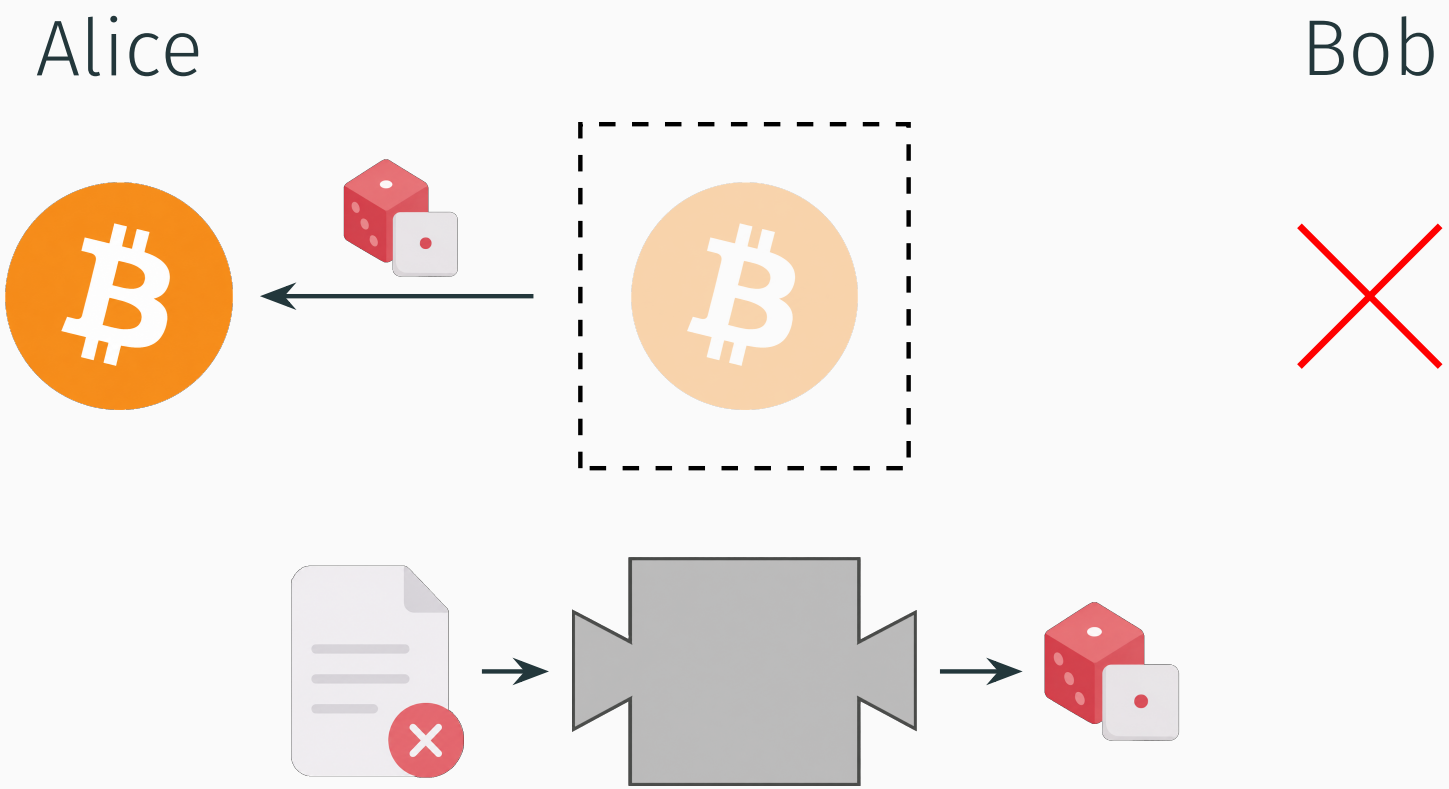
Optimistic Verification

Alice

Bob



Optimistic Verification



Cryptographic Black Box

Box must use Bob's exact bytes.

`OP_CHECKSIG` signs transaction, not bytes.

We emulate signing with existing opcodes.

Lamport Signatures

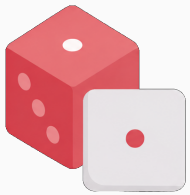
Lamport Bit Assignment

0 

1 

Lamport Bit Assignment

$$0 = f(\ \ )$$



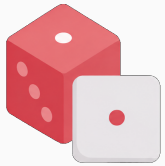
$$1 = f(\ \ )$$

Lamport Locking Script

Give me x such that

$$\text{hash}(x) = \text{  }, \text{ or}$$

$$\text{hash}(x) = \text{  }$$

$$x = \text{  } \quad \text{or} \quad x = \text{  }$$

Adaptor Signatures

Alice Sells Her UTXO

Alice has UTXO.

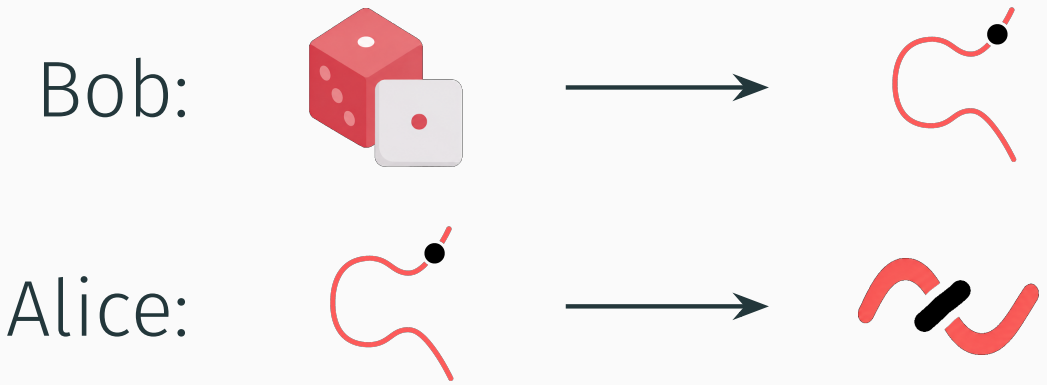
Alice can spend UTXO at any time.

Alice sells UTXO to Bob for  .

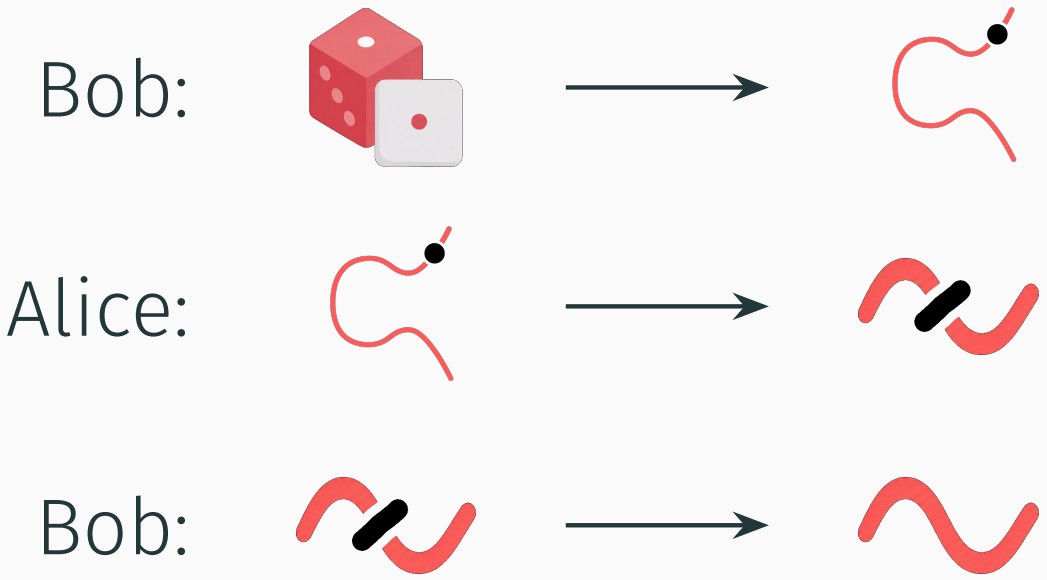
Using Adaptor Signatures

Bob:  

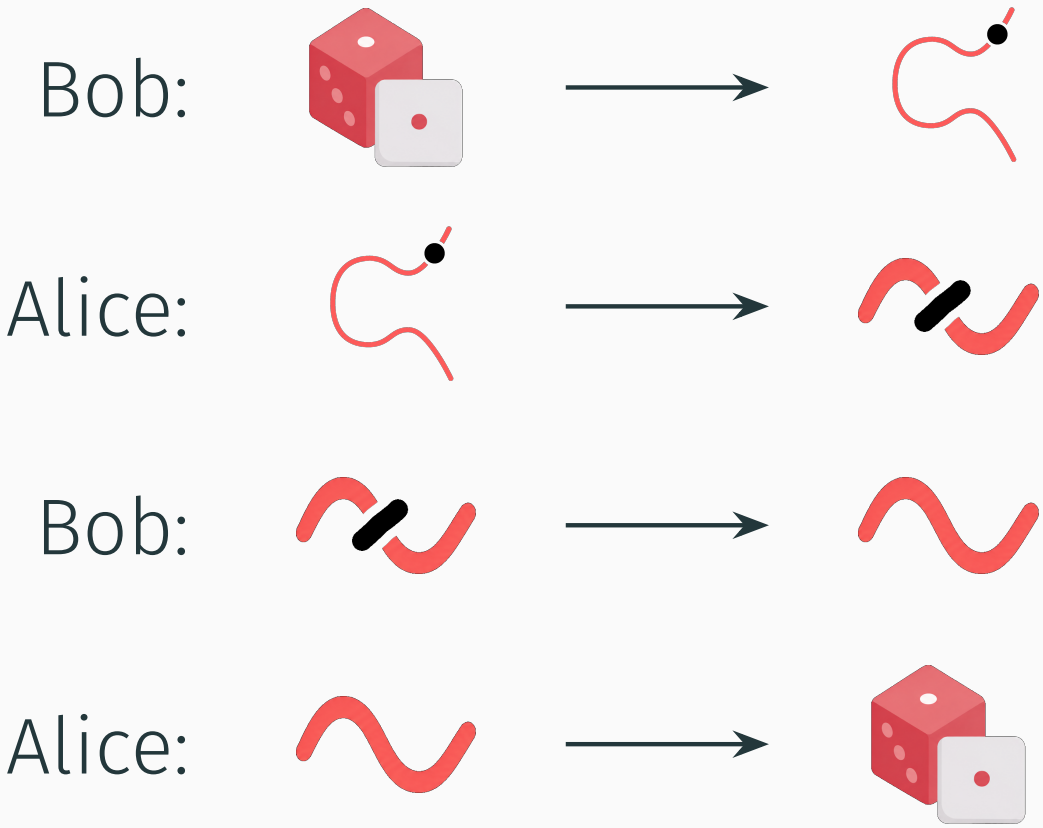
Using Adaptor Signatures



Using Adaptor Signatures



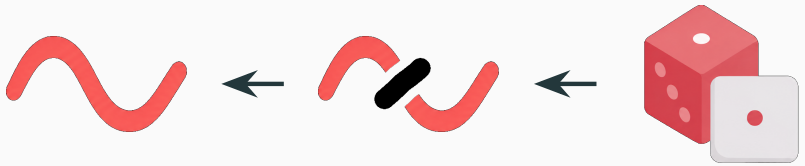
Using Adaptor Signatures



Adaptor Locking Script

Give me x such that

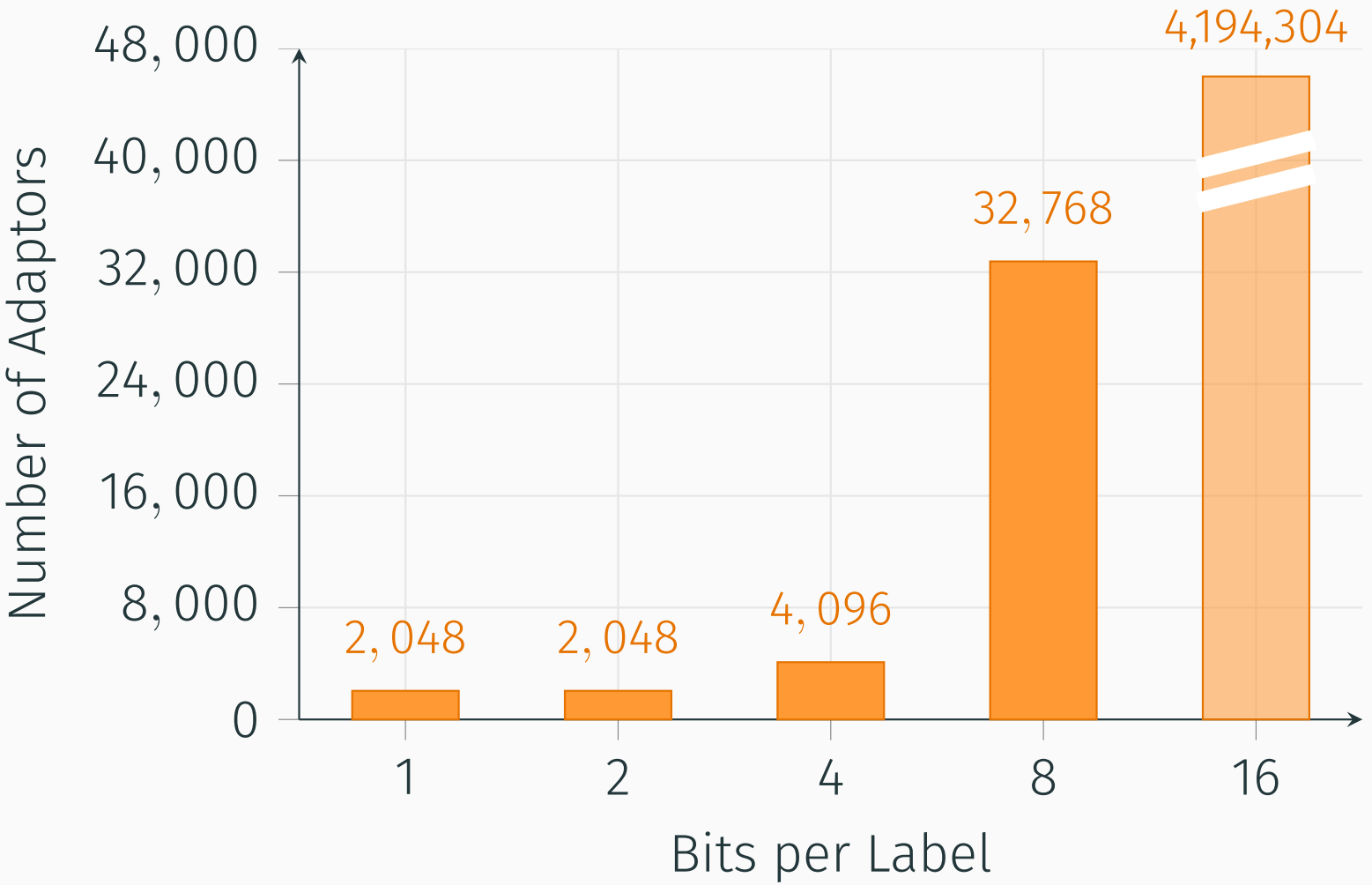
x is signature from Alice

$x =$  , or

$x =$ 

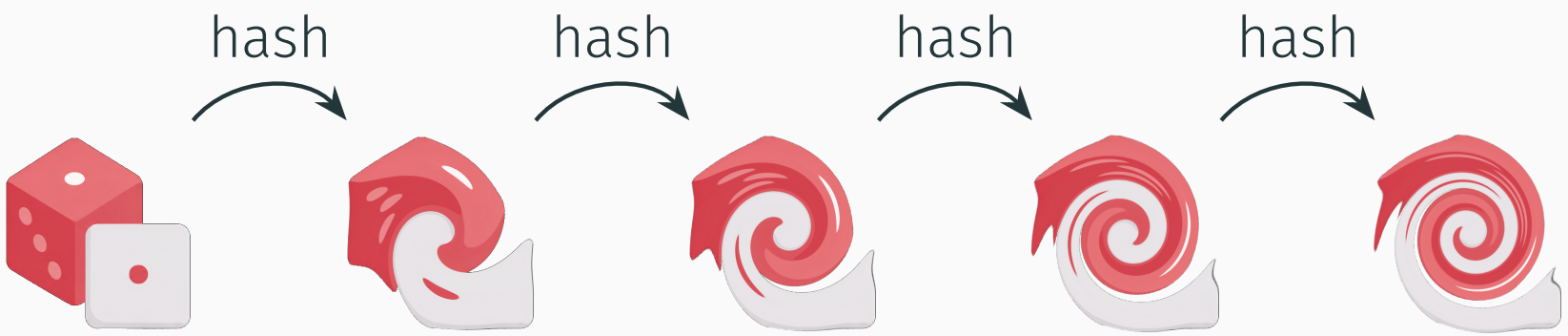
Wide Labels

Adaptors For a 128 Byte Message



Winternitz Signatures

Hash Chain



Winternitz 2-Bit Assignment

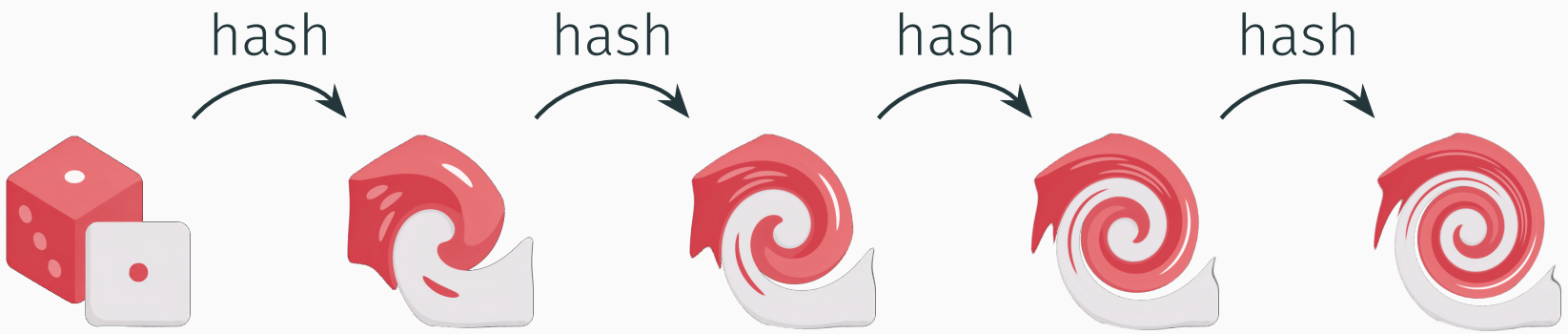
$$0 = f(\ \ )$$

$$1 = f(\ \ )$$

$$2 = f(\ \ )$$

$$3 = f(\ \ )$$

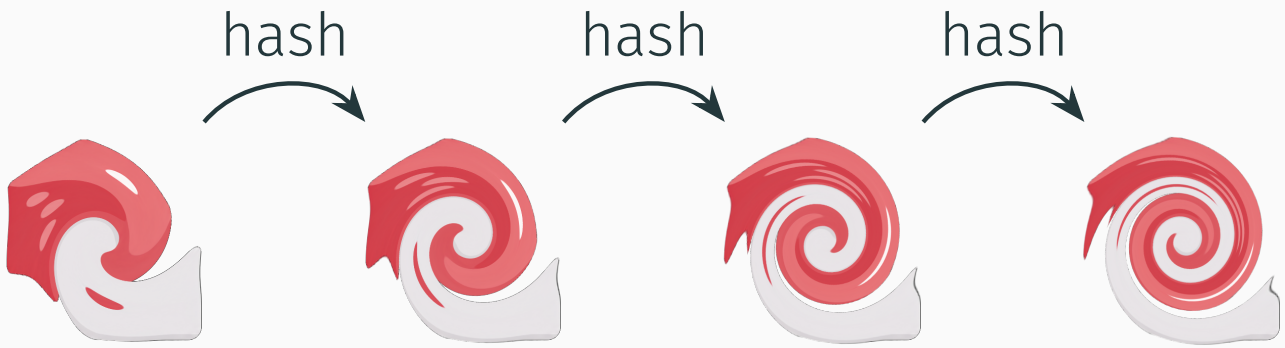
Winternitz Locking Script $d = 0$



||

X

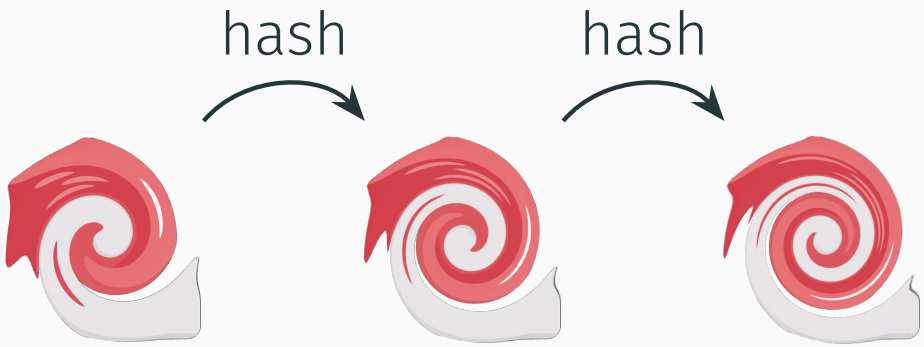
Winternitz Locking Script $d = 1$



$||$

X

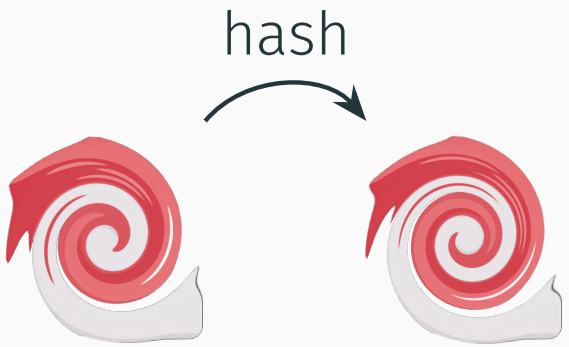
Winternitz Locking Script $d = 2$



||

X

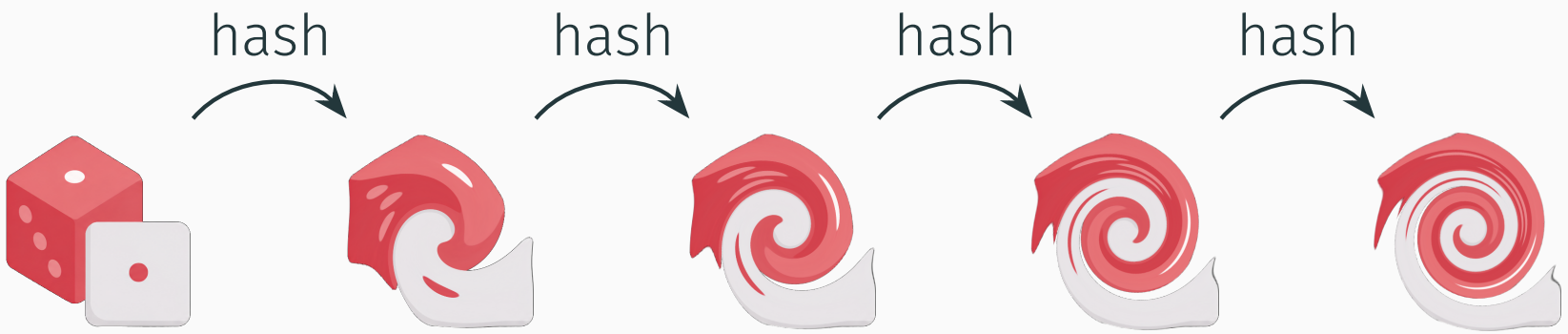
Winternitz Locking Script $d = 3$



$||$

X

Malleability Issue Without Checksum



$\|$ $\|$ $\|$ $\|$

$\mathsf{sig}(d = 0)$ $\mathsf{sig}(d = 1)$ $\mathsf{sig}(d = 2)$ $\mathsf{sig}(d = 3)$

Winternitz And Black Box

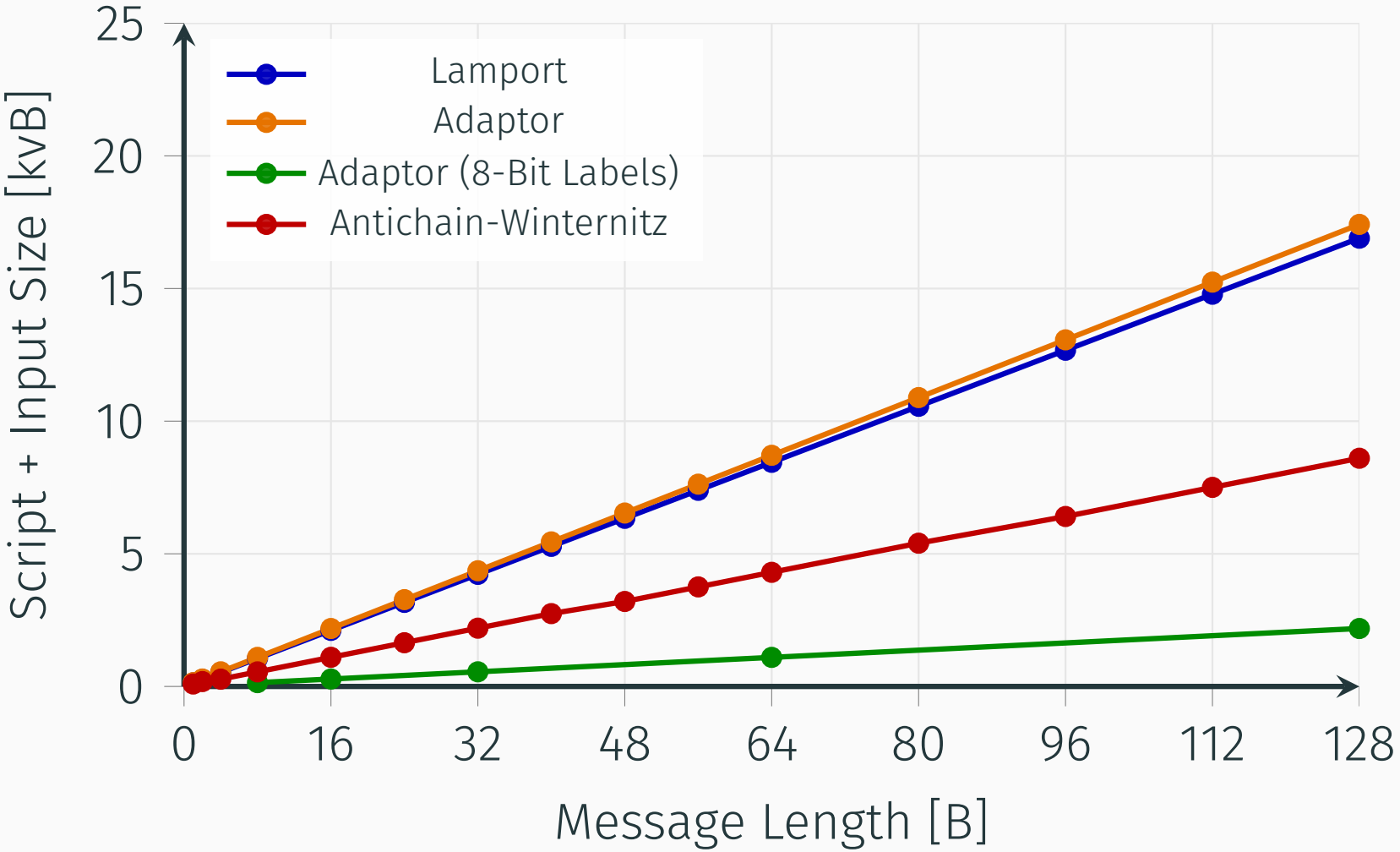
Winternitz	
Checksum for message	
Message fixed	✓
Digit malleable	✗
Black box incompatible	✗

Winternitz And Black Box

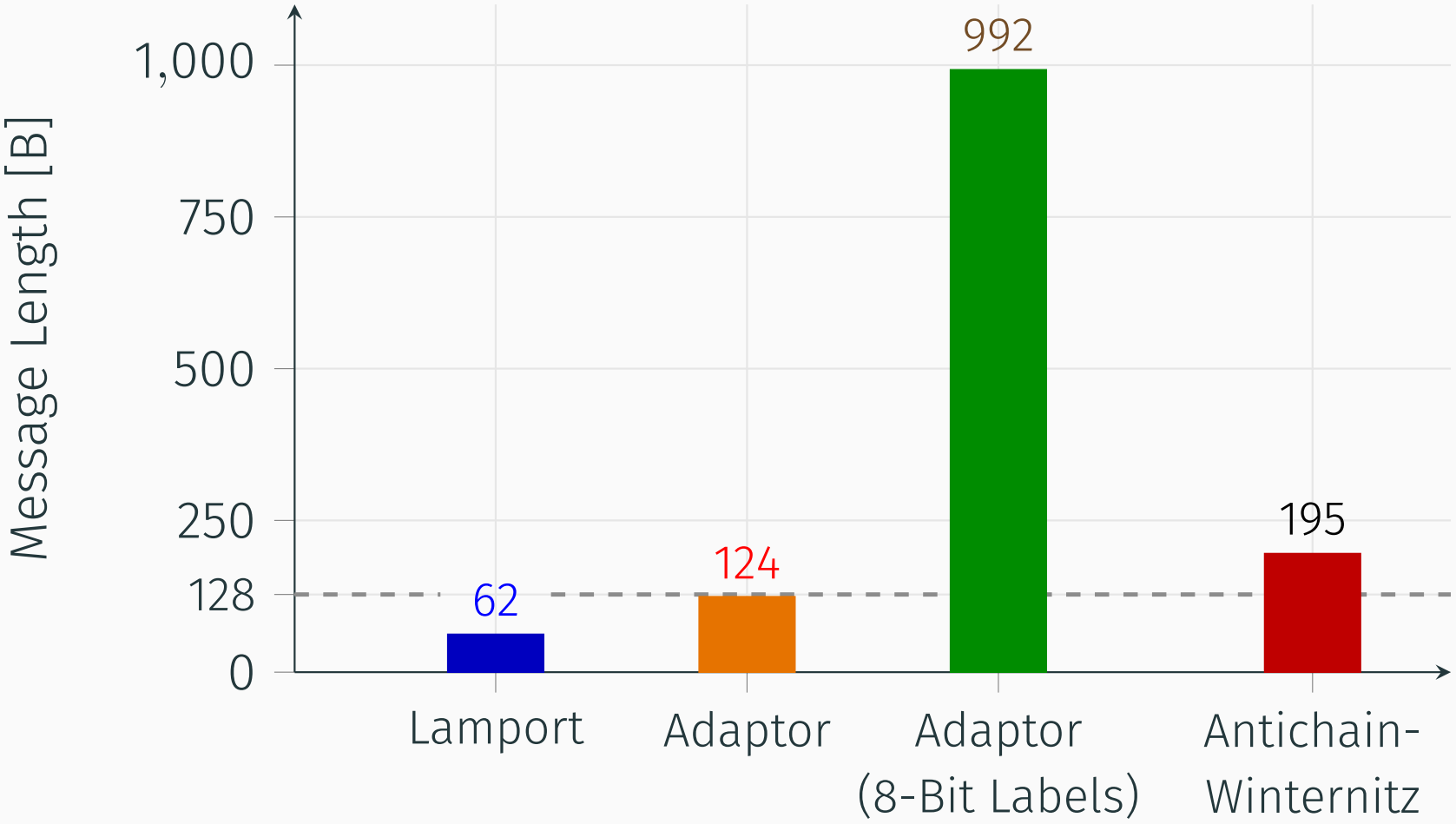
Winternitz	Antichain-Winternitz
Checksum for message	Checksum for digit
Message fixed ✓	Message fixed ✓
Digit malleable ✗	Digit fixed ✓
Black box incompatible ✗	Black box compatible ✓

Comparison

Transaction Input Size



Standardness Limits Per Txin



Conclusion

Conclusion

No arbitrary signing on Bitcoin today.

Wide Labels: less onchain, exponential offchain.

New: Antichain-Winternitz.

When to Use Which Scheme

Adaptor (8-Bit Labels)

✓ smallest onchain

⚠️ interactivity ok, offchain ok

Antichain-Winternitz

✓ simpler setup, non-interactive, 1/4 Lamport

⚠️ 4× onchain ok

Thank you!

One Key Many Signatures

A public key can match many signatures.

We can make many adaptors.

The locking script doesn’t grow!

Reveal Many Bits Per Signature