

A glowing blue padlock with a Bitcoin symbol on a starry background. The padlock is the central focus, rendered in a vibrant blue color with a metallic texture. The Bitcoin symbol is prominently displayed on the front of the padlock. The background is a dark, starry space with a gradient of blue and orange light, suggesting a digital or cryptographic theme. The text "encrypted mempools" is overlaid on the bottom half of the image in a white, sans-serif font.

encrypted mempools

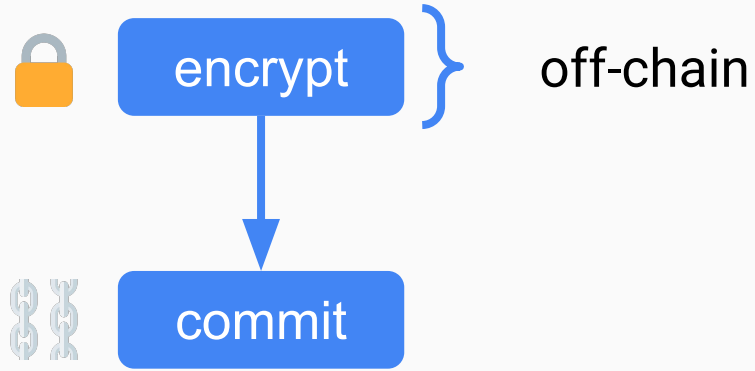
- 1) *"what"* basics
- 2) *"why"* motivation
- 3) *"how"* metadata

1) *"what"* basics

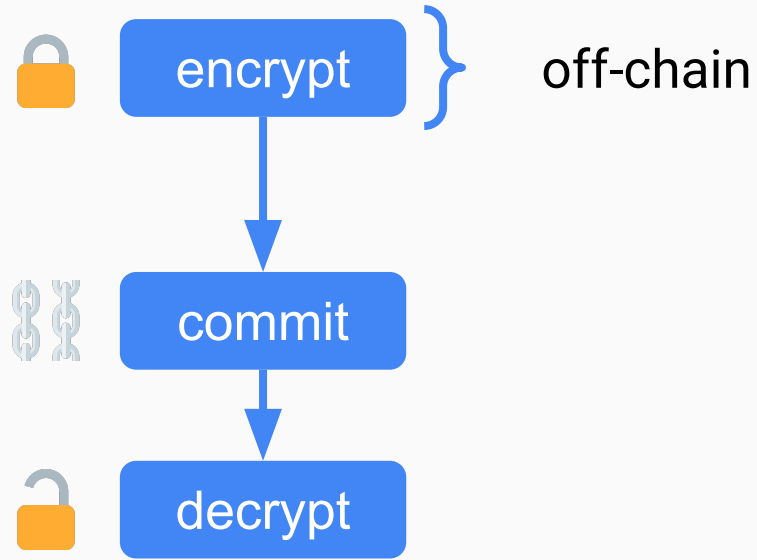
2) *"why"* motivation

3) *"how"* metadata

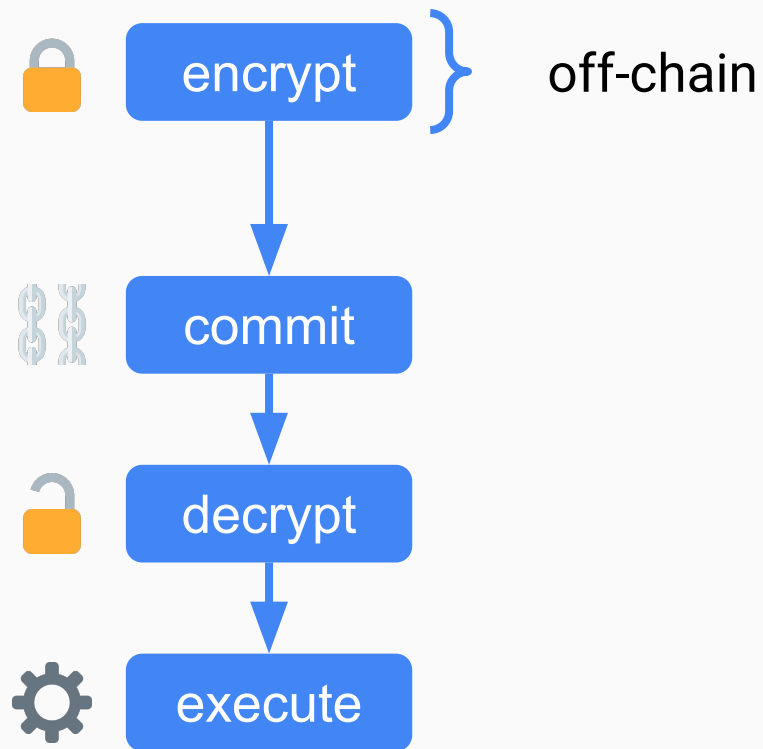




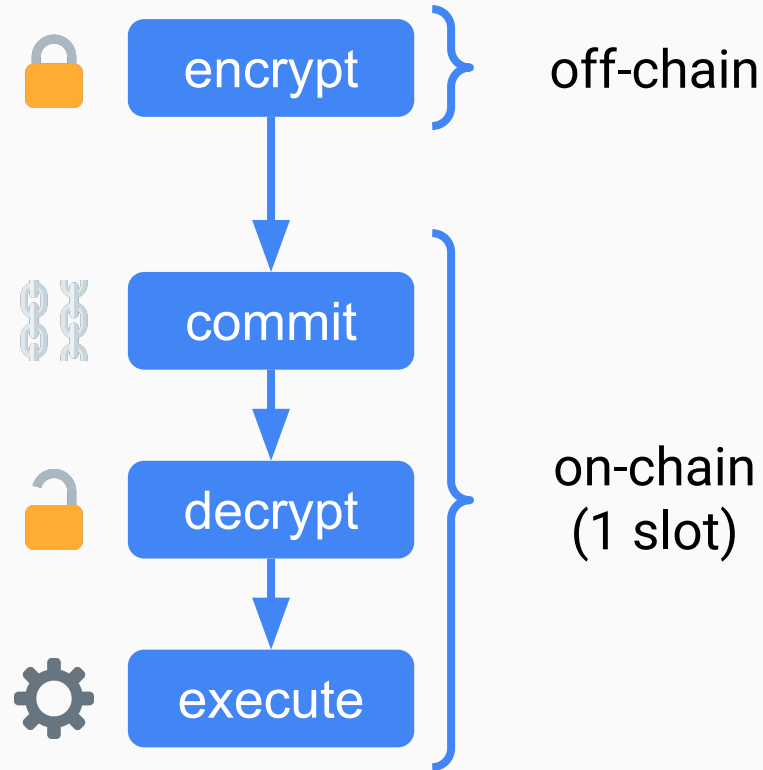
simple framework



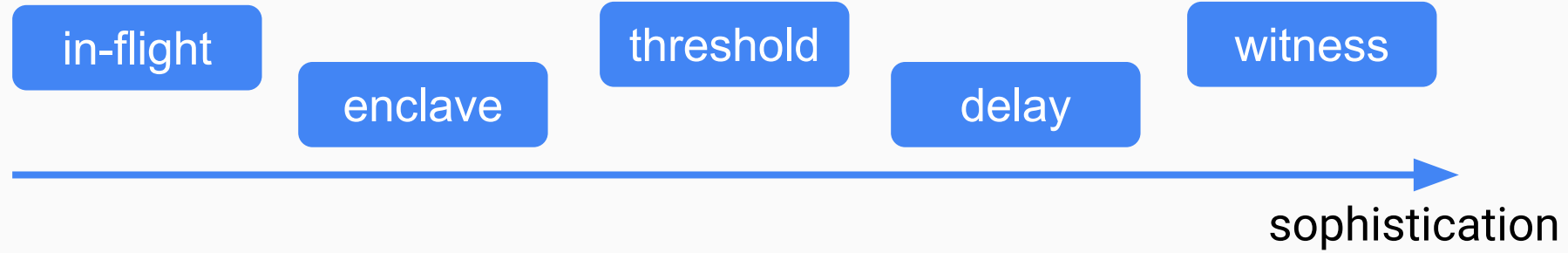
simple framework



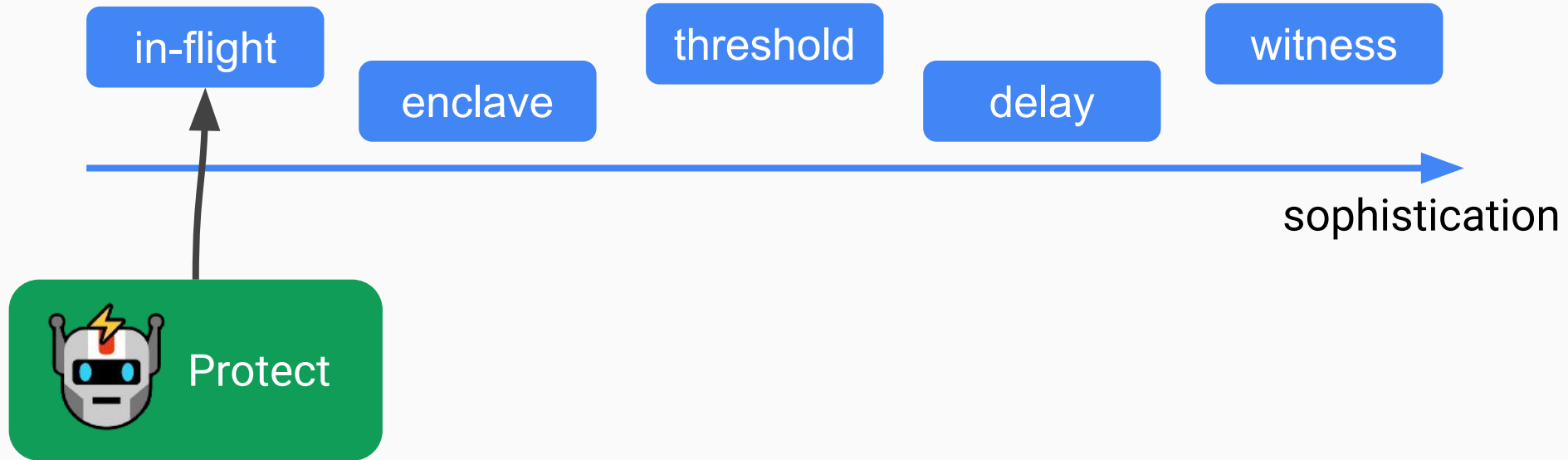
simple framework



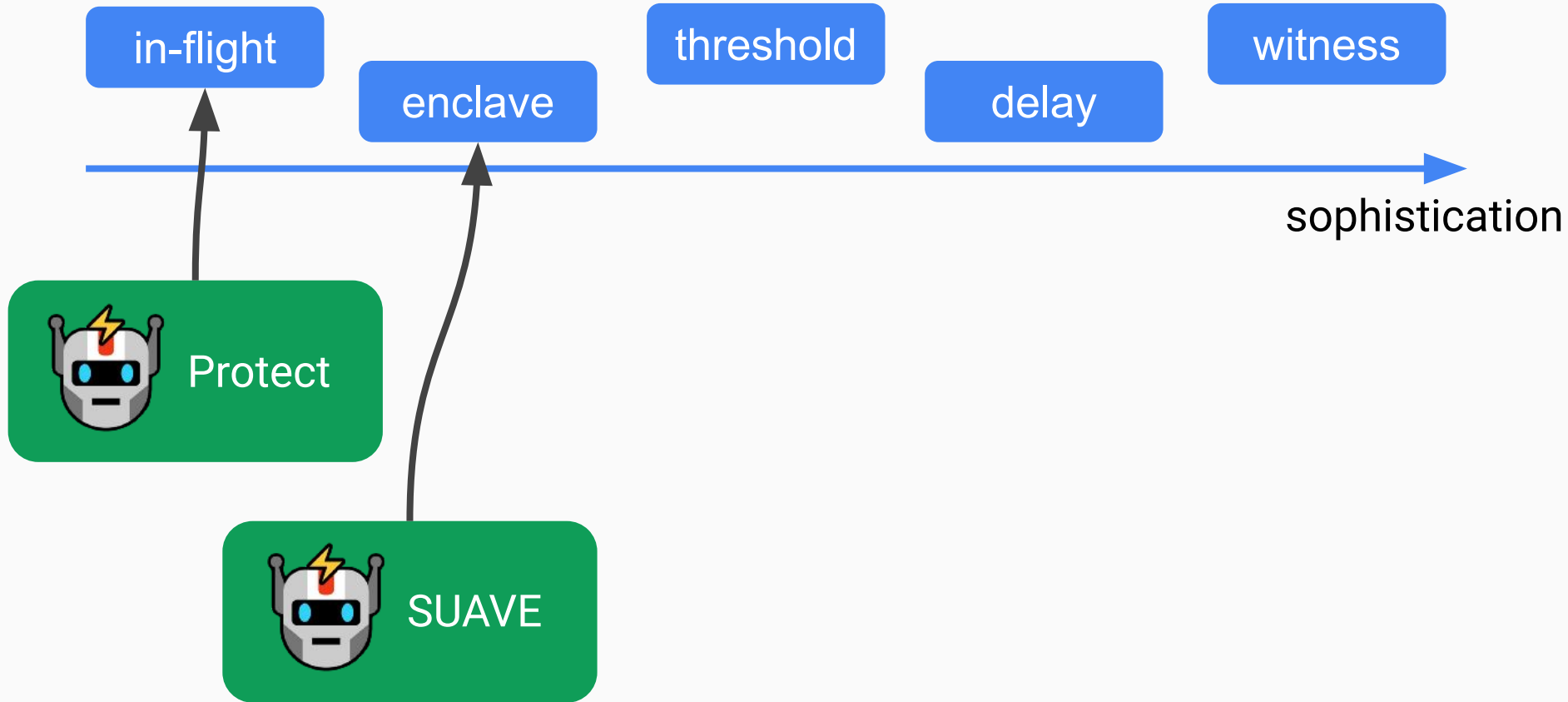
guaranteed decryption



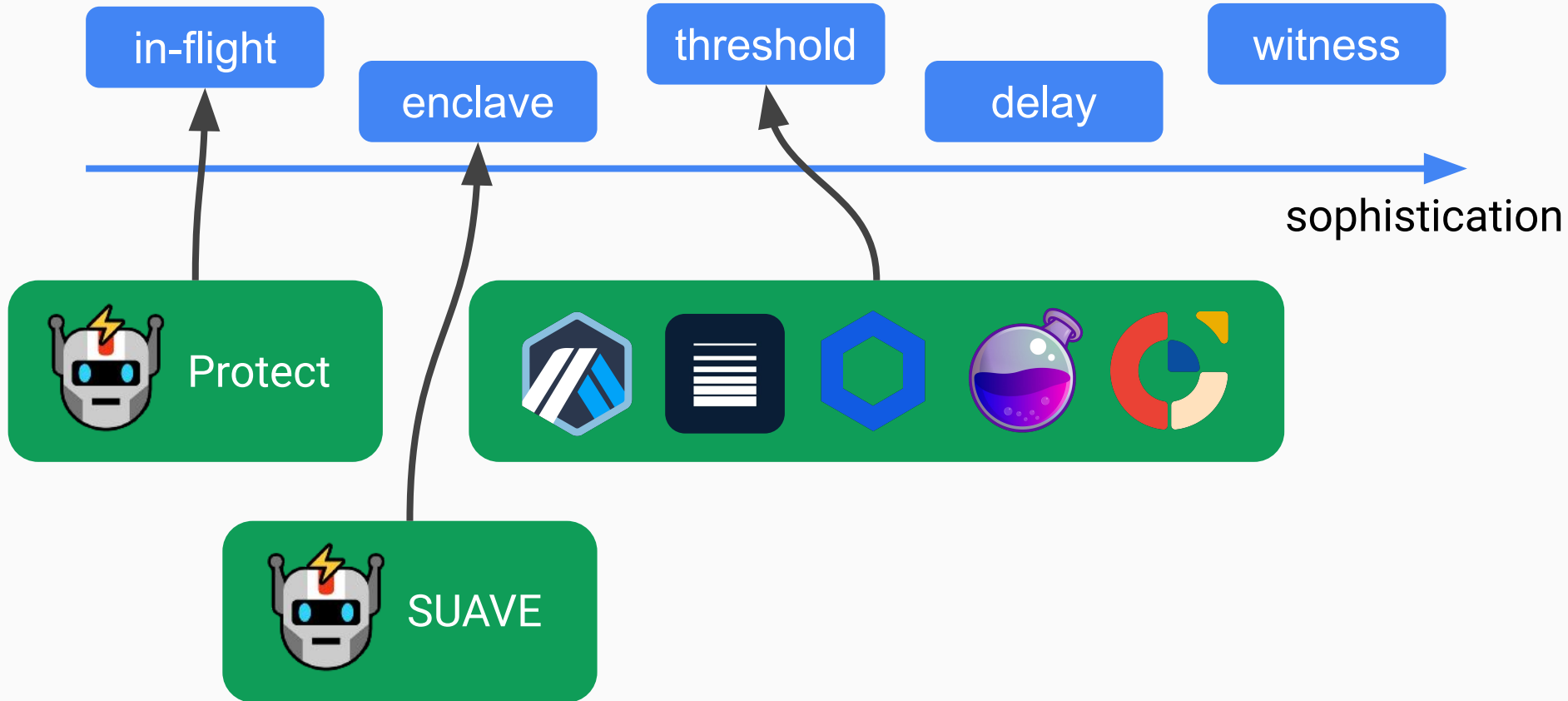
guaranteed decryption



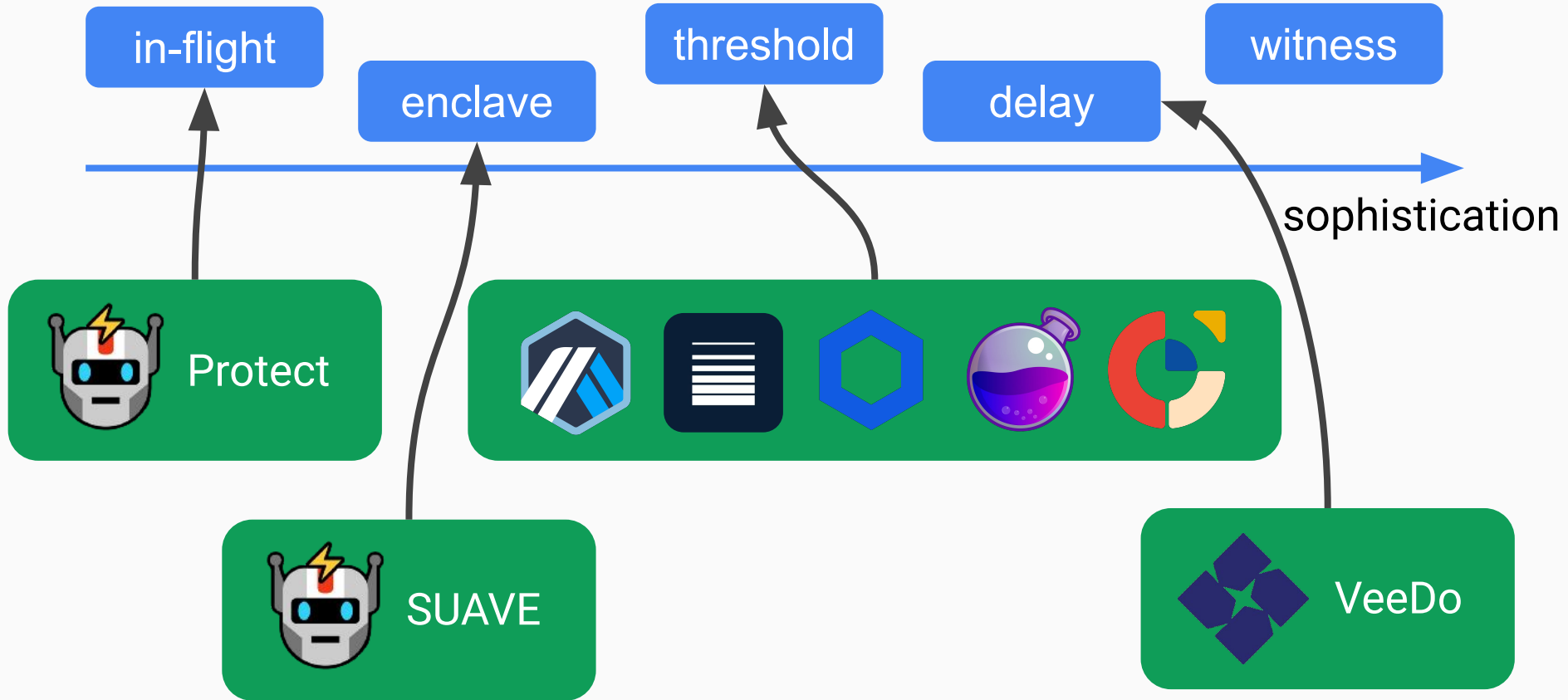
guaranteed decryption






guaranteed decryption



guaranteed decryption



	in-flight	enclave	threshold
ready?			

	in-flight	enclave	threshold	delay
ready?				 SOON

	in-flight	enclave	threshold	delay	witness
ready?				 SOON	

encryption(\mathbf{m}_1), encryption(\mathbf{m}_2)

encryption(\mathbf{m}_1), encryption(\mathbf{m}_2)



encryption($\mathbf{f}(\mathbf{m}_1, \mathbf{m}_2)$)

homomorphism

encryption(m_1), encryption(m_2)

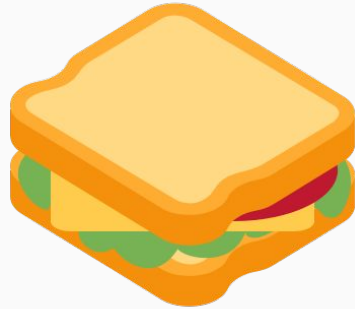


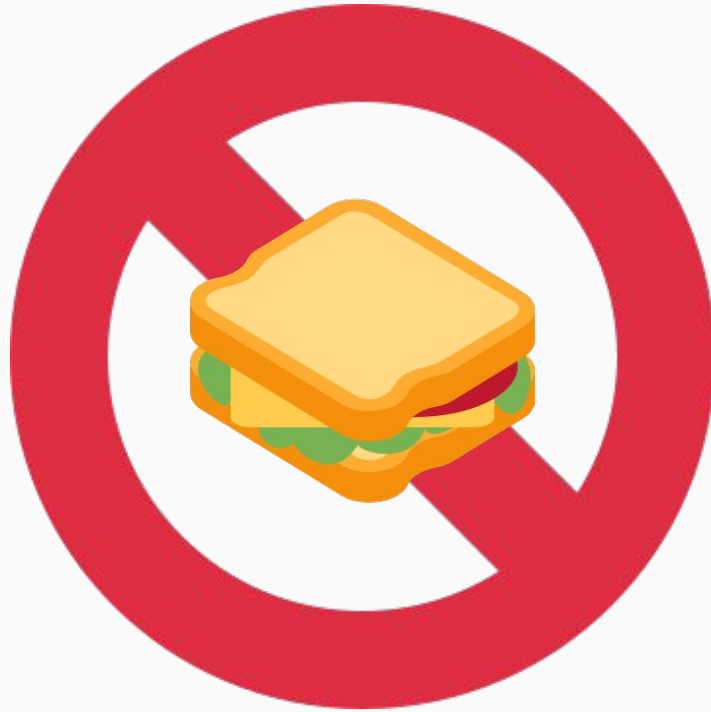
encryption($f(m_1, m_2)$)

	in-flight	enclave	threshold	delay	witness
ready?				SOON	
			SOON	SOON ?	

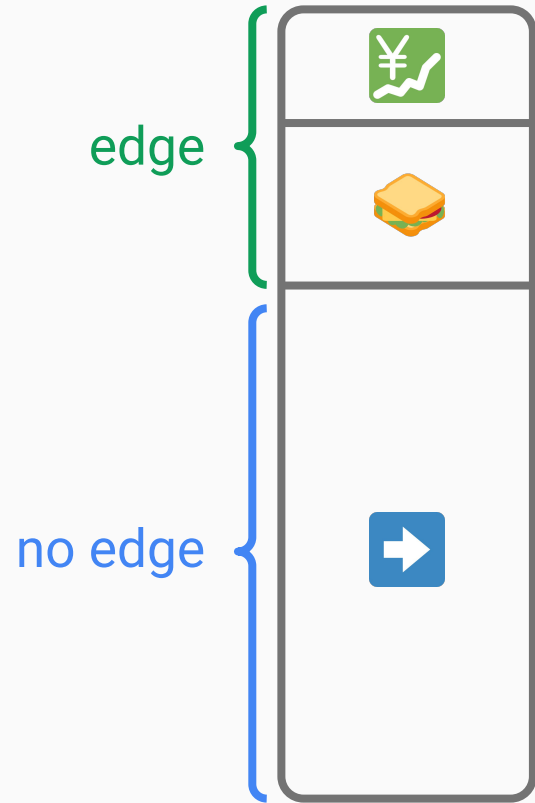
- 1) *"what"* basics
- 2) *"why"* motivation
- 3) *"how"* metadata

problem 1—frontrunning

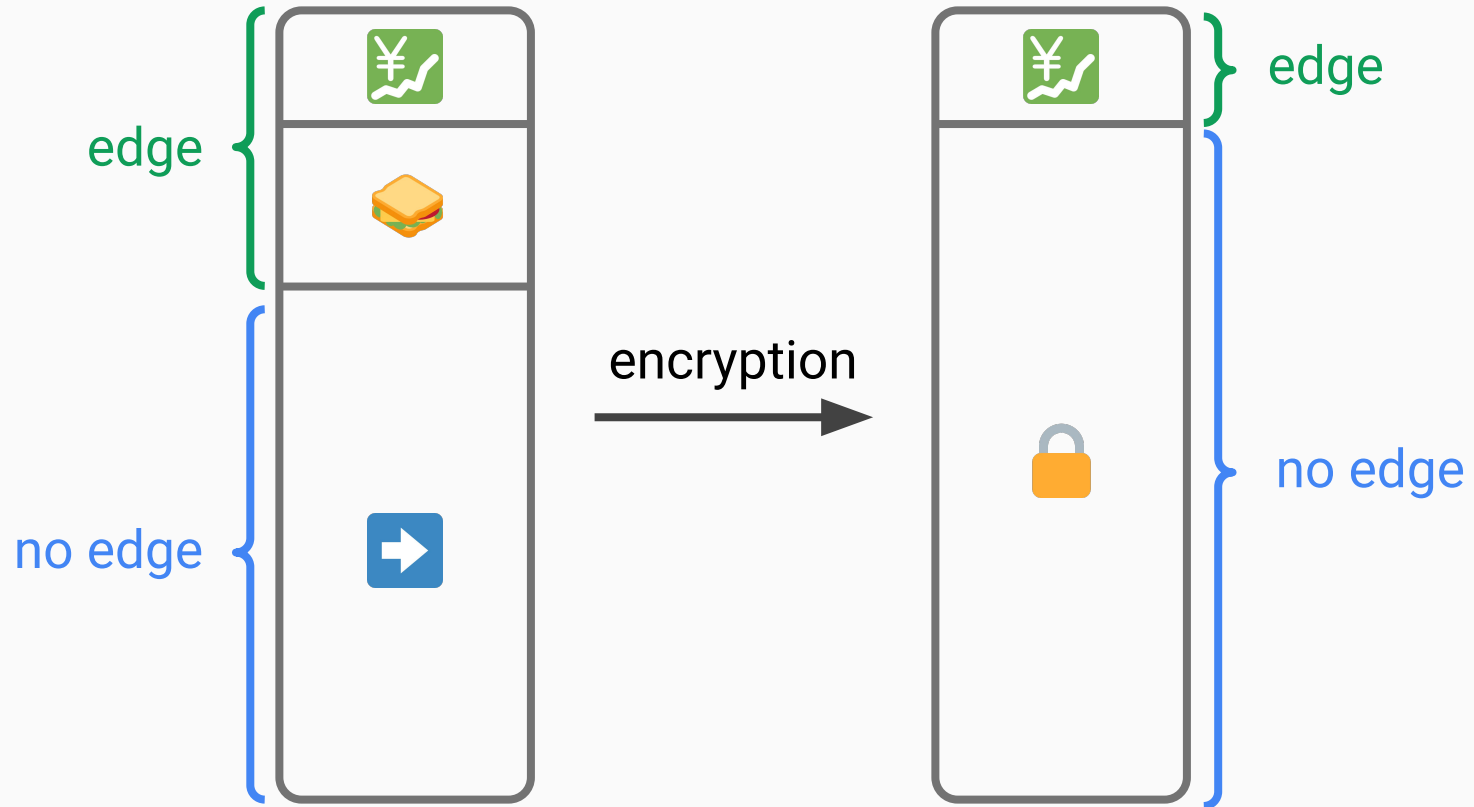




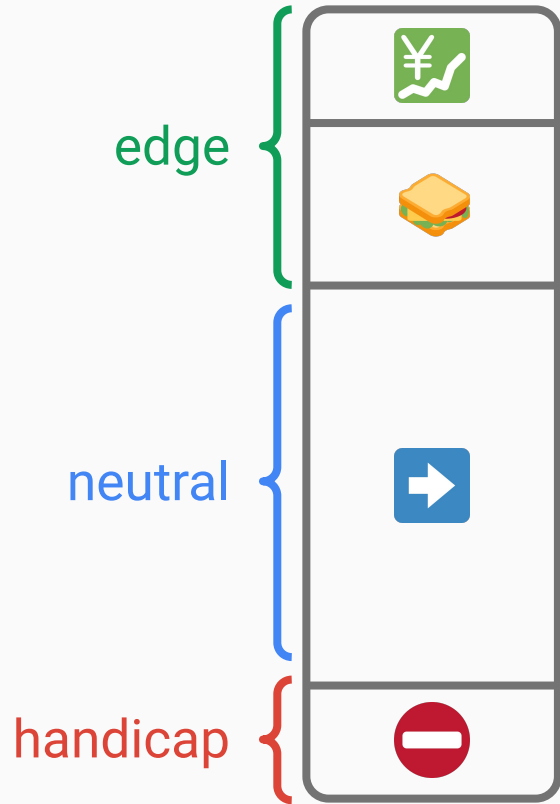
problem 1b—centralisation



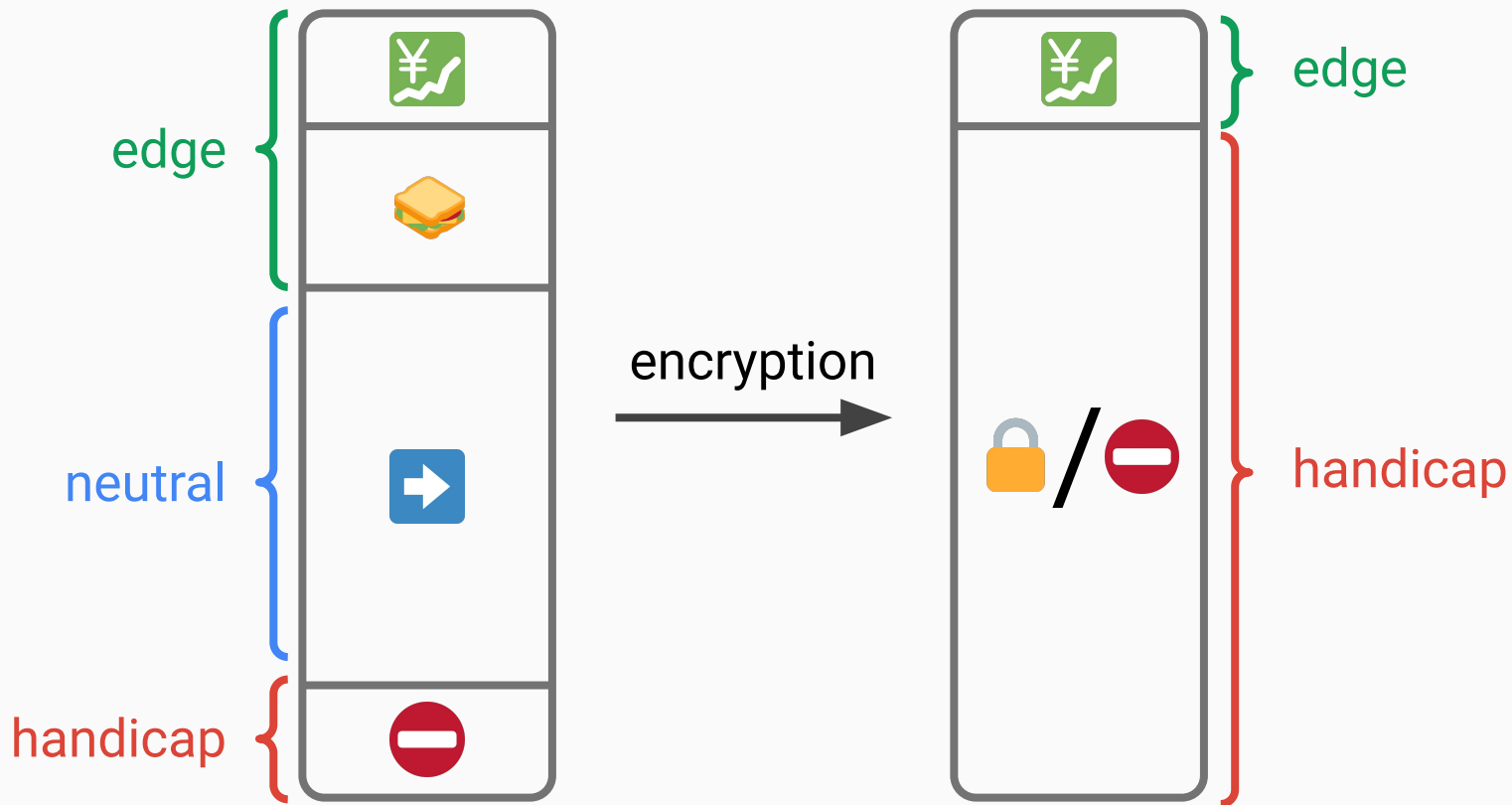
problem 1b—centralisation



problem 2—censorship



problem 2—censorship



- 1) *"what"* basics
- 2) *"why"* motivation
- 3) *"how"* metadata

transaction metadata



IP address



size



sender



tip

transaction metadata



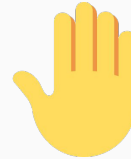
IP address



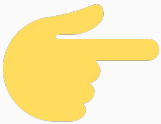
gas price



size



gas limit



sender



nonce

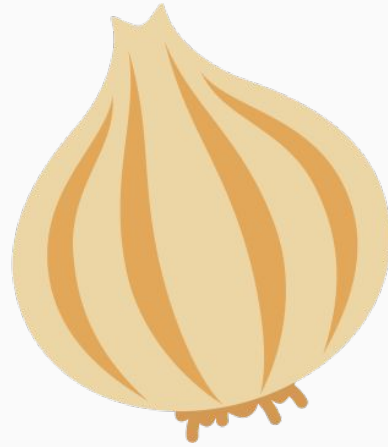


tip



signature

IP address



private broadcast
(e.g. Tor)



public input: tx ciphertext

private witness: tx plaintext

zk statement: tx ciphertext valid



public input: tx ciphertext + state root

private witness: tx plaintext + sender pubkey Merkle proof

zk statement: tx ciphertext valid + Merkle proof valid



public input: tx ciphertext + state root

private witness: tx plaintext + sender pubkey Merkle proof

zk statement: tx ciphertext valid + Merkle proof valid

signature valid

public input: tx ciphertext + state root

private witness: tx plaintext + sender balance Merkle proof

zk statement: tx ciphertext valid + Merkle proof valid

public input: tx ciphertext + state root

private witness: tx plaintext + sender balance Merkle proof

zk statement: tx ciphertext valid + Merkle proof valid

sufficient sender balance



public input: tx ciphertext + state root

private witness: tx plaintext + nonce Merkle proof

zk statement: tx ciphertext valid + Merkle proof valid

new nonce valid

nonce



- public input:** tx ciphertext + state root + replay tag
 - private witness:** tx plaintext + nonce Merkle proof
 - zk statement:** tx ciphertext valid + Merkle proof valid
- new nonce valid
- replay tag = $H(\text{nonce}, \text{private key})$

nonce



public input: tx ciphertext + state root + replay tag + slot

private witness: tx plaintext + nonce Merkle proof

zk statement: tx ciphertext valid + Merkle proof valid

new nonce valid

replay tag = $H(\text{nonce}, \text{private key}, \text{slot})$

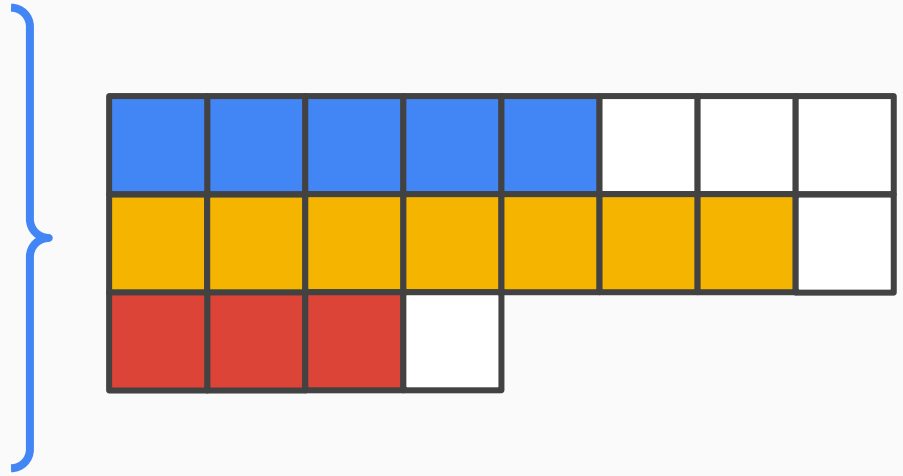
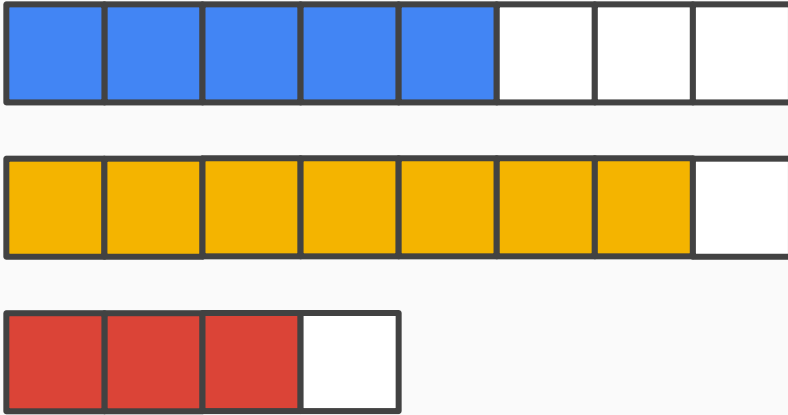
size 



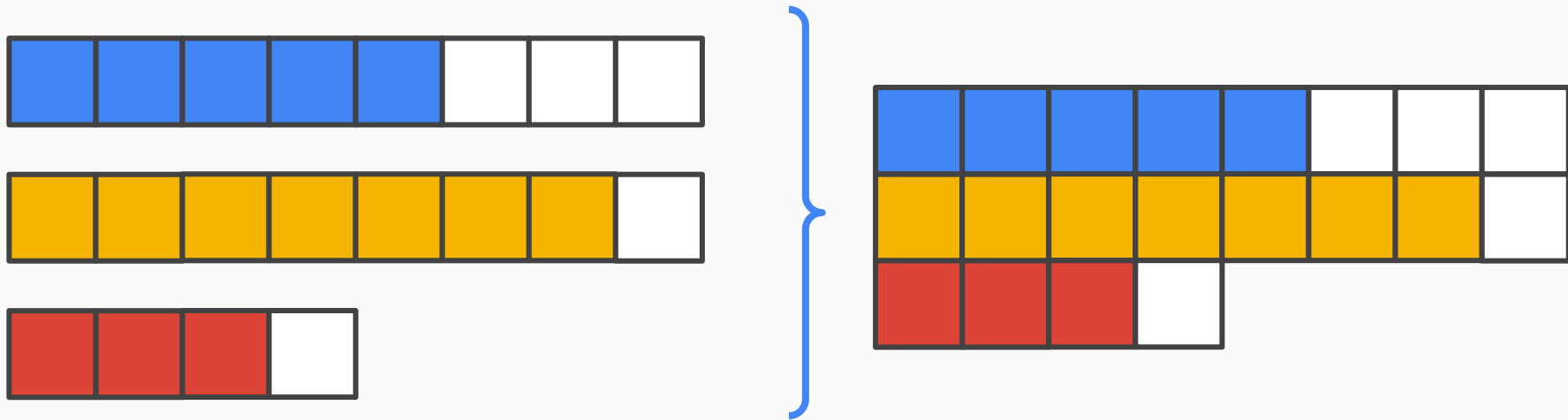
idea 1—pad to power of two



idea 1—pad to power of two

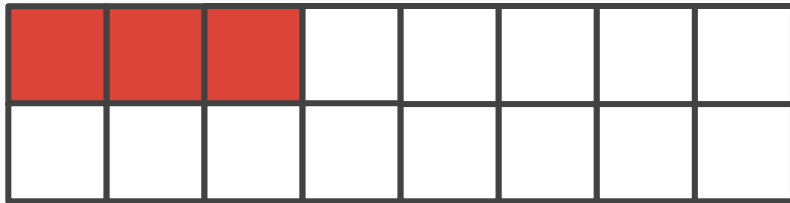


idea 1—pad to power of two



problem 1: imperfect packing

problem 2: imperfect privacy



idea 2—use homomorphism



blue	blue	blue	blue	blue	white	white	white
white	white	white	white	white	white	white	white

yellow	yellow	yellow	yellow	yellow	yellow	yellow	white
white	white	white	white	white	white	white	white

red	red	red	white	white	white	white	white
white	white	white	white	white	white	white	white



idea 2—use homomorphism

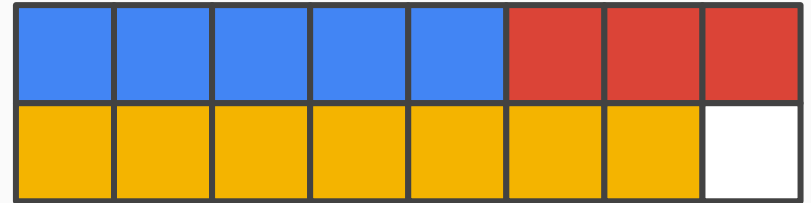
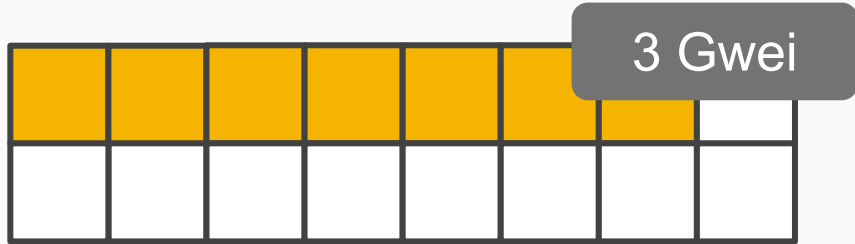
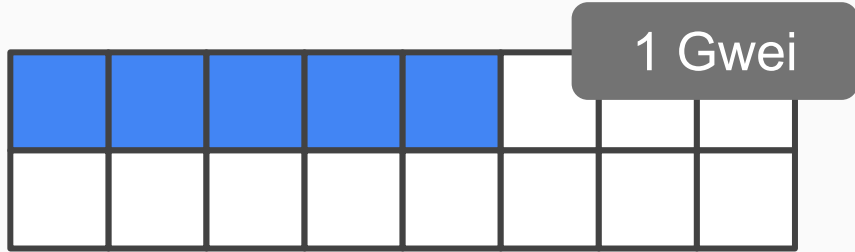


blue	blue	blue	blue	blue	yellow	yellow	yellow
yellow	yellow	yellow	yellow	red	red	red	white

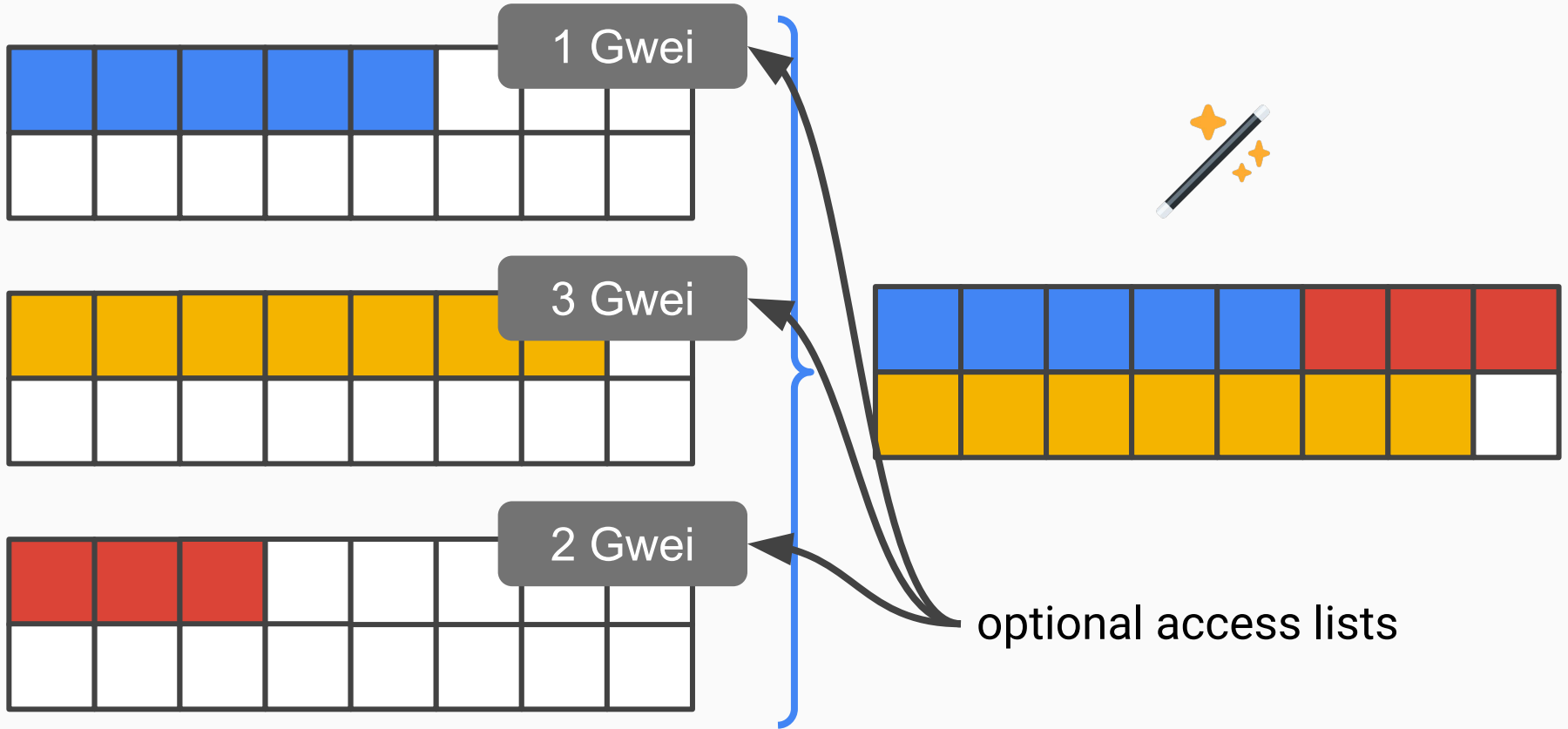
ordering by fee



ordering by fee



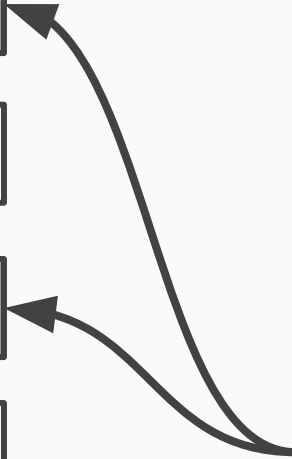
ordering by fee



timestamp

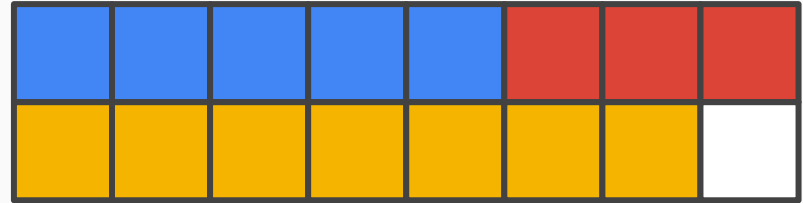
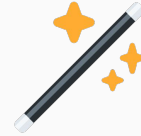


timestamp



dummy transactions

timestamp





thank you :)

justin@ethereum.org

commitment strength

