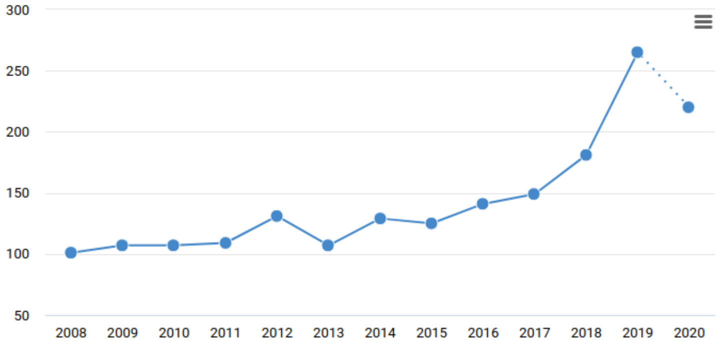
The Zero-Knowledge Proof Revolution

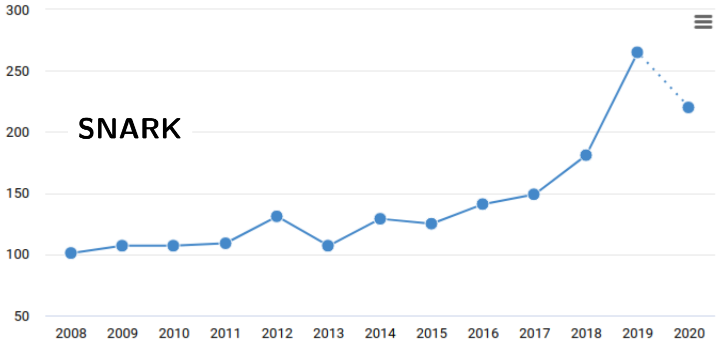
interesting insights about

Alan Szepieniec
alan@asdm.gmbh

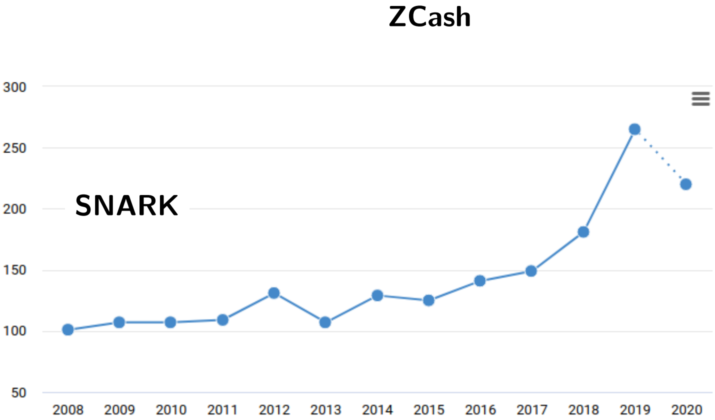
Revolution


300
250
200
150
100
50
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020

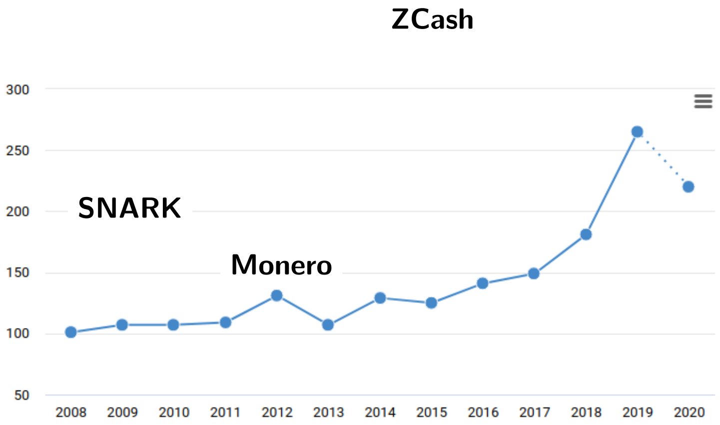
Revolution


SNARK
300
250
200
150
100
50
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020

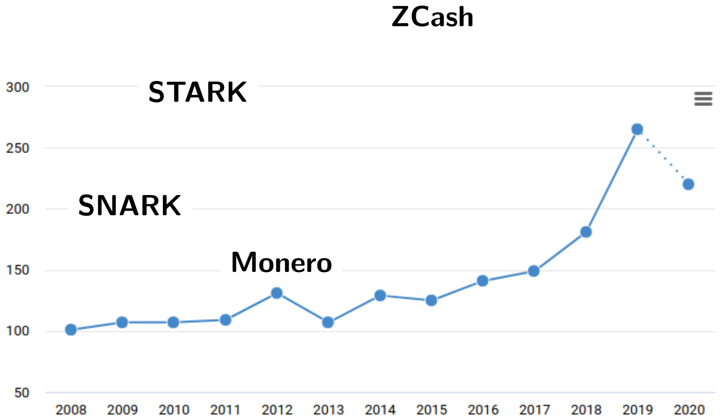
Revolution


ZCash
SNARK
300
250
200
150
100
50
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020

Revolution

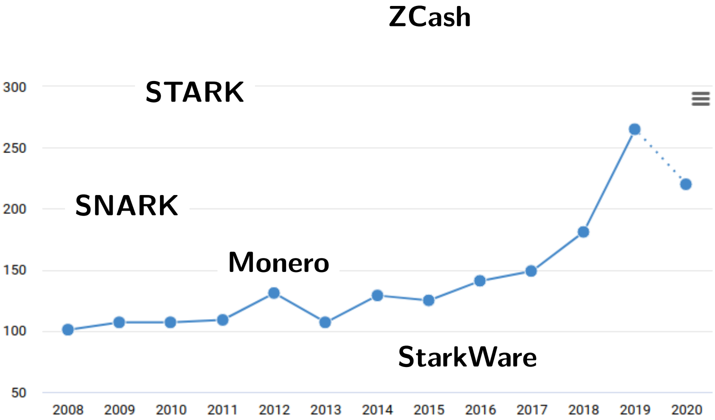

ZCash
SNARK
Monero
300
250
200
150
100
50
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020

Revolution

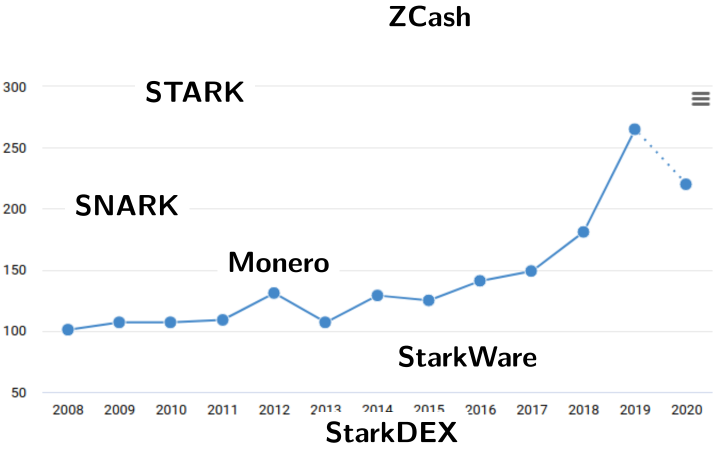


ZCash
STARK
SNARK
Monero
300
250
200
150
100
50
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020

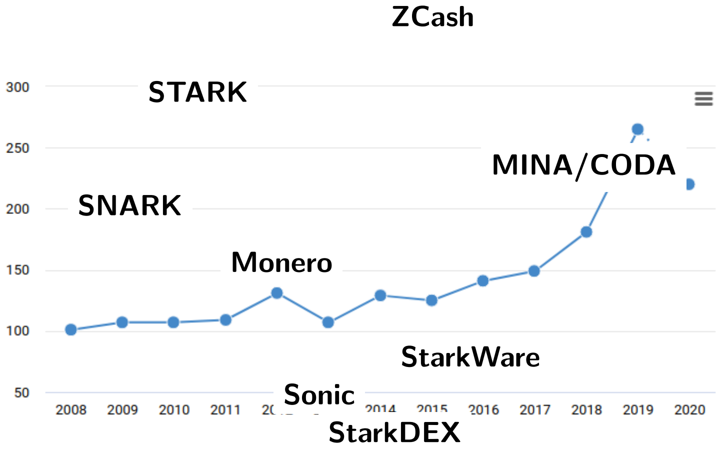
Revolution


ZCash
STARK
SNARK
Monero
StarkWare
300
250
200
150
100
50
2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

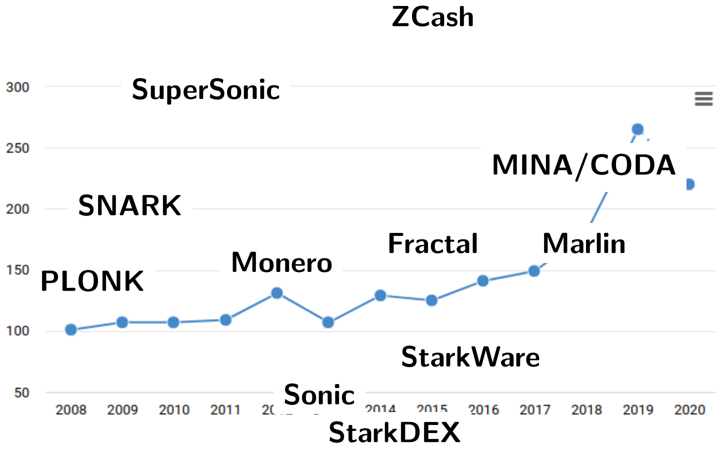
Revolution


ZCash
STARK
SNARK
Monero
StarkWare
StarkDEX
300
250
200
150
100
50
2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

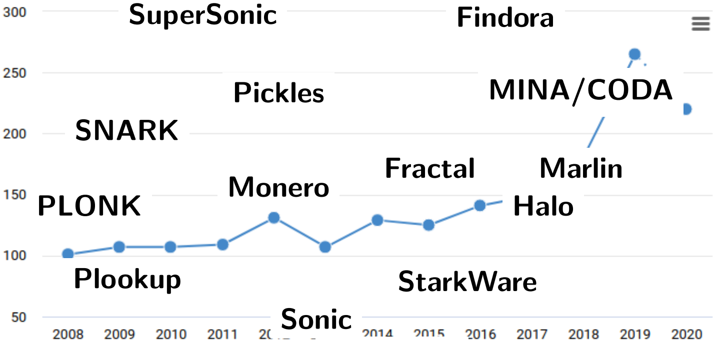
Revolution


ZCash
STARK
SNARK
MINA/CODA
Monero
StarkWare
Sonic
StarkDEX
300
250
200
150
100
50
2008
2009
2010
2011
2014
2015
2016
2017
2018
2019
2020

Revolution


ZCash
SuperSonic
MINA/CODA
SNARK
Fractal
Marlin
Monero
PLONK
StarkWare
Sonic
StarkDEX
300
250
200
150
100
50
2008
2009
2010
2011
2016
2017
2018
2019
2020

Revolution



ZCash

SuperSonic

Findora

Pickles

MINA/CODA

SNARK

Fractal

Marlin

Monero

PLONK

Halo

Plookup

StarkWare

Sonic

StarkDEX

QED-it

Questions

Why is there a ZKP Revolution?

What does it mean for
me / Bitcoin / cryptocurrencies?

~~How do ZKPs work?~~

What can ZKPs achieve?

What does the future hold?

Questions

Why is there a ZKP Revolution?

What does it mean for
me / Bitcoin / cryptocurrencies?

} 1. Philosophy

~~How do ZKPs work?~~

What can ZKPs achieve?

What does the future hold?

Questions

Why is there a ZKP Revolution?

What does it mean for
me / Bitcoin / cryptocurrencies?

1. Philosophy

~~How do ZKPs work?~~

What can ZKPs achieve?

2. Technology

What does the future hold?

Questions

Why is there a ZKP Revolution?

What does it mean for
me / Bitcoin / cryptocurrencies?

~~How do ZKPs work?~~

What can ZKPs achieve?

What does the future hold?

1. Philosophy

2. Technology

3. Applications

1. PHILOSOPHY

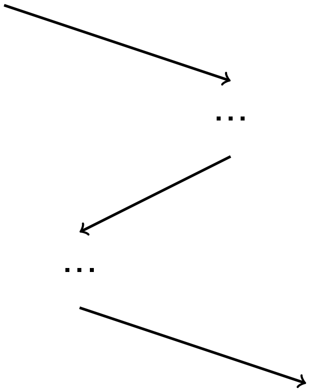
Motivation

Motivation

what is money?

Motivation

what is money?



Motivation

what is money?

...

...

cryptography

Motivation

what is money?

...

...

cryptography

is the natural medium

for money

Motivation

what is money?

...

...

cryptography

is the natural medium

for money

What is Money?

What is Money?

what you buy stuff with

What is Money?

✓ practical

what you buy stuff with

x recursive

What is Money?

✓ practical

what you buy stuff with

x recursive

$$\left\{ \begin{array}{c} \text{medium of exchange} \\ \text{store of value} \\ \text{unit of account} \end{array} \right\}$$

What is Money?

✓ practical

what you buy stuff with

x recursive

$$\left\{ \begin{array}{c} \text{medium of exchange} \\ \text{store of value} \\ \text{unit of account} \end{array} \right\}$$

✓ functions

x not properties

What is Money?

✓ practical

what you buy stuff with

x recursive

medium of exchange
store of value
unit of account

✓ functions
x not properties
x subjective

What is Money?

✓ practical

what you buy stuff with

x recursive

{ medium of exchange
store of value
unit of account }

✓ functions
x not properties
x subjective

the most marketable good

What is Money?

✓ practical

what you buy stuff with

x recursive

medium of exchange
store of value
unit of account

✓ functions
x not properties
x subjective

the most marketable good ✓ ✓

What is Money?

✓ practical

what you buy stuff with

x recursive

{ medium of exchange, store of value, unit of account }

✓ functions

x not properties

x subjective

the most marketable good

∼ context-dependent

What is Money?

✓ practical

what you buy stuff with

x recursive

{ medium of exchange, store of value, unit of account }

✓ functions

x not properties

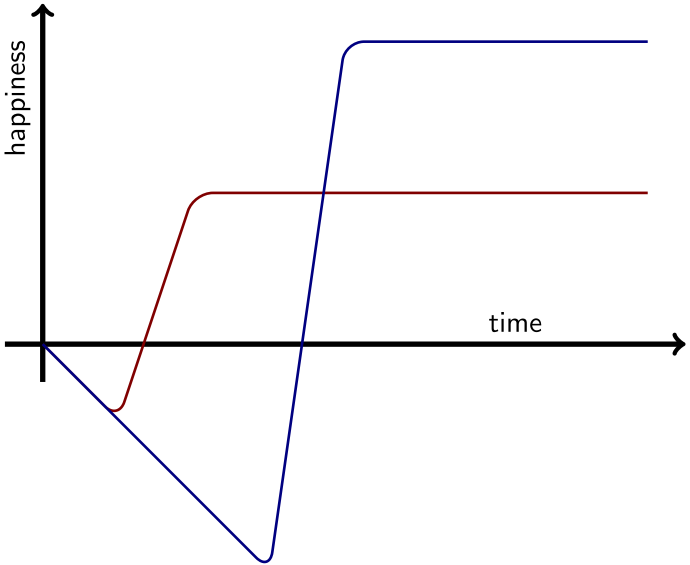
x subjective

the most marketable ✓ good ✓

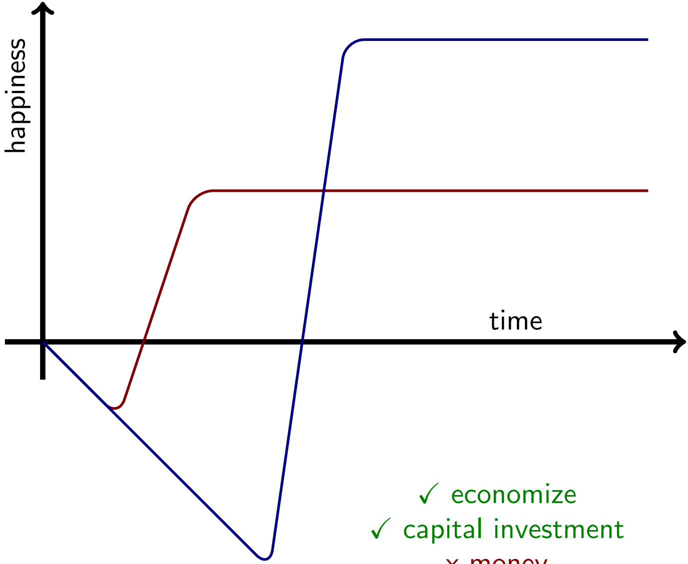
∼ context-dependent

x subjective

Robinson Crusoe

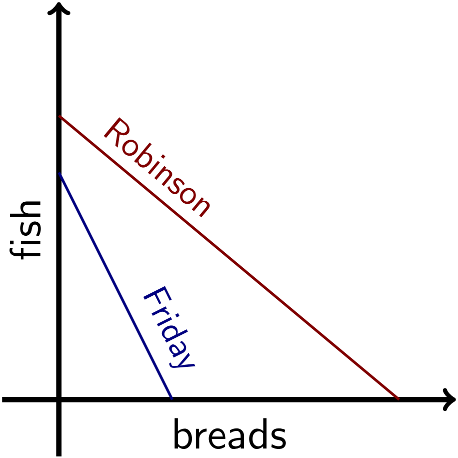


Robinson Crusoe

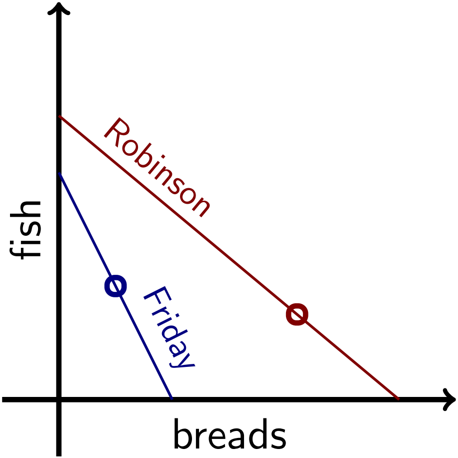


✓ economize
✓ capital investment
x money

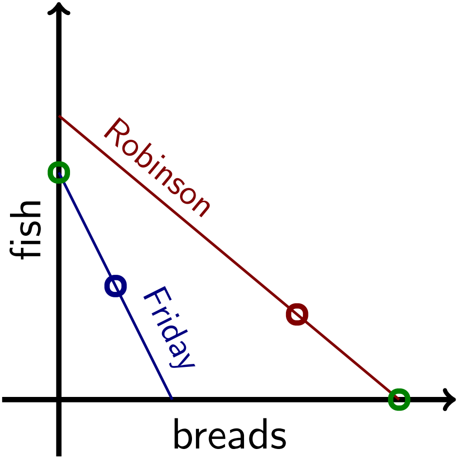
Robinson and Friday



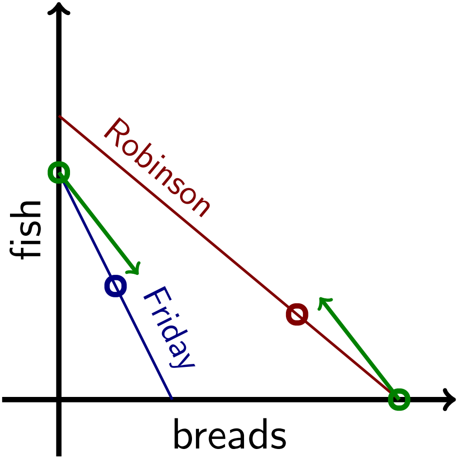
Robinson and Friday



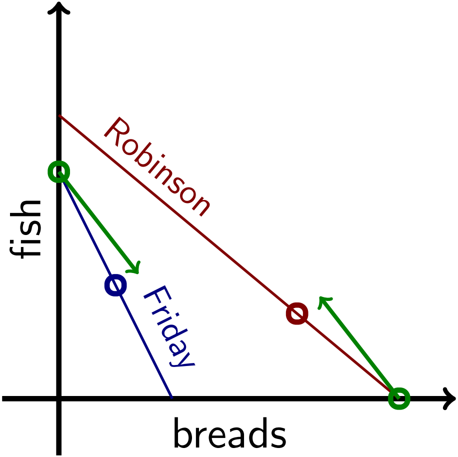
Robinson and Friday



Robinson and Friday



Robinson and Friday



✓ division of labor

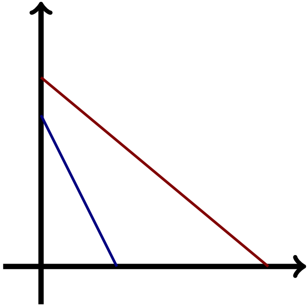
✓ ~ trust

x money

Larger Economies Need Money

Larger Economies Need Money

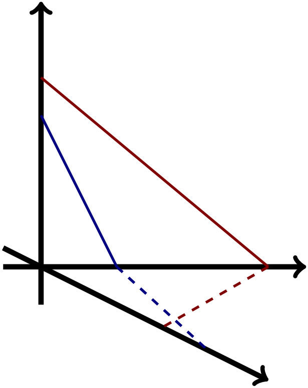
trust



Larger Economies Need Money

trust

coincidence of wants

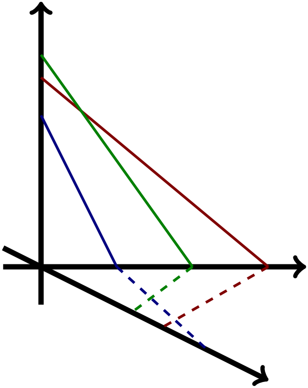


Larger Economies Need Money

trust

coincidence of wants

coordination



Larger Economies Need Money

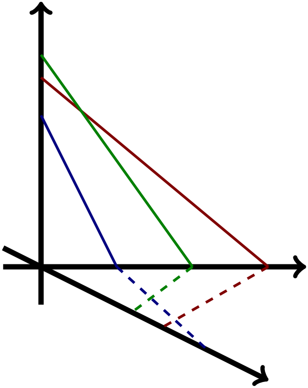
trust

coincidence of wants

coordination

↑

money fixes this



Larger Economies Need Money

trust

coincidence of wants

coordination

↑

money fixes this

Larger Economies Need Money

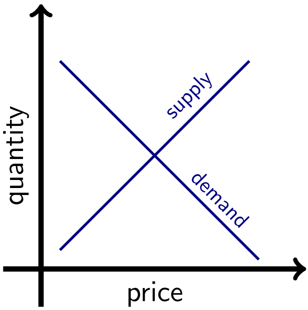
trust

coincidence of wants

coordination

↑

money fixes this



Larger Economies Need Money

trust

coincidence of wants

coordination

↑

money fixes this

Larger Economies Need Money

trust ⟶ adversarial context ✓

coincidence of wants

coordination

↑

money fixes this

Larger Economies Need Money

trust ⟶ adversarial context ✓

coincidence of wants ⟶ medium of exchange ✓

coordination

↑

money fixes this

Larger Economies Need Money

trust ⟶ adversarial context ✓

coincidence of wants ⟶ medium of exchange ✓

coordination ⟶ **carrier of information ✓**

↑

money fixes this

Larger Economies Need Money

trust ⟶ adversarial context ✓

coincidence of wants ⟶ medium of exchange ✓

coordination ⟶ carrier of information ✓

↑ money fixes this

↑ cryptography fixes this

Objectives of Cryptography

Objectives of Cryptography

CONFIDENTIALITY

INTEGRITY

AUTHENTICITY

Objectives of Cryptography

CONFIDENTIALITY

INTEGRITY

AUTHENTICITY

for money?

Objectives of Cryptography

~~CONFIDENTIALITY~~

INTEGRITY

AUTHENTICITY

for money?

Objectives of Cryptography

~~CONFIDENTIALITY~~

INTEGRITY

~~AUTHENTICITY~~

for money?

Objectives of Cryptography

~~CONFIDENTIALITY~~

INTEGRITY

VERIFIABILITY ✓ ✓ ✓

~~AUTHENTICITY~~

for money?

Objectives of Cryptography

~~CONFIDENTIALITY~~

INTEGRITY ⟸ VERIFIABILITY ✓ ✓ ✓

~~AUTHENTICITY~~

for money?

2. BASICS of ZERO-KNOWLEDGE PROOFS

Proof Systems in Mathematics

Proof Systems in Mathematics

in theory:

mathematician

mathematician

Proof Systems in Mathematics

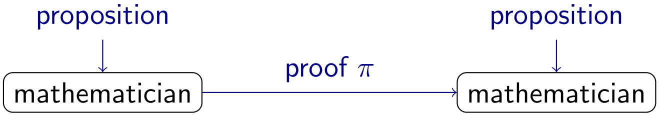
in theory:

proposition
↓
mathematician

proposition
↓
mathematician

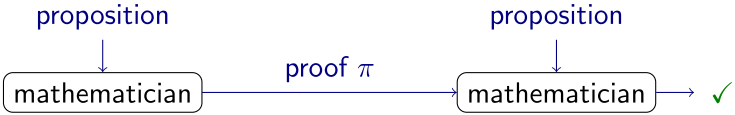
Proof Systems in Mathematics

in theory:



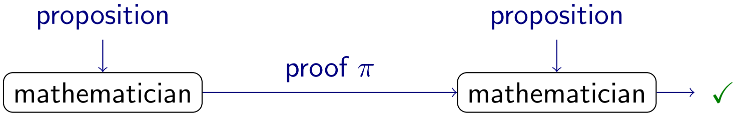
Proof Systems in Mathematics

in theory:



Proof Systems in Mathematics

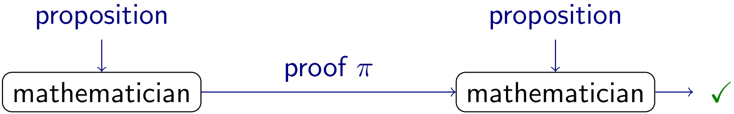
in theory:



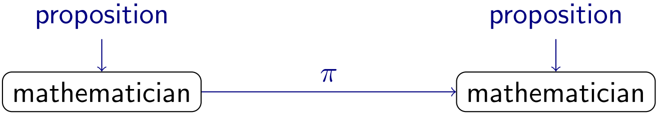
in practice:

Proof Systems in Mathematics

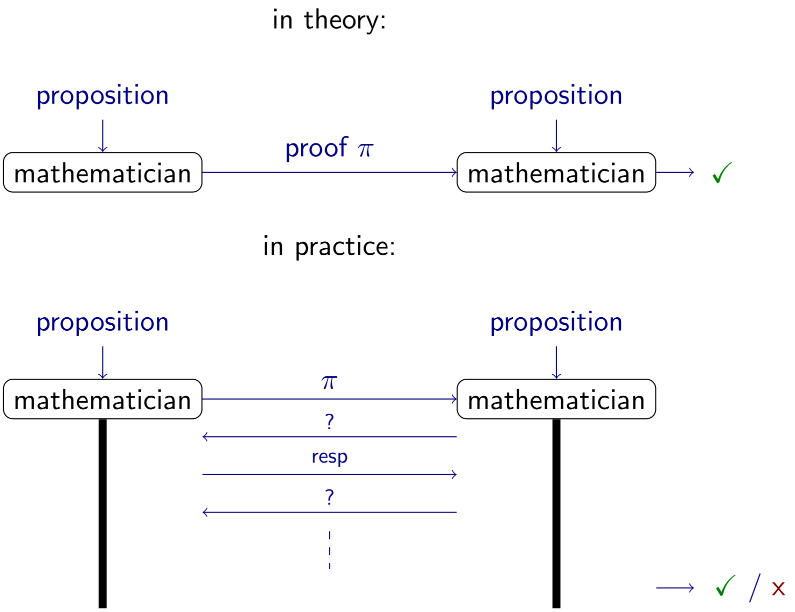
in theory:



in practice:



Proof Systems in Mathematics



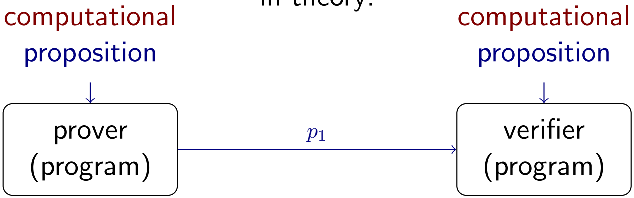
Proof Systems in Computer Science

Proof Systems in Computer Science

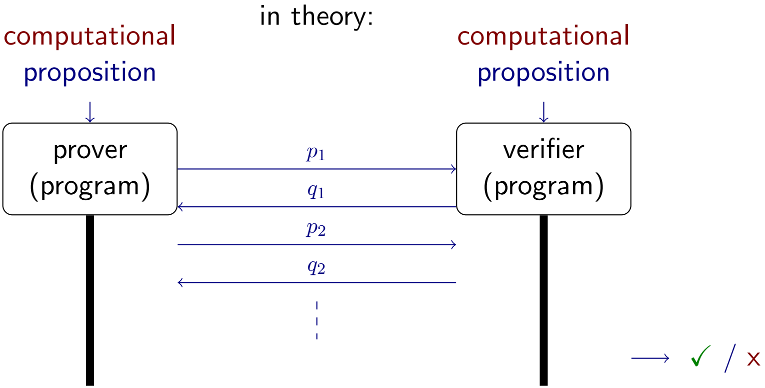
in theory:

Proof Systems in Computer Science

in theory:

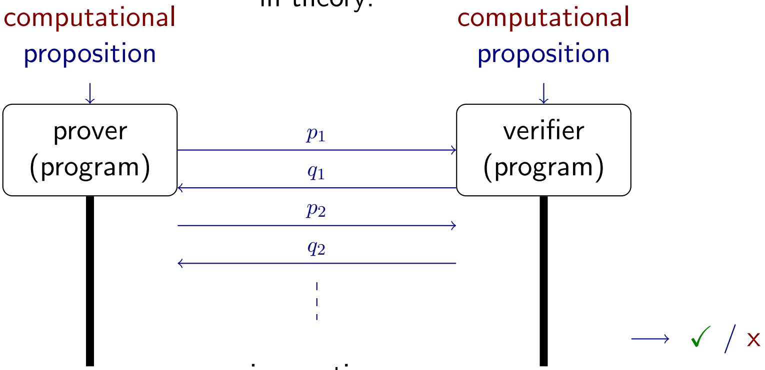


Proof Systems in Computer Science



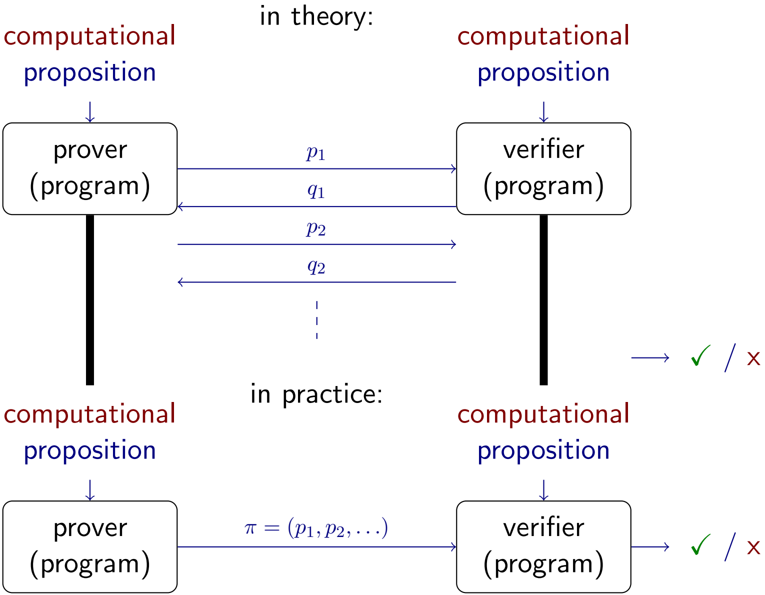
Proof Systems in Computer Science

in theory:



in practice:

Proof Systems in Computer Science



Computational Propositions

Computational Propositions

Program A

Computational Propositions

Program A

- takes public input $\mathbf{x}$

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$
- outputs public value $\mathbf{z}$

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$
- outputs public value $\mathbf{z}$
- runs in time T

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$
- outputs public value $\mathbf{z}$
- runs in time T

Naïve Verifier $(\mathbf{x}, \mathbf{y}, \mathbf{z})$:

- run $A(\mathbf{x}, \mathbf{y})$ for T steps
- test output against $\mathbf{z}$

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$
- outputs public value $\mathbf{z}$
- runs in time T

Naïve Verifier $(\mathbf{x}, \mathbf{y}, \mathbf{z})$:

- run $A(\mathbf{x}, \mathbf{y})$ for T steps
- test output against $\mathbf{z}$

Prover $(\mathbf{x}, \mathbf{y})$

- generate π
- while running $\mathbf{z} \leftarrow A(\mathbf{x}, \mathbf{y})$

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$
- outputs public value $\mathbf{z}$
- runs in time T

Naïve Verifier $(\mathbf{x}, \mathbf{y}, \mathbf{z})$:

- run $A(\mathbf{x}, \mathbf{y})$ for T steps
- test output against $\mathbf{z}$

Prover $(\mathbf{x}, \mathbf{y})$

- generate π
- while running $\mathbf{z} \leftarrow A(\mathbf{x}, \mathbf{y})$

Resource-Constrained Verifier $(\mathbf{x}, \mathbf{z}, \boldsymbol{\pi})$

- no access to secrets
- running time $t \ll T$

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$
- outputs public value $\mathbf{z}$
- runs in time T

Naïve Verifier $(\mathbf{x}, \mathbf{y}, \mathbf{z})$:

- run $A(\mathbf{x}, \mathbf{y})$ for T steps
- test output against $\mathbf{z}$

Prover $(\mathbf{x}, \mathbf{y})$

- generate π
- while running $\mathbf{z} \leftarrow A(\mathbf{x}, \mathbf{y})$

Resource-Constrained Verifier $(\mathbf{x}, \mathbf{z}, \boldsymbol{\pi})$

- no access to secrets $\longrightarrow$ zero-knowledge proof
- running time $t \ll T$

Computational Propositions

Program A

- takes public input $\mathbf{x}$
- takes secret input $\mathbf{y}$
- outputs public value $\mathbf{z}$
- runs in time T

Naïve Verifier $(\mathbf{x}, \mathbf{y}, \mathbf{z})$:

- run $A(\mathbf{x}, \mathbf{y})$ for T steps
- test output against $\mathbf{z}$

Prover $(\mathbf{x}, \mathbf{y})$

- generate π
- while running $\mathbf{z} \leftarrow A(\mathbf{x}, \mathbf{y})$

Resource-Constrained Verifier $(\mathbf{x}, \mathbf{z}, \boldsymbol{\pi})$

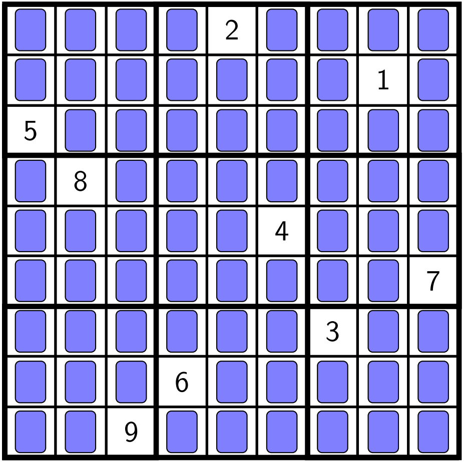
- no access to secrets $\longrightarrow$ zero-knowledge proof
- running time $t \ll T$ $\longrightarrow$ succinct proof (SNARK)

Succinct and Zero-Knowledge — Intuition

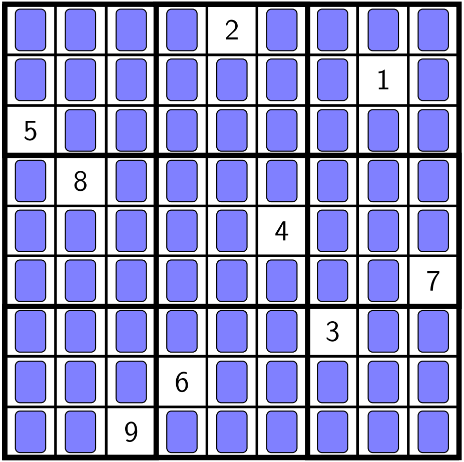
Succinct and Zero-Knowledge — Intuition

				2				
							1	
5								
	8							
					4			
								7
						3		
			6					
		9						

Succinct and Zero-Knowledge — Intuition

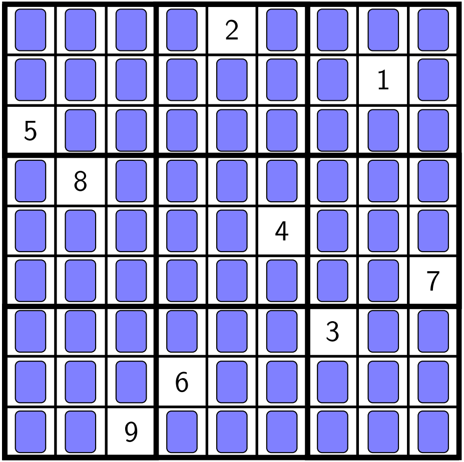


Succinct and Zero-Knowledge — Intuition



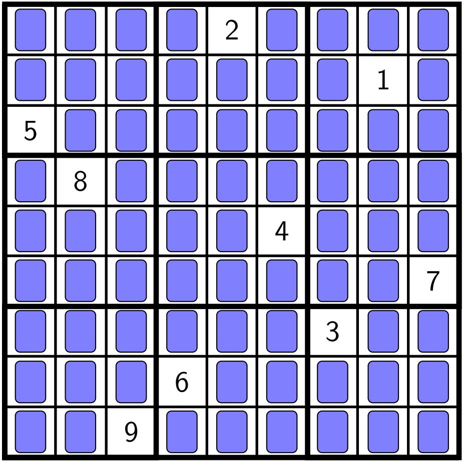
1. select row, column, or block

Succinct and Zero-Knowledge — Intuition



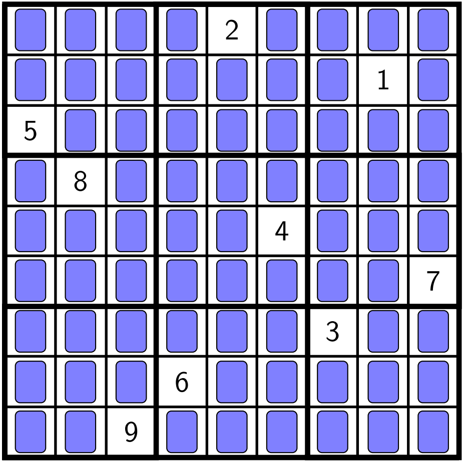
1. select row, column, or block
2. shuffle

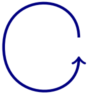
Succinct and Zero-Knowledge — Intuition



1. select row, column, or block
2. shuffle
3. flip and check

Succinct and Zero-Knowledge — Intuition





1. select row, column, or block
2. shuffle
3. flip and check

III Applications

III Applications A) to cryptocurrencies

Schnorr

Schnorr

Schnorr zero-knowledge proof

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

Schnorr

Schnorr zero-knowledge proof

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$ $\mathcal{V}$

Schnorr

Schnorr zero-knowledge proof

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$ $\mathcal{V}$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\mathbf{R} \leftarrow r \times \mathbf{G}$

$\xrightarrow{\quad\quad\mathbf{R}\quad\quad}$

Schnorr

Schnorr zero-knowledge proof

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$		$\mathcal{V}$
$r \xleftarrow{\$} \mathbb{Z}_p$		
$\mathbf{R} \leftarrow r \times \mathbf{G}$		
	$\xrightarrow{\mathbf{R}}$	
		$e \xleftarrow{\$} \mathbb{Z}_p$
	$\xleftarrow{e}$	

Schnorr

Schnorr zero-knowledge proof

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$ $\qquad\qquad\qquad$ $\mathcal{V}$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\mathbf{R} \leftarrow r \times \mathbf{G}$

$\xrightarrow{\quad \mathbf{R} \quad}$

$e \xleftarrow{\$} \mathbb{Z}_p$

$\xleftarrow{\quad e \quad}$

$s \leftarrow ex + r$

$\xrightarrow{\quad s \quad}$

Schnorr

Schnorr zero-knowledge proof

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$		$\mathcal{V}$
$r \xleftarrow{\$} \mathbb{Z}_p$ $\mathbf{R} \leftarrow r \times \mathbf{G}$		
	$\xrightarrow{\mathbf{R}}$	
		$e \xleftarrow{\$} \mathbb{Z}_p$
	$\xleftarrow{e}$	
$s \leftarrow ex + r$		
	$\xrightarrow{s}$	
		$s \times \mathbf{G} \stackrel{?}{=} e \times \mathbf{P} + \mathbf{R}$

Schnorr

Schnorr zero-knowledge proof

signature scheme

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$ $\qquad\qquad\qquad\qquad$ $\mathcal{V}$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\mathbf{R} \leftarrow r \times \mathbf{G}$

$\xrightarrow{\quad \mathbf{R} \quad}$

$e \xleftarrow{\$} \mathbb{Z}_p$

$\xleftarrow{\quad e \quad}$

$s \leftarrow ex + r$

$\xrightarrow{\quad s \quad}$

$s \times \mathbf{G} \stackrel{?}{=} e \times \mathbf{P} + \mathbf{R}$

Schnorr

Schnorr zero-knowledge proof

signature scheme

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$ $\qquad\qquad\qquad$ $\mathcal{V}$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\mathbf{R} \leftarrow r \times \mathbf{G}$

$\xrightarrow{\quad \mathbf{R} \quad}$

$e \xleftarrow{\$} \mathbb{Z}_p$ $\quad$ $e \leftarrow \mathsf{H}(\mathbf{R} \| \mathbf{P} \| m)$

$\xleftarrow{\quad e \quad}$

$s \leftarrow ex + r$

$\xrightarrow{\quad s \quad}$

$s \times \mathbf{G} \stackrel{?}{=} e \times \mathbf{P} + \mathbf{R}$

Schnorr

Schnorr zero-knowledge proof

signature scheme

signature: $(\mathbf{R}, s)$

secret key: $x \in \mathbb{Z}_p$

public key: $\mathbf{P} = x \times \mathbf{G}$

protocol:

$\mathcal{P}$ $\qquad\qquad$ $\mathcal{V}$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\mathbf{R} \leftarrow r \times \mathbf{G}$

$\xrightarrow{\mathbf{R}}$

$e \xleftarrow{\$} \mathbb{Z}_p$ $\quad$ $e \leftarrow \mathsf{H}(\mathbf{R} \| \mathbf{P} \| m)$

$\xleftarrow{e}$

$s \leftarrow ex + r$

$\xrightarrow{s}$

$s \times \mathbf{G} \stackrel{?}{=} e \times \mathbf{P} + \mathbf{R}$

Multisig Protocol

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, ex_a + r_a)$

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, e x_a + r_a)$
Bob	x_b	$x_b \times \mathbf{G}$	$(r_b \times \mathbf{G}, e x_b + r_b)$

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, ex_a + r_a)$
Bob	x_b	$x_b \times \mathbf{G}$	$(r_b \times \mathbf{G}, ex_b + r_b)$
joint	$x_a + x_b$	$(x_a + x_b) \times \mathbf{G}$	$((r_a + r_b) \times \mathbf{G},$ $e(x_a + x_b) + r_a + r_b)$

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, ex_a + r_a)$
Bob	x_b	$x_b \times \mathbf{G}$	$(r_b \times \mathbf{G}, ex_b + r_b)$
joint	$x_a + x_b$	$(x_a + x_b) \times \mathbf{G}$	$((r_a + r_b) \times \mathbf{G},$ $e(x_a + x_b) + r_a + r_b)$

$$e = \mathsf{H}((\mathbf{R}_a + \mathbf{R}_b) \| \mathbf{P} \| m)$$

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, ex_a + r_a)$
Bob	x_b	$x_b \times \mathbf{G}$	$(r_b \times \mathbf{G}, ex_b + r_b)$
joint	$x_a + x_b$	$(x_a + x_b) \times \mathbf{G}$	$((r_a + r_b) \times \mathbf{G}, e(x_a + x_b) + r_a + r_b)$

Alice   Bob

$$e = \mathsf{H}((\mathbf{R}_a + \mathbf{R}_b) \| \mathbf{P} \| m)$$

$\xrightarrow{\mathbf{R}_a}$

$\xleftarrow{\mathbf{R}_b}$

$\xrightarrow{s_a}$

$\xleftarrow{s_b}$

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, ex_a + r_a)$
Bob	x_b	$x_b \times \mathbf{G}$	$(r_b \times \mathbf{G}, ex_b + r_b)$
joint	$x_a + x_b$	$(x_a + x_b) \times \mathbf{G}$	$((r_a + r_b) \times \mathbf{G}, e(x_a + x_b) + r_a + r_b)$

Alice Bob $e = \mathsf{H}((\mathbf{R}_a + \mathbf{R}_b) \| \mathbf{P} \| m)$

$\xrightarrow{\mathbf{R}_a}$

$\xleftarrow{\mathbf{R}_b}$ X

$\xrightarrow{s_a}$

$\xleftarrow{s_b}$

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, ex_a + r_a)$
Bob	x_b	$x_b \times \mathbf{G}$	$(r_b \times \mathbf{G}, ex_b + r_b)$
joint	$x_a + x_b$	$(x_a + x_b) \times \mathbf{G}$	$((r_a + r_b) \times \mathbf{G},$ $e(x_a + x_b) + r_a + r_b)$

Alice Bob $e = \mathsf{H}((\mathbf{R}_a + \mathbf{R}_b) \| \mathbf{P} \| m)$

$\mathbf{R}_a$, $\boldsymbol{\pi}_a$ →

$\mathbf{R}_b$, $\boldsymbol{\pi}_b$ ←

s_a →

s_b ←

Multisig Protocol

	sk	pk	sig
Alice	x_a	$x_a \times \mathbf{G}$	$(r_a \times \mathbf{G}, e x_a + r_a)$
Bob	x_b	$x_b \times \mathbf{G}$	$(r_b \times \mathbf{G}, e x_b + r_b)$
joint	$x_a + x_b$	$(x_a + x_b) \times \mathbf{G}$	$((r_a + r_b) \times \mathbf{G},$ $e(x_a + x_b) + r_a + r_b)$

Alice Bob $e = \mathsf{H}((\mathbf{R}_a + \mathbf{R}_b) \| \mathbf{P} \| m)$

$\xrightarrow{\mathbf{R}_a\ ,\ \boldsymbol{\pi}_a}$

$\xleftarrow{\mathbf{R}_b\ ,\ \boldsymbol{\pi}_b}$

$\xrightarrow{s_a}$

$\xleftarrow{s_b}$

honest-but-curious security $\xrightarrow{\text{ZKPs}}$ malicious security

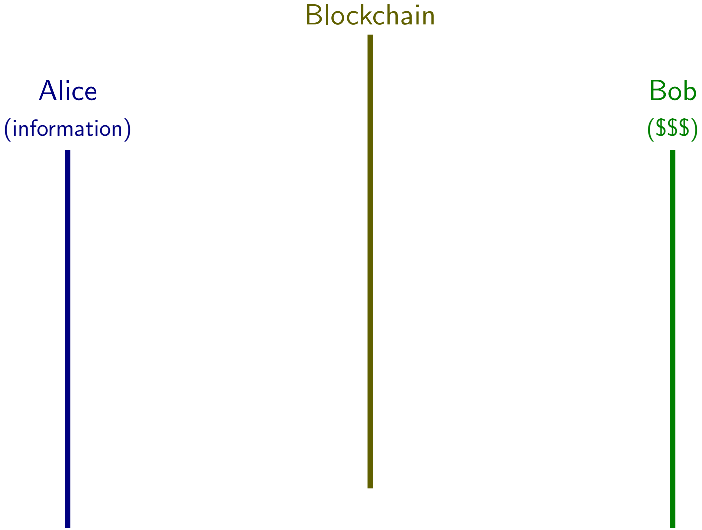
Zero-Knowledge Contingent Payments

Zero-Knowledge Contingent Payments

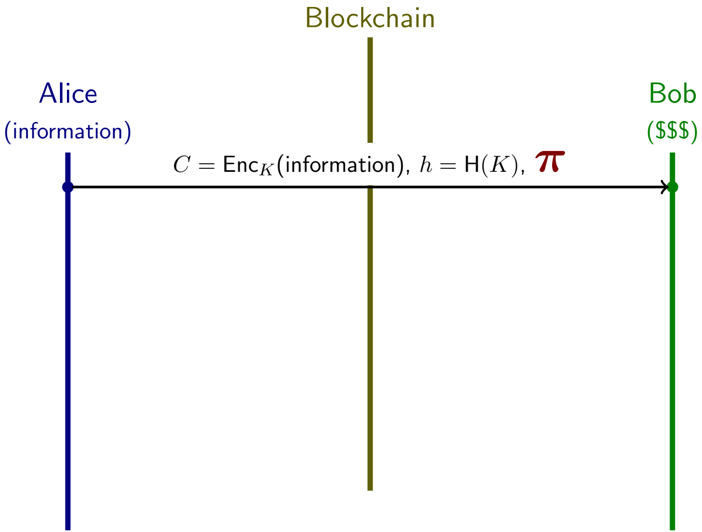
Alice
(information)

Bob
($$$)

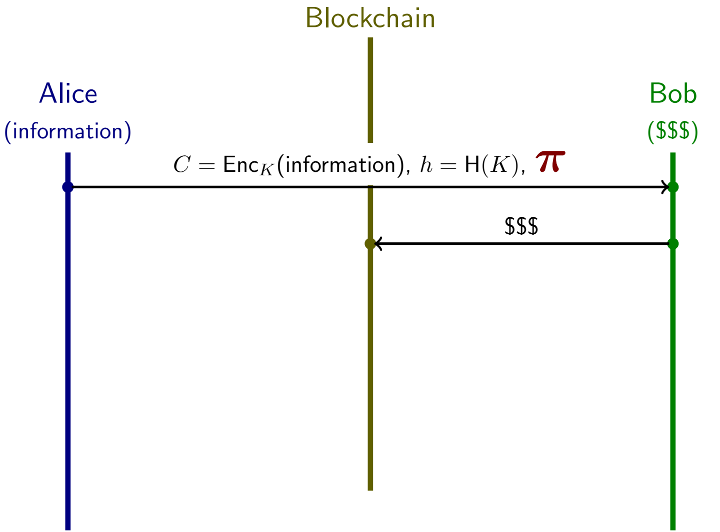
Zero-Knowledge Contingent Payments



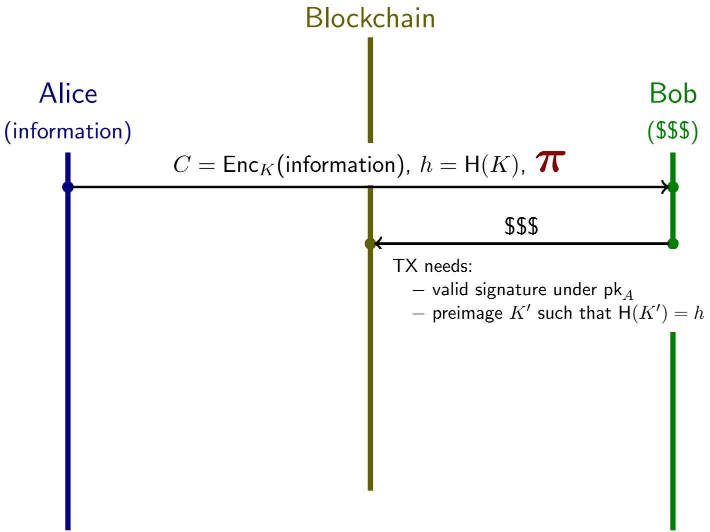
Zero-Knowledge Contingent Payments



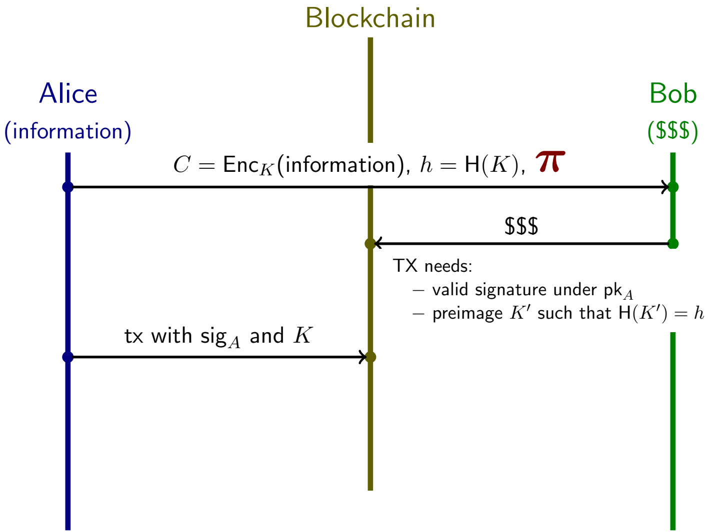
Zero-Knowledge Contingent Payments



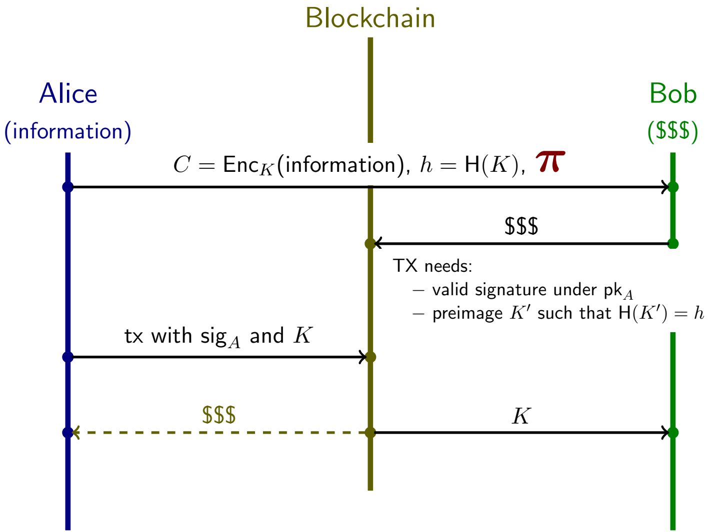
Zero-Knowledge Contingent Payments



Zero-Knowledge Contingent Payments

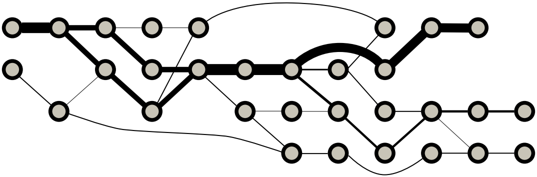


Zero-Knowledge Contingent Payments



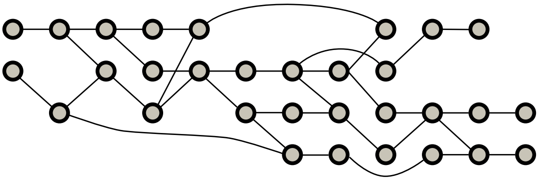
Privacy Coins

Privacy Coins



no privacy

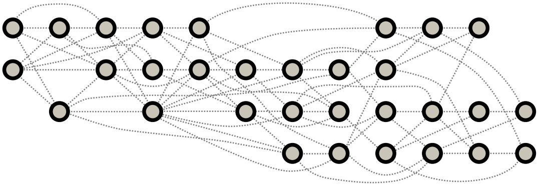
Privacy Coins



confidential transactions

$\pi \quad \leftrightarrow \quad$ "amounts are positive"

Privacy Coins

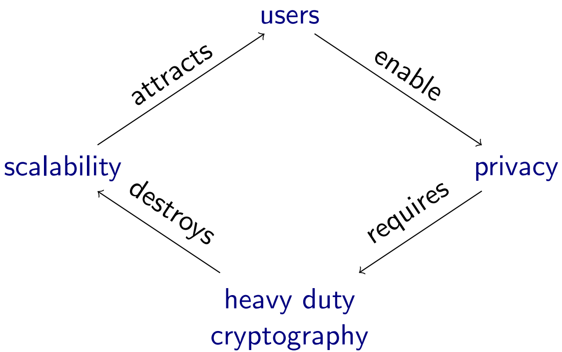


obfuscate origin

$\boldsymbol{\pi} \quad \leftrightarrow$ "amounts are positive and one these UTXOs is the true origin"

Privacy Coins — Disadvantage

Privacy Coins — Disadvantage



Scalability – Four Types of Information

Scalability – Four Types of Information

- unverified witness
- state update
- state information
- verified witness

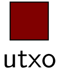
Scalability – Four Types of Information

unverified witness

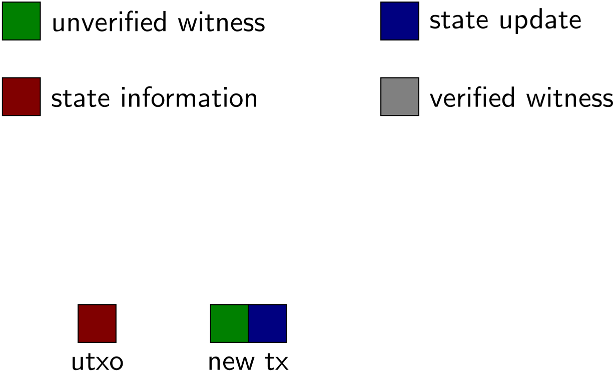
state update

state information

verified witness

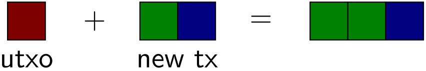


Scalability – Four Types of Information

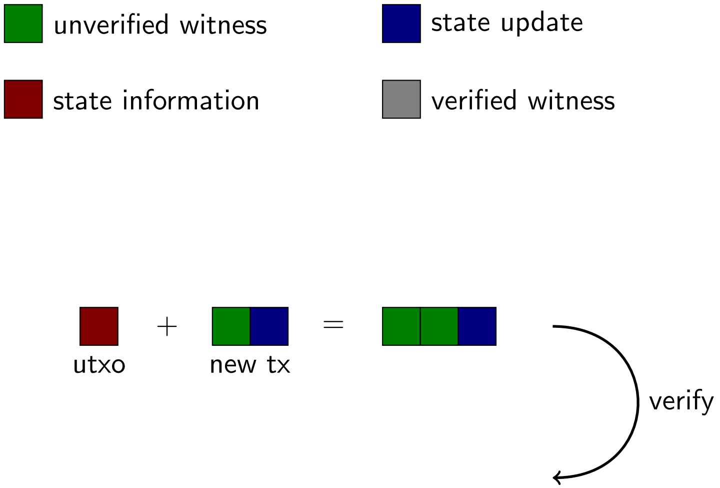


Scalability – Four Types of Information

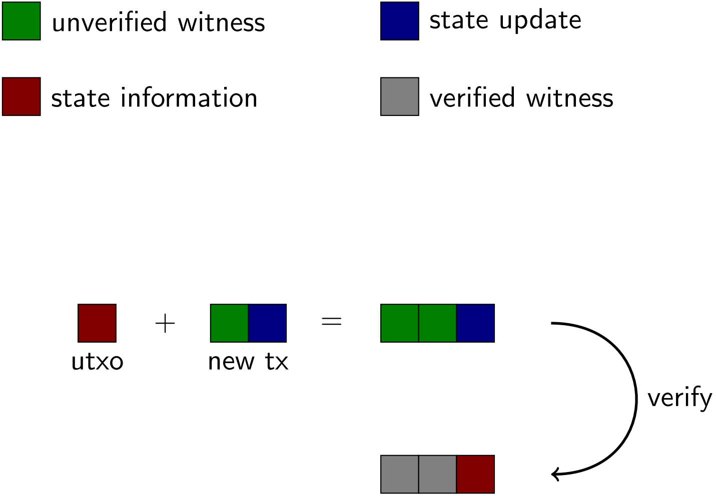
- unverified witness (green)
- state update (blue)
- state information (red)
- verified witness (grey)



Scalability – Four Types of Information



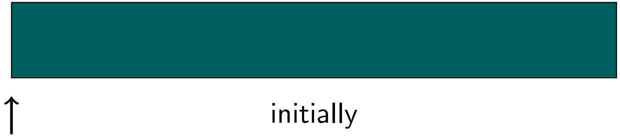
Scalability – Four Types of Information



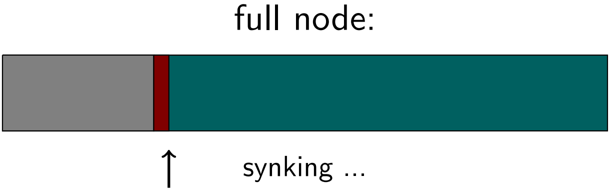
Scalability – Synking

Scalability – Synking

full node:

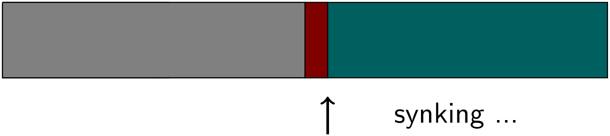


Scalability – Synking



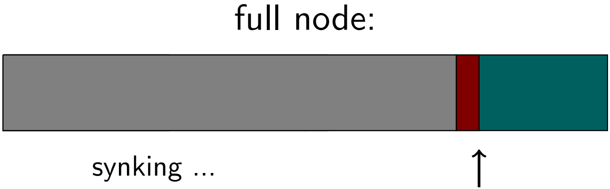
Scalability – Synking

full node:



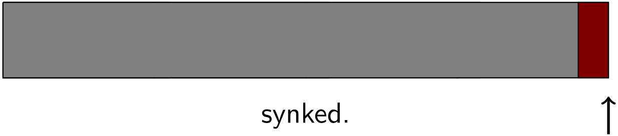
synking ...

Scalability – Synking

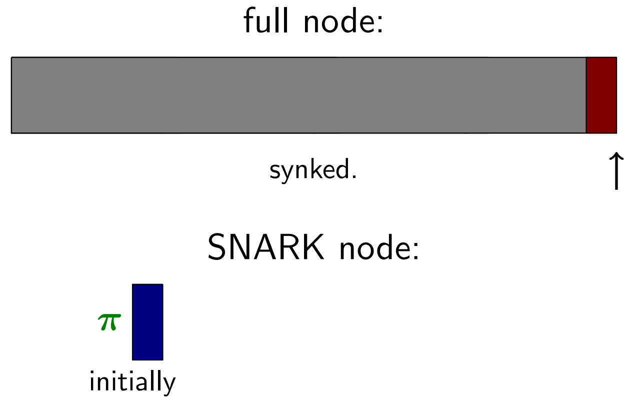


Scalability – Synking

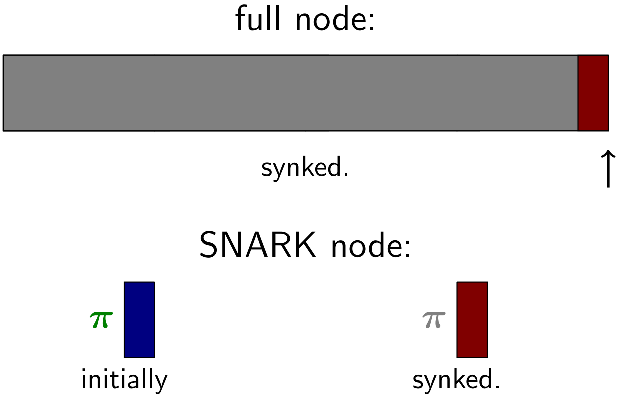
full node:



Scalability – Synking



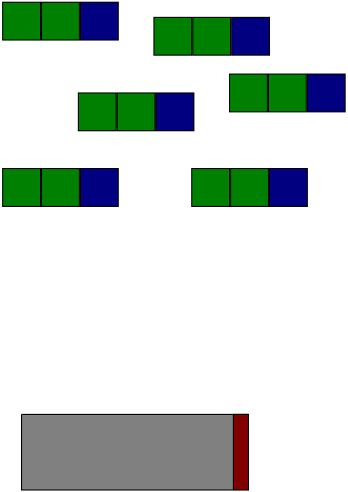
Scalability – Synking



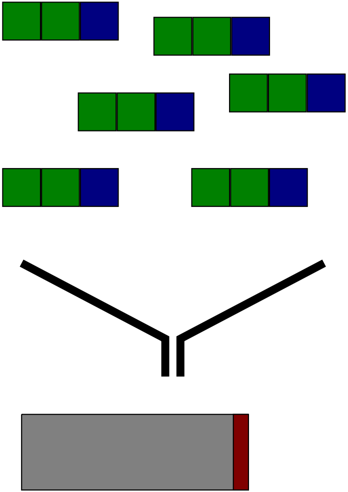
Scalability — Aggregation

Scalability — Aggregation

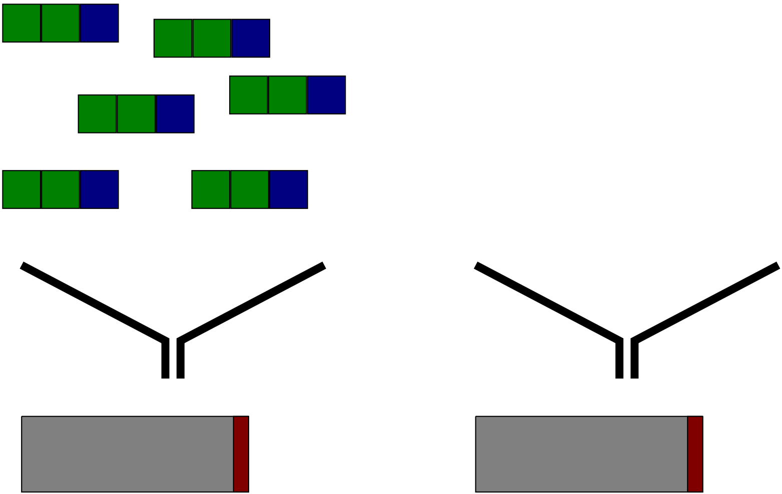
Scalability — Aggregation



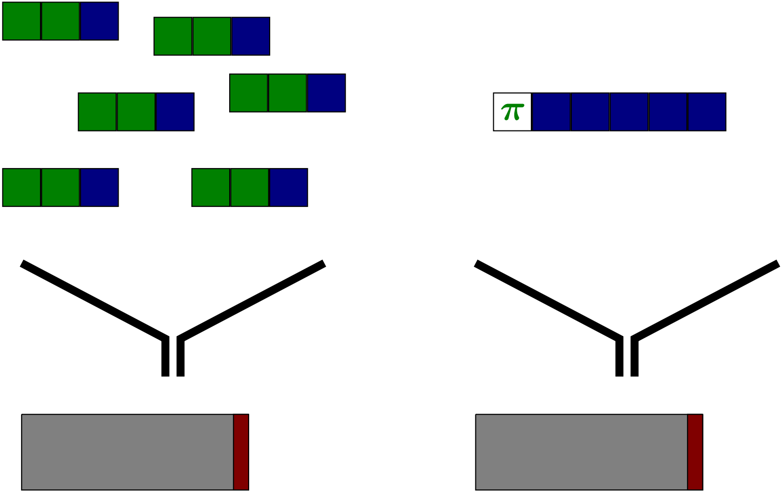
Scalability — Aggregation



Scalability — Aggregation



Scalability — Aggregation



III Applications

III Applications B) Other

Private Finance

Private Finance

trades

guarantee: integral order matching

hide: algorithm, volume

Private Finance

trades

guarantee: integral order matching

hide: algorithm, volume

lending

guarantee: cash flow positivity, qualification

hide: transaction history

Private Finance

trades

guarantee: integral order matching

hide: algorithm, volume

lending

guarantee: cash flow positivity, qualification

hide: transaction history

investment

guarantee: blacklist non-membership

hide: investor identity, source of funds, allocation

Private Finance

trades

guarantee: integral order matching

hide: algorithm, volume

lending

guarantee: cash flow positivity, qualification

hide: transaction history

investment

guarantee: blacklist non-membership

hide: investor identity, source of funds, allocation

audit

guarantee: regulatory compliance, valid accounting

hide: balance sheet

Private eGovernment

Private eGovernment

identity

guarantee: qualification

hide: personal data

Private eGovernment

identity

guarantee: qualification

hide: personal data

voting

guarantee: election integrity

hide: individual votes

Private eGovernment

identity

guarantee: qualification

hide: personal data

voting

guarantee: election integrity

hide: individual votes

taxes

guarantee: tax compliance

hide: wealth, assets

Private eGovernment

identity

guarantee: qualification

hide: personal data

voting

guarantee: election integrity

hide: individual votes

taxes

guarantee: tax compliance

hide: wealth, assets

surveillance

guarantee: legality,
blacklist non-membership

hide: movements, interactions,
communications

Other

Other

gaming

guarantee: unbiased shuffling, legal moves

hide: strategy, position, randomness

Other

gaming

guarantee: unbiased shuffling, legal moves

hide: strategy, position, randomness

exploits and vulnerabilities

guarantee: existence of vulnerability, fair exchange

hide: vulnerability