ZERO KNOWLEDGE & BLOCKCHAINS

Prof. Aviv Zohar

The Hebrew University of Jerusalem & QEDIT

About me

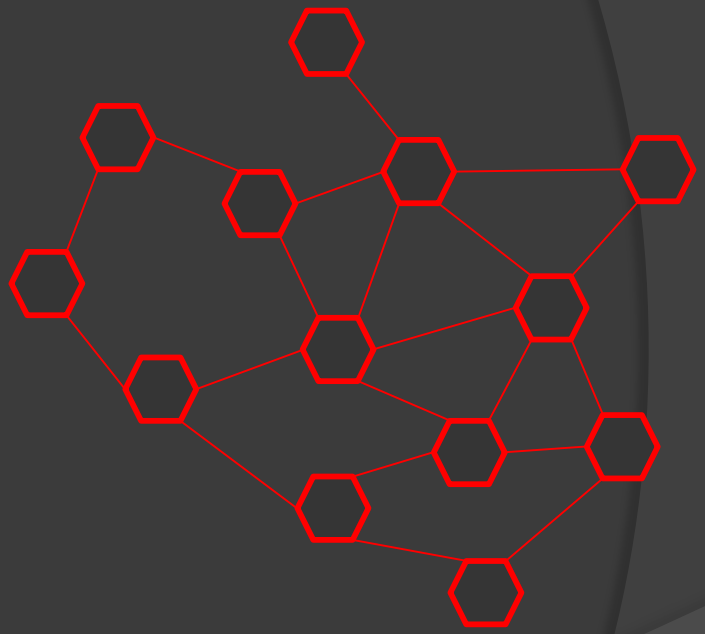
- Computer Scientist at Hebrew U.
- Researching cryptocurrencies (Security, scalability, economic incentives etc.) since 2011

- Co-founder & Chief scientist at QEDIT
  - a company creating “enhanced privacy” solutions for enterprise market.

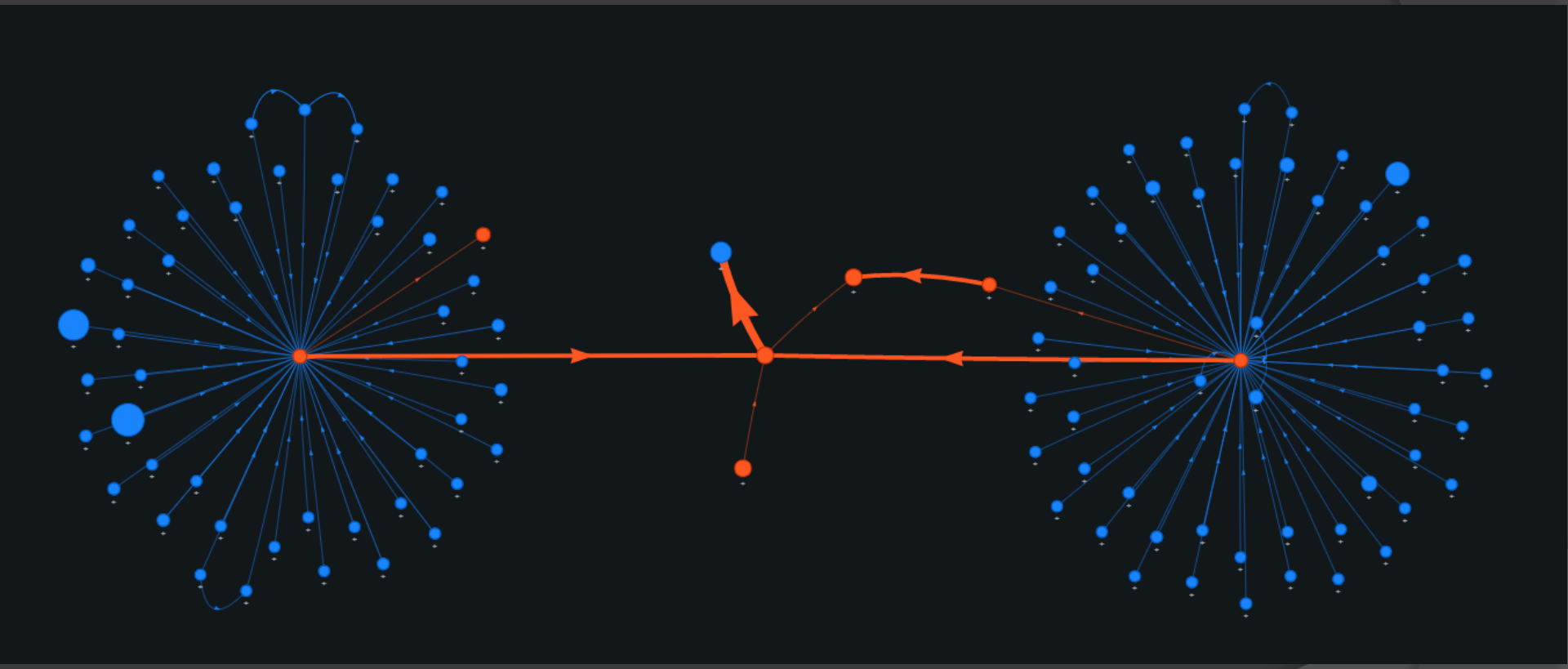
qedit

Blockchain systems

- Reliably duplicate data between many computers
- Repeat the same computation and reach the same conclusions
- For Bitcoin: data is a ledger containing all transactions



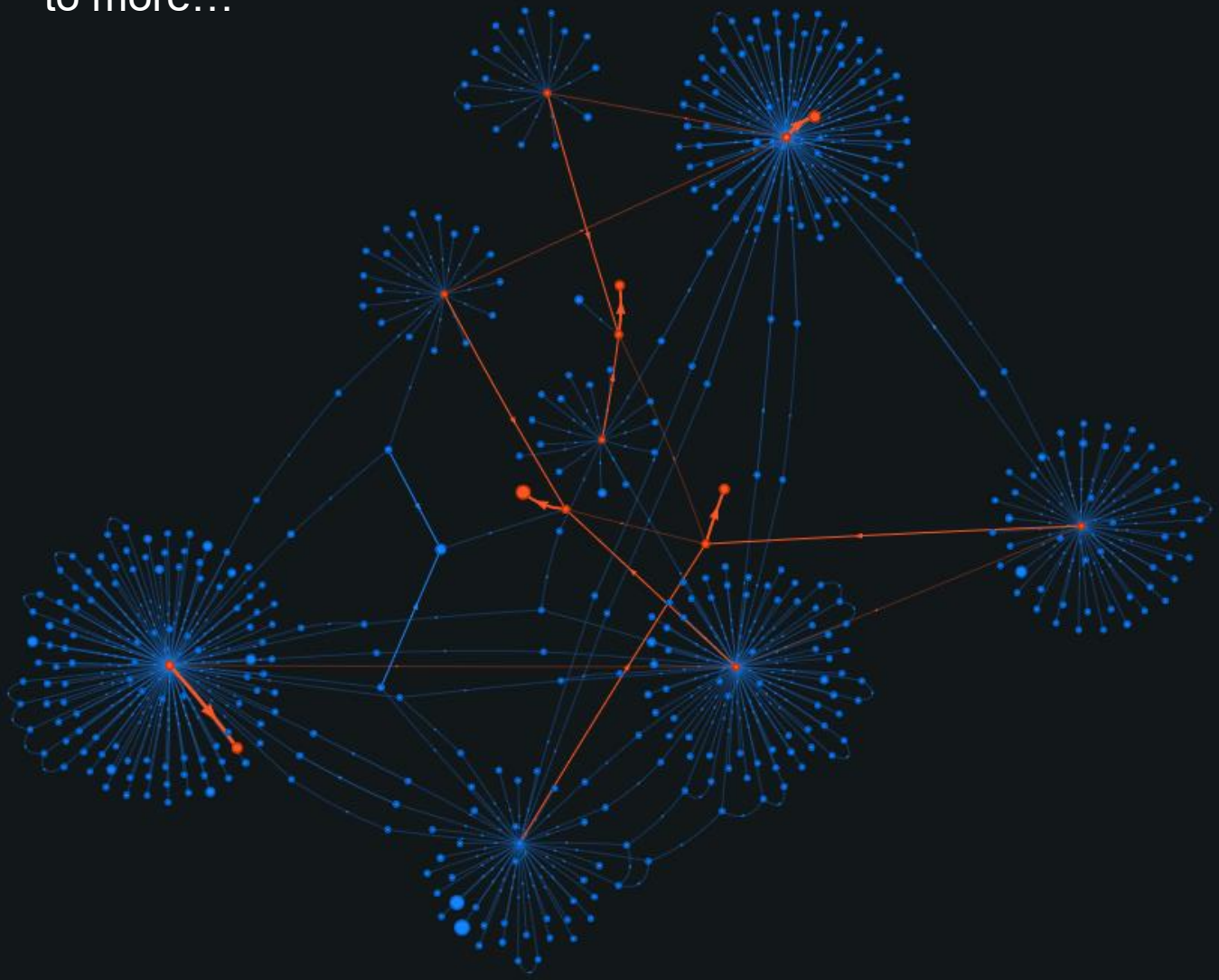
Bitcoin isn’t Private



100BTC of paymets to Locky aggregated into an exchange
(payments 0.5,1,2,3,7 BTC collected into two 50 BTC transactions)

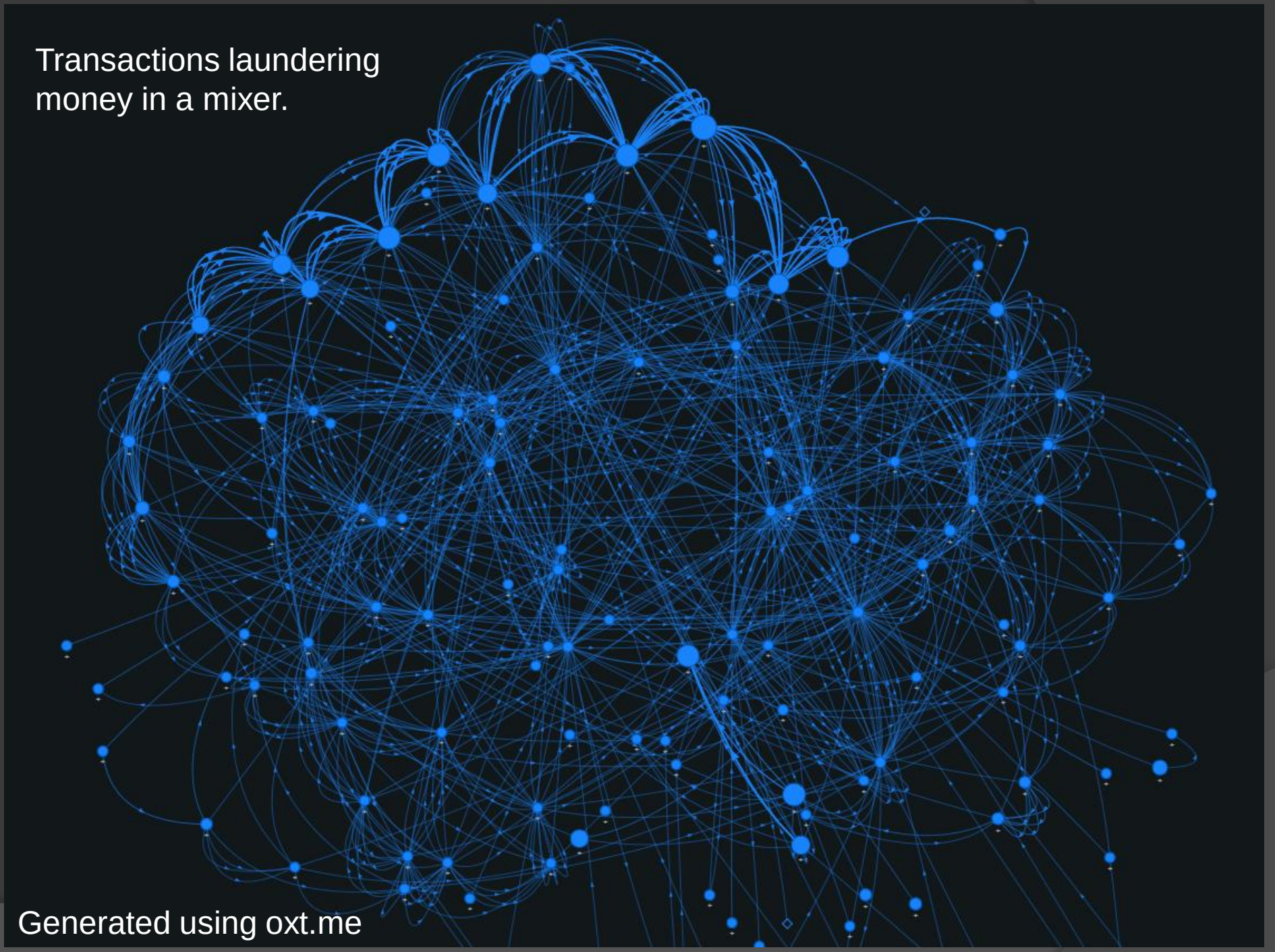
Generated using oxt.me

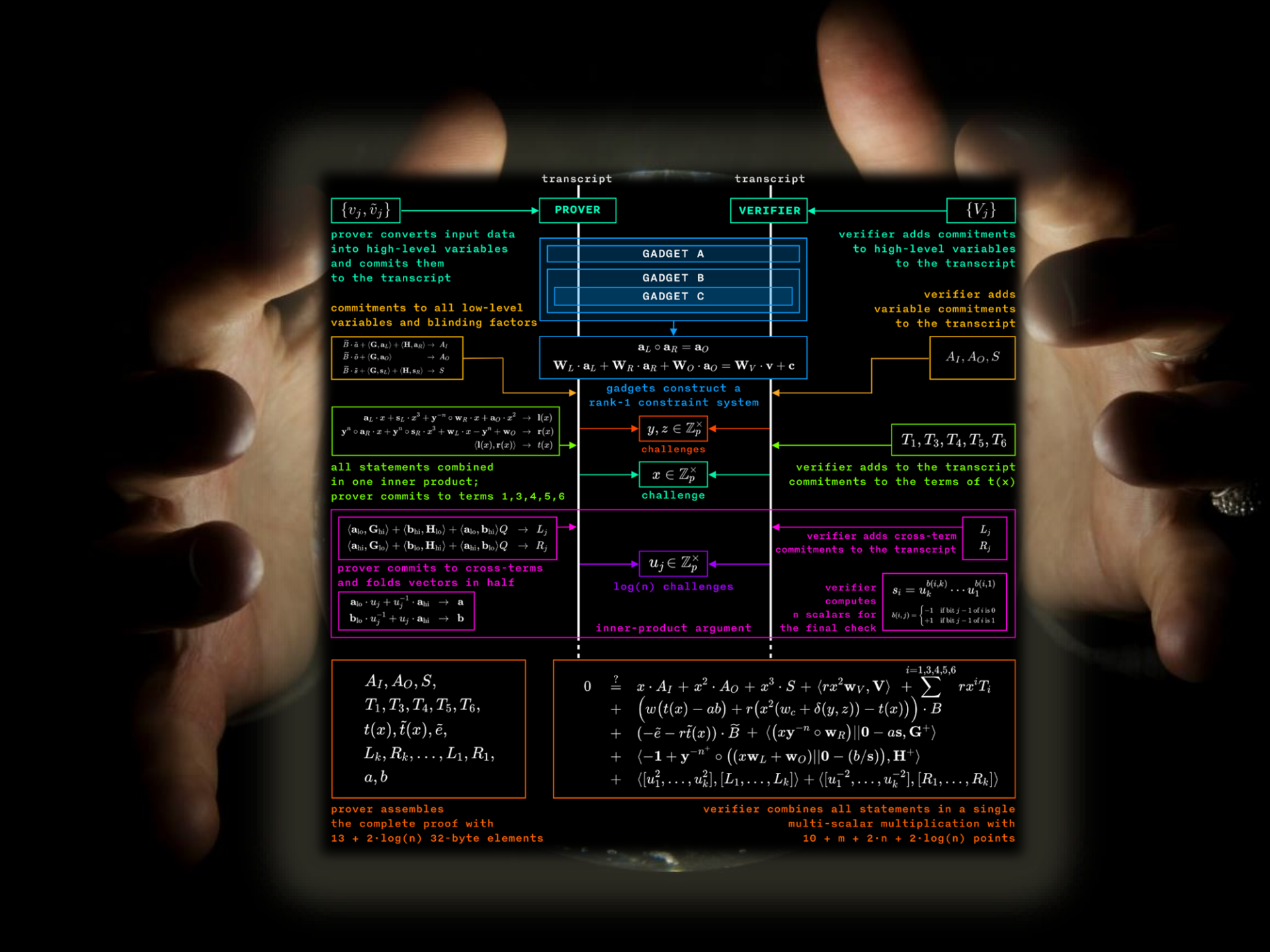
Following change addresses leads to more…



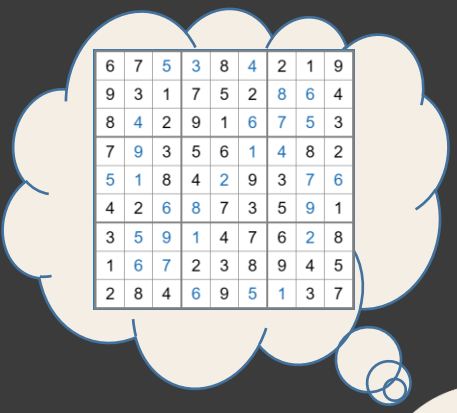
Generated using oxt.me

Generated using oxt.me

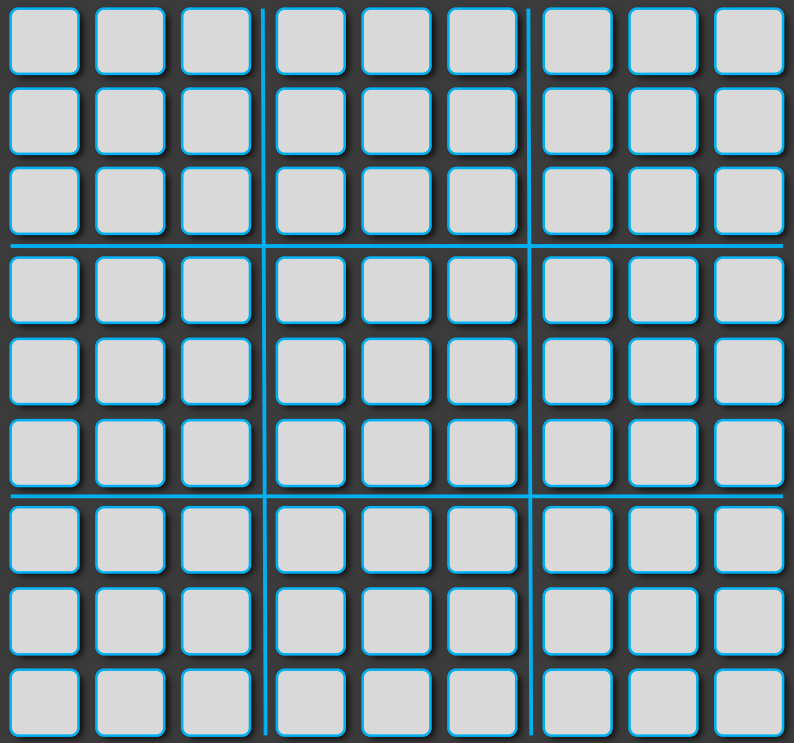

Transactions laundering
money in a mixer.
Generated using oxt.me


transcript
transcript
$\{v_j, \tilde{v}_j\}$
PROVER
VERIFIER
$\{V_j\}$
prover converts input data into high-level variables and commits them to the transcript
GADGET A
GADGET B
GADGET C
verifier adds commitments to high-level variables to the transcript
commitments to all low-level variables and blinding factors
$\tilde{B} \cdot \tilde{a} + \langle \mathbf{G}, \mathbf{a}_L \rangle + \langle \mathbf{H}, \mathbf{a}_R \rangle \rightarrow A_I$
$\tilde{B} \cdot \tilde{o} + \langle \mathbf{G}, \mathbf{a}_O \rangle \rightarrow A_O$
$\tilde{B} \cdot \tilde{s} + \langle \mathbf{G}, \mathbf{s}_L \rangle + \langle \mathbf{H}, \mathbf{s}_R \rangle \rightarrow S$
$\mathbf{a}_L \circ \mathbf{a}_R = \mathbf{a}_O$
$\mathbf{W}_L \cdot \mathbf{a}_L + \mathbf{W}_R \cdot \mathbf{a}_R + \mathbf{W}_O \cdot \mathbf{a}_O = \mathbf{W}_V \cdot \mathbf{v} + \mathbf{c}$
verifier adds variable commitments to the transcript
A_I, A_O, S
gadgets construct a rank-1 constraint system
$\mathbf{a}_L \cdot x + \mathbf{s}_L \cdot x^3 + \mathbf{y}^{-n} \circ \mathbf{w}_R \cdot x + \mathbf{a}_O \cdot x^2 \rightarrow \mathbf{l}(x)$
$\mathbf{y}^n \circ \mathbf{a}_R \cdot x + \mathbf{y}^n \circ \mathbf{s}_R \cdot x^3 + \mathbf{w}_L \cdot x - \mathbf{y}^n + \mathbf{w}_O \rightarrow \mathbf{r}(x)$
$\langle \mathbf{l}(x), \mathbf{r}(x) \rangle \rightarrow t(x)$
$y, z \in \mathbb{Z}_p^\times$
challenges
T_1, T_3, T_4, T_5, T_6
all statements combined in one inner product; prover commits to terms 1,3,4,5,6
$x \in \mathbb{Z}_p^\times$
challenge
verifier adds to the transcript commitments to the terms of t(x)
$\langle \mathbf{a}_{\text{lo}}, \mathbf{G}_{\text{hi}} \rangle + \langle \mathbf{b}_{\text{hi}}, \mathbf{H}_{\text{lo}} \rangle + \langle \mathbf{a}_{\text{lo}}, \mathbf{b}_{\text{hi}} \rangle Q \rightarrow L_j$
$\langle \mathbf{a}_{\text{hi}}, \mathbf{G}_{\text{lo}} \rangle + \langle \mathbf{b}_{\text{lo}}, \mathbf{H}_{\text{hi}} \rangle + \langle \mathbf{a}_{\text{hi}}, \mathbf{b}_{\text{lo}} \rangle Q \rightarrow R_j$
verifier adds cross-term commitments to the transcript
L_j
R_j
prover commits to cross-terms and folds vectors in half
$u_j \in \mathbb{Z}_p^\times$
log(n) challenges
$\mathbf{a}_{\text{lo}} \cdot u_j + u_j^{-1} \cdot \mathbf{a}_{\text{hi}} \rightarrow \mathbf{a}$
$\mathbf{b}_{\text{lo}} \cdot u_j^{-1} + u_j \cdot \mathbf{a}_{\text{hi}} \rightarrow \mathbf{b}$
verifier computes n scalars for the final check
$s_i = u_k^{b(i,k)} \cdots u_1^{b(i,1)}$
$b(i,j) = \begin{cases} -1 & \text{if bit } j-1 \text{ of } i \text{ is } 0 \\ +1 & \text{if bit } j-1 \text{ of } i \text{ is } 1 \end{cases}$
inner-product argument
$A_I, A_O, S,$
$T_1, T_3, T_4, T_5, T_6,$
$t(x), \tilde{t}(x), \tilde{e},$
$L_k, R_k, \ldots, L_1, R_1,$
a, b
$0 \stackrel{?}{=} x \cdot A_I + x^2 \cdot A_O + x^3 \cdot S + \langle rx^2 \mathbf{w}_V, \mathbf{V} \rangle + \sum_{i=1,3,4,5,6} rx^i T_i$
$+ \left(w(t(x) - ab) + r(x^2(w_c + \delta(y,z)) - t(x)) \right) \cdot B$
$+ (-\tilde{e} - r\tilde{t}(x)) \cdot \widetilde{B} + \langle (x\mathbf{y}^{-n} \circ \mathbf{w}_R) || \mathbf{0} - as, \mathbf{G}^+ \rangle$
$+ \langle -\mathbf{1} + \mathbf{y}^{-n^+} \circ ((x\mathbf{w}_L + \mathbf{w}_O) || \mathbf{0} - (b/\mathbf{s})), \mathbf{H}^+ \rangle$
$+ \langle [u_1^2, \ldots, u_k^2], [L_1, \ldots, L_k] \rangle + \langle [u_1^{-2}, \ldots, u_k^{-2}], [R_1, \ldots, R_k] \rangle$
prover assembles the complete proof with 13 + 2·log(n) 32-byte elements
verifier combines all statements in a single multi-scalar multiplication with 10 + m + 2·n + 2·log(n) points

		5	3		4			
						8	6	
	4				6	7	5	
	9				1	4		
5	1			2			7	6
		6	8				9	
	5	9	1				2	
	6	7						
			6		5	1		



I know the solution.
And I can prove it!
… but without showing you the answer



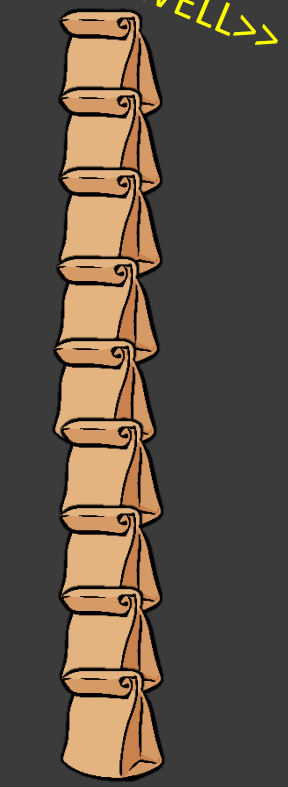
		5	3		4			
						8	6	
	4				6	7	5	
	9				1	4		
5	1			2			7	6
		6	8				9	
	5	9	1				2	
	6	7						
			6		5	1		

Pick what to test:
Rows, Columns, or Boxes

<<rolls some dice>>

Rows please.

		5	3		4			
						8	6	
	4				6	7	5	
	9				1	4		
5	1			2			7	6
		6	8				9	
	5	9	1				2	
	6	7						
			6		5	1		



<<Checks each bag>>
<<Each contains digits 1-9>>

Okay.

You were lucky.
Do that again.

Completeness:

If Peter knows the solution, he can always pass the test.

Soundness:

If Peter tries to cheat: there is at least one row / column / box that is incorrect. Veronica will catch him with probability $\geq \frac{1}{3}$

Repeating the procedure N times means he cheats with probability $\leq \left(\frac{2}{3}\right)^N$

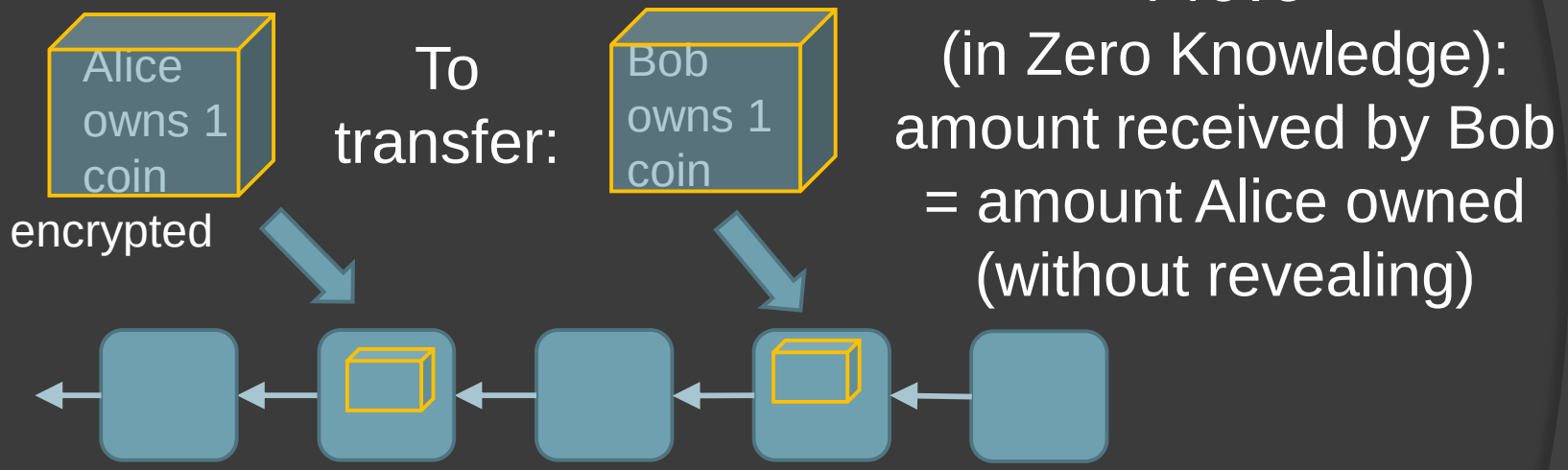
Zero Knowledge:

Veronica learns nothing about the solution, except that it's correct.

Advanced privacy layers

Zero knowledge proofs applied to blockchains:

(ZeroCash [Ben Sasson et. al])



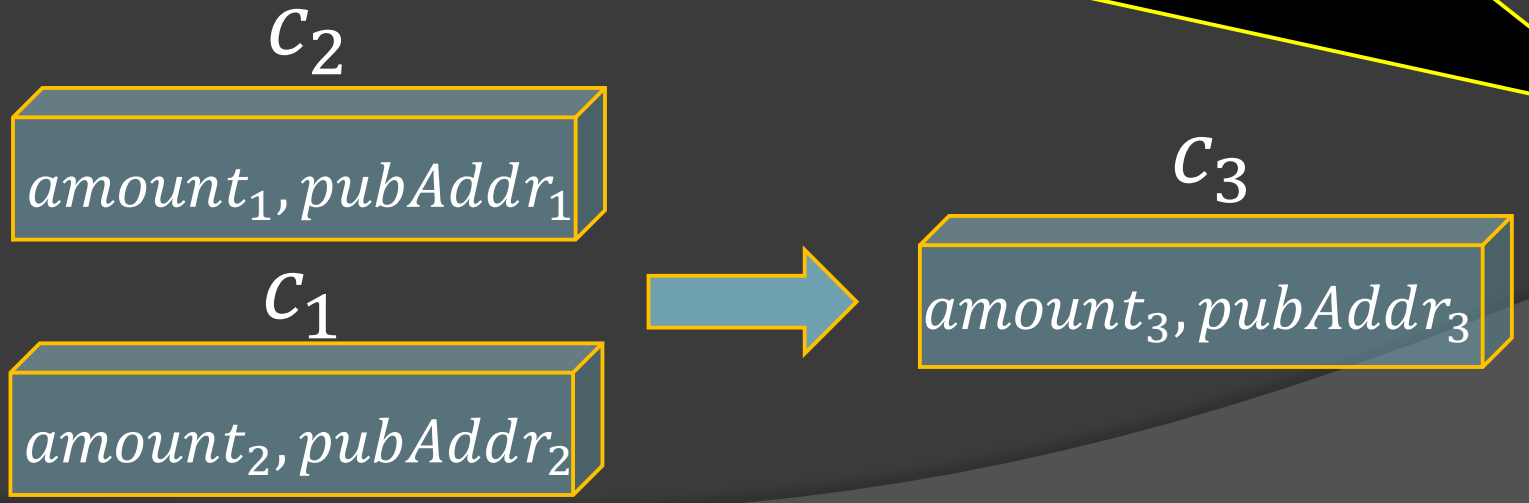
Outcomes:

1. Cannot see amounts
2. Cannot link payments

But, transactions are still validated.

- $c_3 = commit(amount_3, pubAddr_3)$
- ∃ records c_1, c_2 on the blockchain
- $c_1 = commit(amount_1, pubAddr_1)$
- $c_2 = commit(amount_2, pubAddr_2)$
- $amount_3 = amount_1 + amount_2$
- $amount_3 \geq 0$
- ∃ $secretKey_1, secretKey_2$ that match $pubAddr_1, pubAddr_2$ (and I know them)

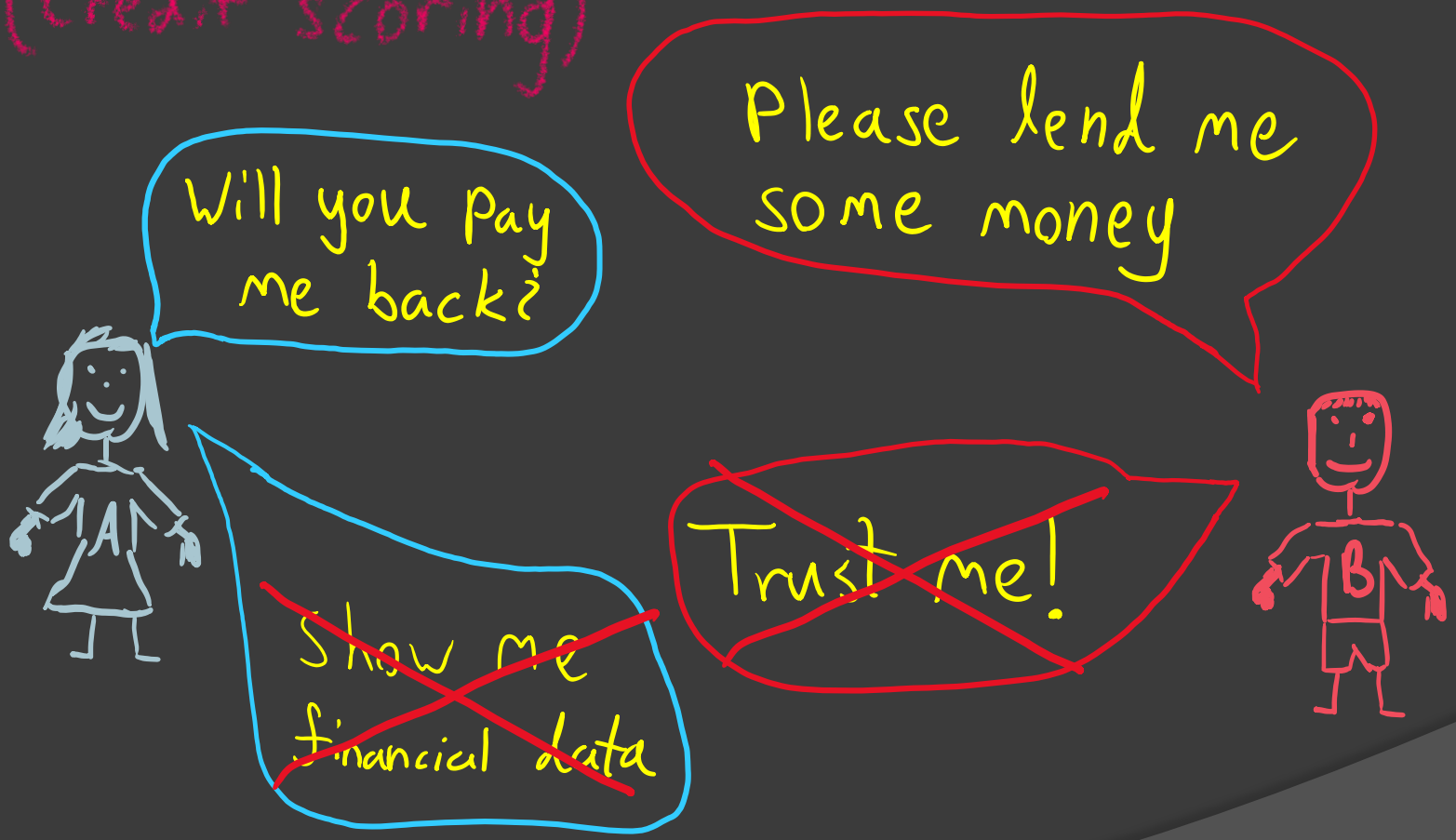
π




Blockchain dreams
& privacy problems

An Example

(credit scoring)



An Example

(credit scoring)

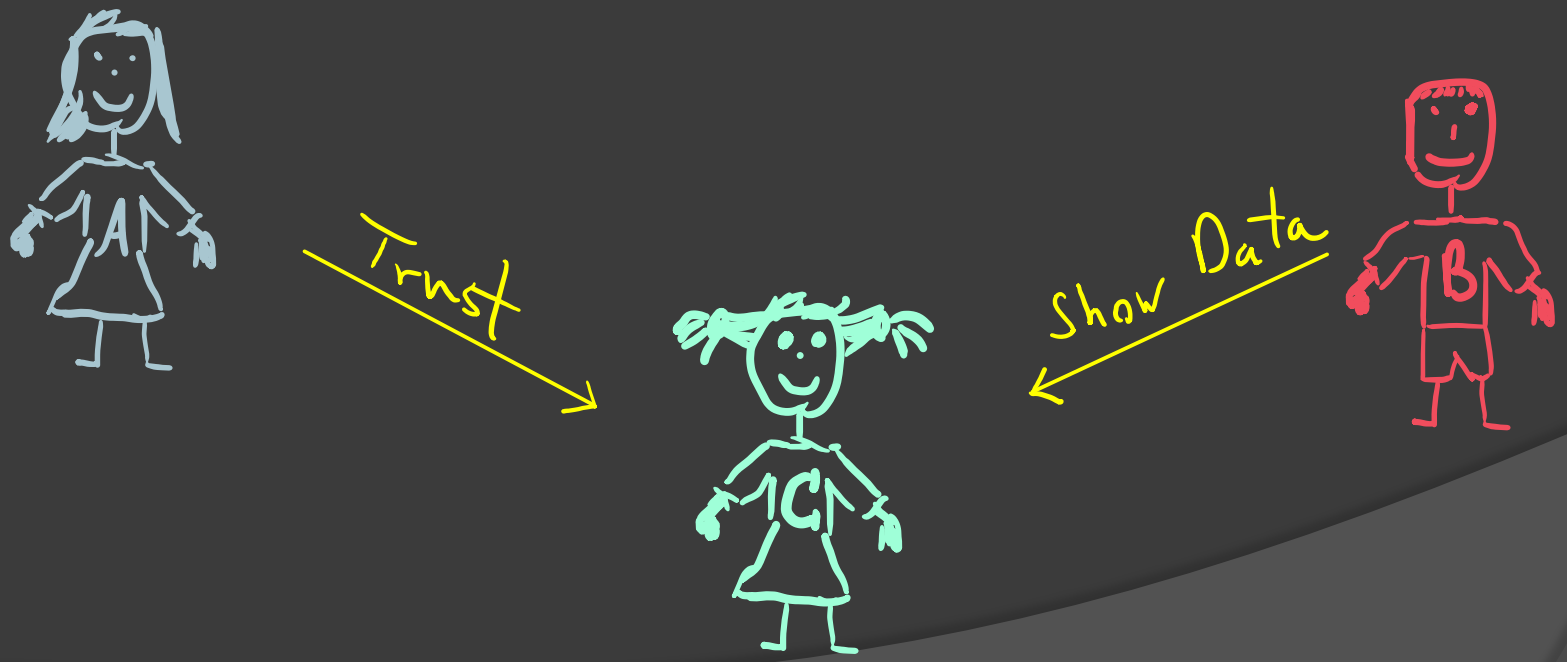
TODAY'S TOP STORIES

Equifax data breach FAQ: What happened, who was affected, what was the impact?

In 2017, attackers exfiltrated hundreds of millions of customer records from the credit reporting agency. Here's a timeline of the security lapses that allowed the breach to happen and the company's response.

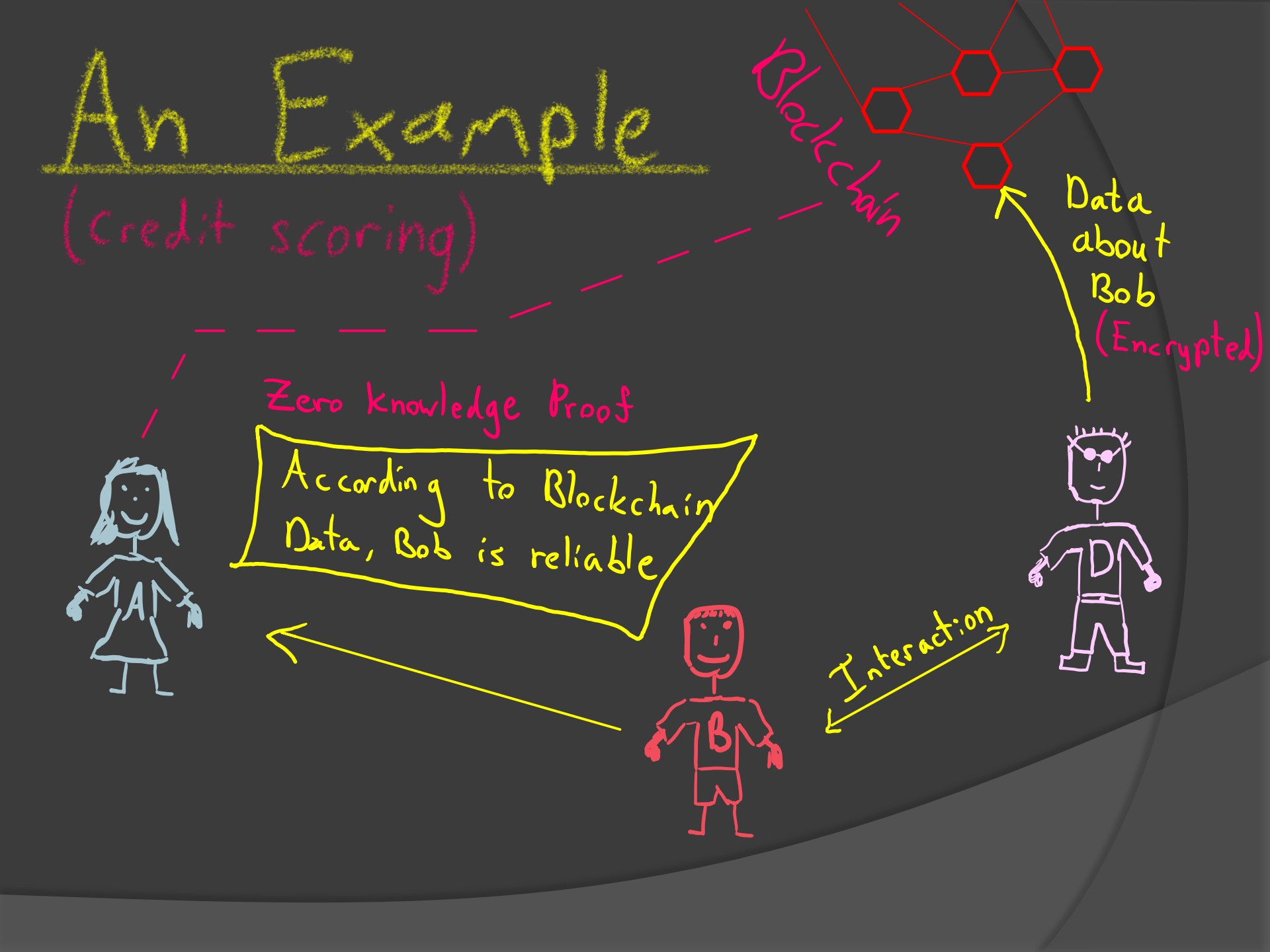
By Josh Fruhlinger

CSO | OCT 14, 2019 3:00 AM PDT



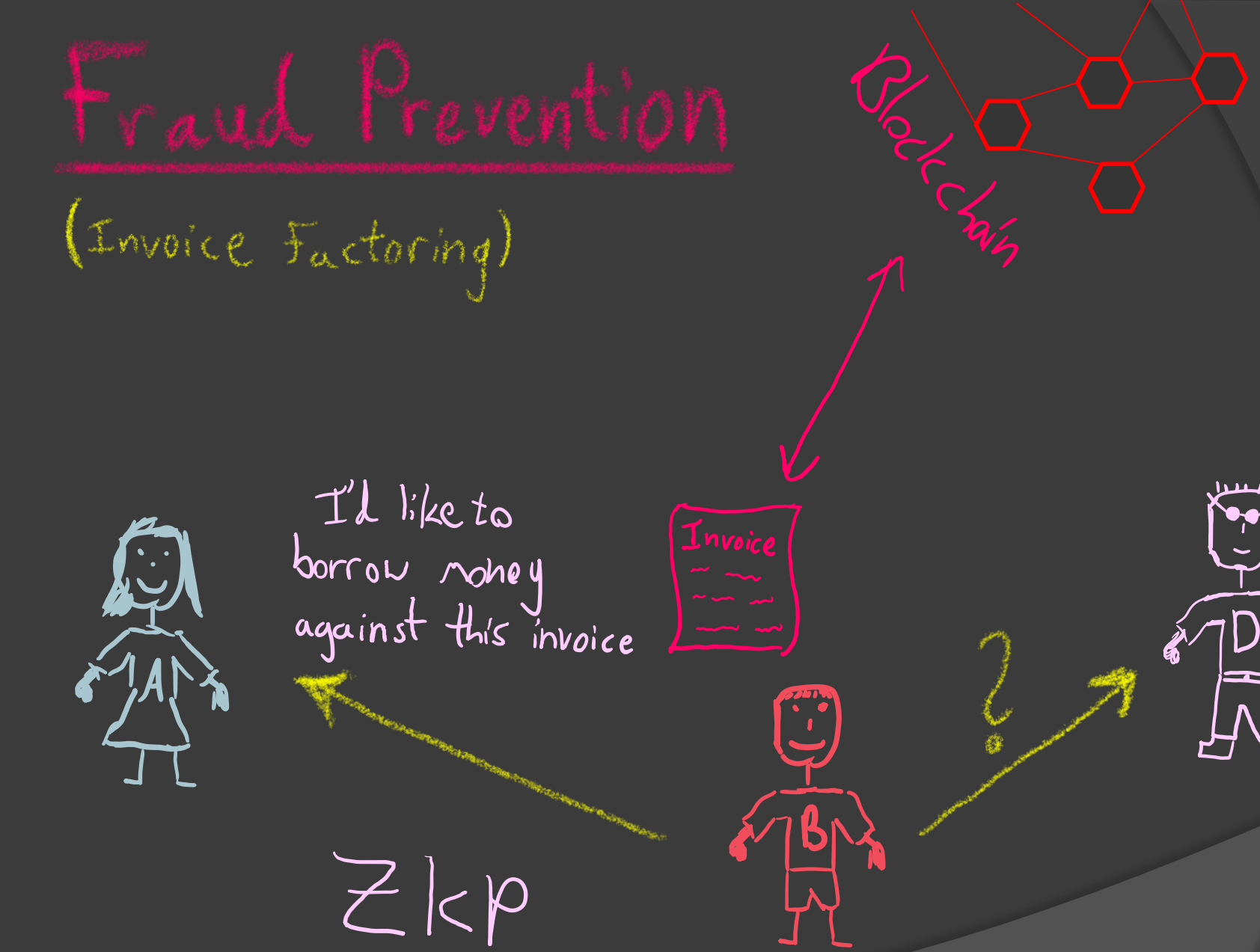
An Example

(credit scoring)

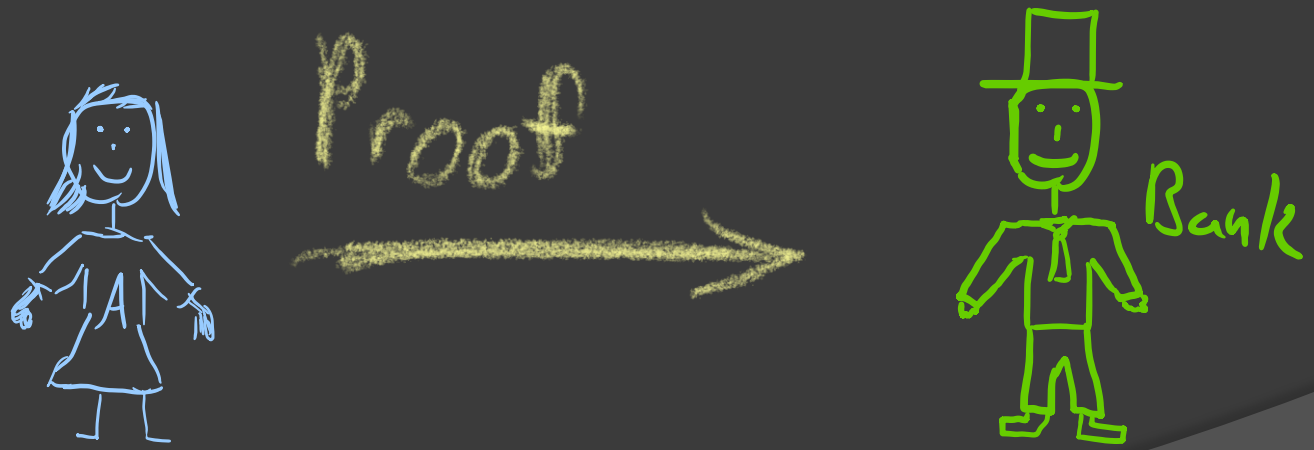


Fraud Prevention

(Invoice Factoring)



- The account I am sending to is private, but it’s not blacklisted
- Transaction is below 10K or was reported to regulator
- I paid taxes on my income (but don’t reveal income amounts)



Many more uses

- KYC
  - I’m an accredited investor
- Insurance
  - I properly maintain my car
  - I get checked by the doctor periodically
- Supply Chain
  - My supplier is on time so I too will supply on time

Summary:

Zero knowledge proofs:

- Enabling a new kind of information economy. Data stays in silo, proofs move around.
- Also extreme privacy in cryptocurrencies
- Can regulate / tax without seeing all data?

Thanks!

For more information:

avivz@cs.huji.ac.il