Privacy is dead, Scalability is boring: ZK proofs, what are they good for?

Ian Miers @secparam

UMD Computer Science

Devcon Bogotá

Privacy is dead is clickbait, but….

- We haven’t seen large demand for private consumer payments
- **What if demand is 10+ years out?**
- And anonymous payments are mostly done research
  - Zero-knowledge proof plus an accumulator
  - Developed in Zerocash,
  - deployed/beta in Zcash, Tornadocash, Aztec, Anoma, Penumbra, Railgun, etc.
  - Sure tweaks:
    - change accumulators or zk proofs
    - Make extra features
- What else do we do with zk proofs?

Privacy is not dead everywhere as a motivator for cryptocurrency

Defi: presumably, financial trading needs confidentiality

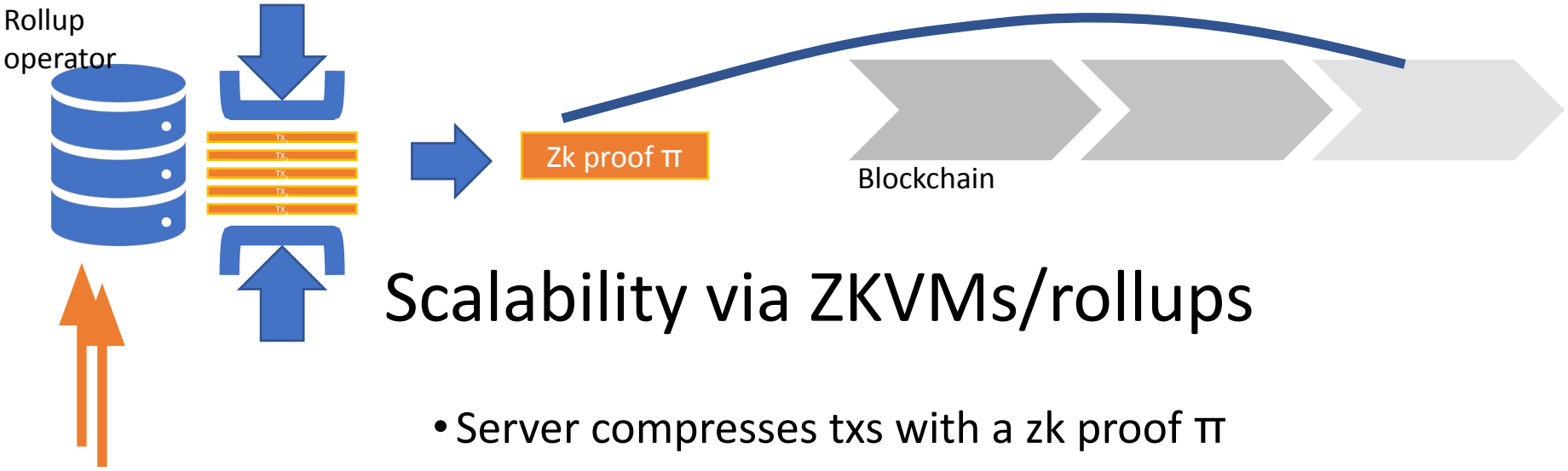
MEV/front running prevention (to the extent zk helps)

But …the core zk protocols still are pretty much known

Blockchains…

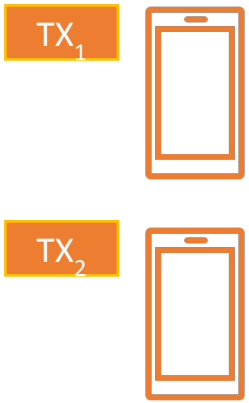
are slow

Zk proofs are supposed to be everything a growing blockchain needs



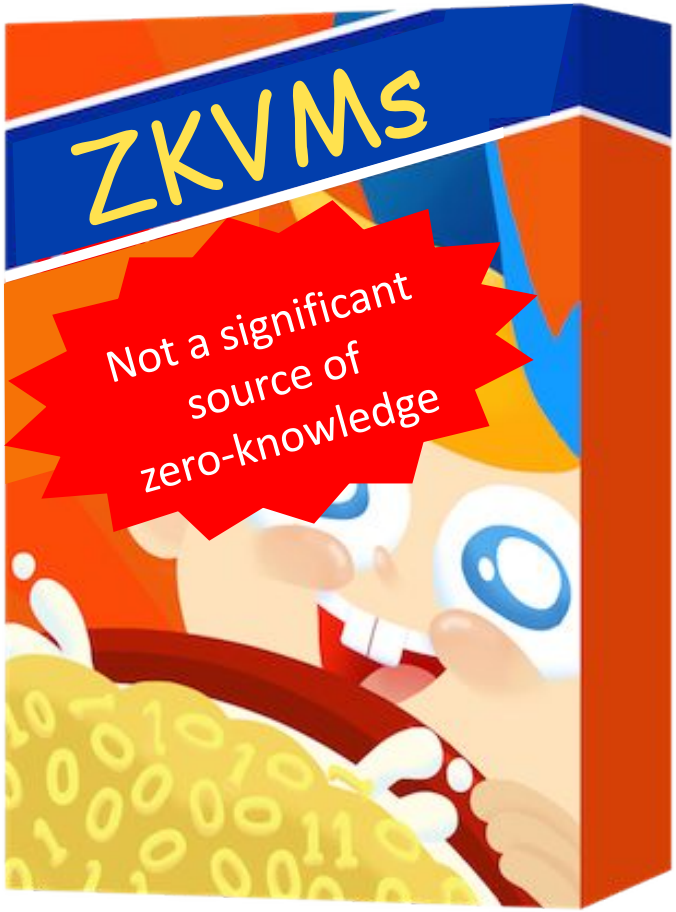
Scalability via ZKVMs/rollups

- Server compresses txs with a zk proof π
- Server submits proof π to the blockchain
- Verifying the proof π on chain is faster than checking all transactions
- It doesn't matter if your chain does 10 transactions per second if each transaction has 10k payments in it.



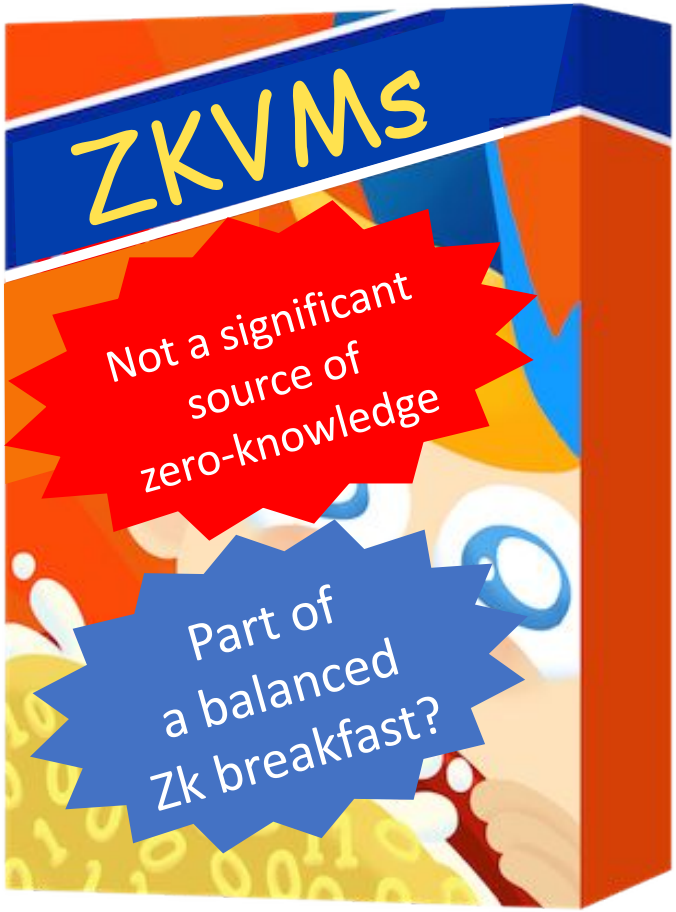
ZkVMs/ rollups aren’t even zk

- “Zk” VMs compress TXs to scale blockchains
- Scalability doesn’t require you hide data
- ZKVMs/rollups likely won’t hide data
  - Zk rollups reveal a merkle hash of data
  - Like publishing Hash(password)
- Boring from a zk standpoint:
  - Sure, you need fast proofs
  - But it’s the zero-knowledge part that’s cool



Scalability isn't zk, but

- Scaling is driving innovation in zk proofs
- Like 80s/90s computer processors
  - Need for faster spreadsheets drove development
  - Some people nerded out on fast/better microchips
  - But people also dreamed bigger
- We need to dream bigger for zk+blockchains



What are zero-knowledge proofs good for?

What is a zero-knowledge proof?

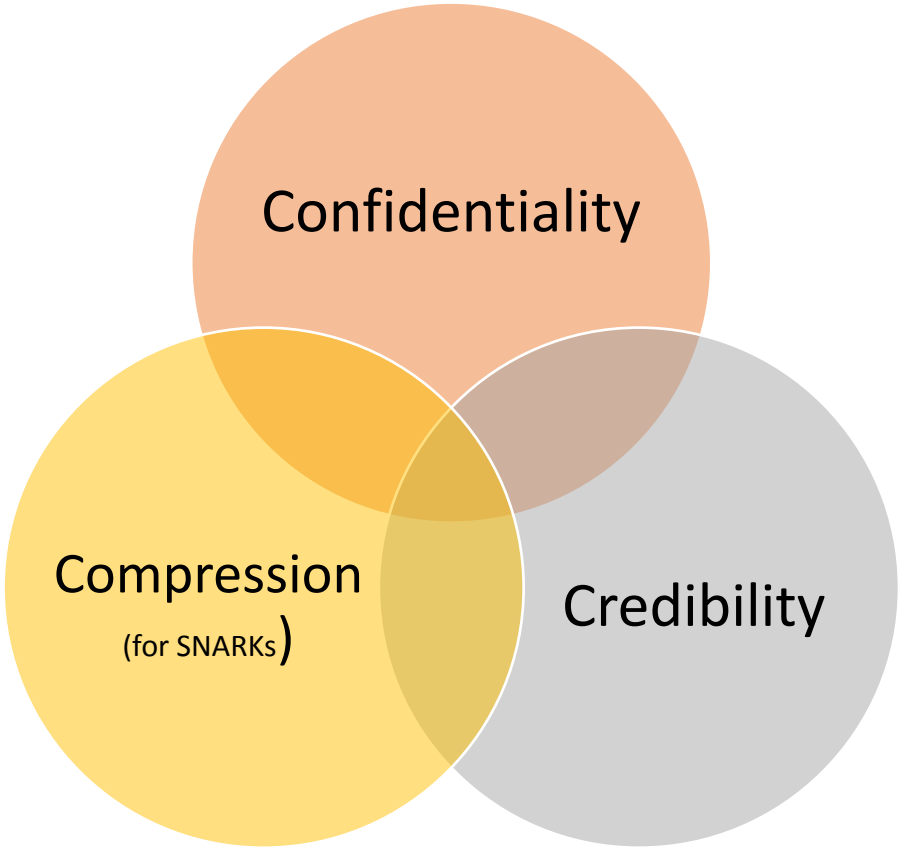
A prover P proves to a ve…some statement is true ***without*** revealing any othe…rmation

Prope…

- Correct…P can convince V
- Soundness:…nnot lie
- Zero-knowledg…oes not lea…ything else but that a statement is true
- (much latter) succinct…p…s tiny regardless of statement size

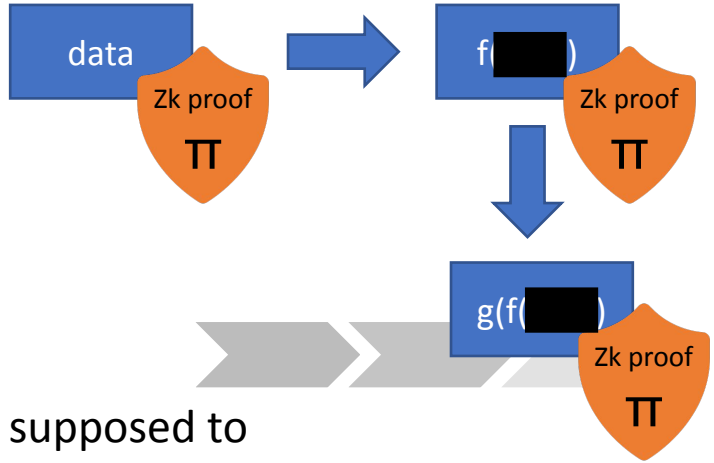
What are zk proofs doing?

(in deliberately non-standard terminology)

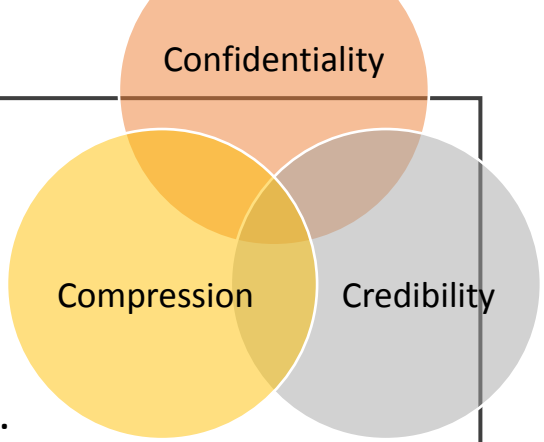


Credibility carrying data from blockchains +zk proofs

- Proof carrying data(CT10)
  - Data has proofs,
  - Can redact data
  - But how do you agree on data?
  - What do is it good for?
- Zk proofs + blockchains give us credibility
  - Someone started with the right data
  - They didn't see anything they weren't supposed to
  - They did the correct thing
  - And it's a shared consensus this happened without equvication



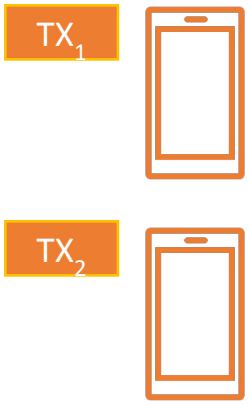
What are ZK proofs good for?



Sure, privacy, but also …..

- Credible safety for/from rollup operators (aka censorship resistance)
- Credibility for markets, migrated data, and, money laundering prevention
- Identity, moderation, and decentralized social media

Photo: Suzanne Hamilton cc-by-nc-nd-2

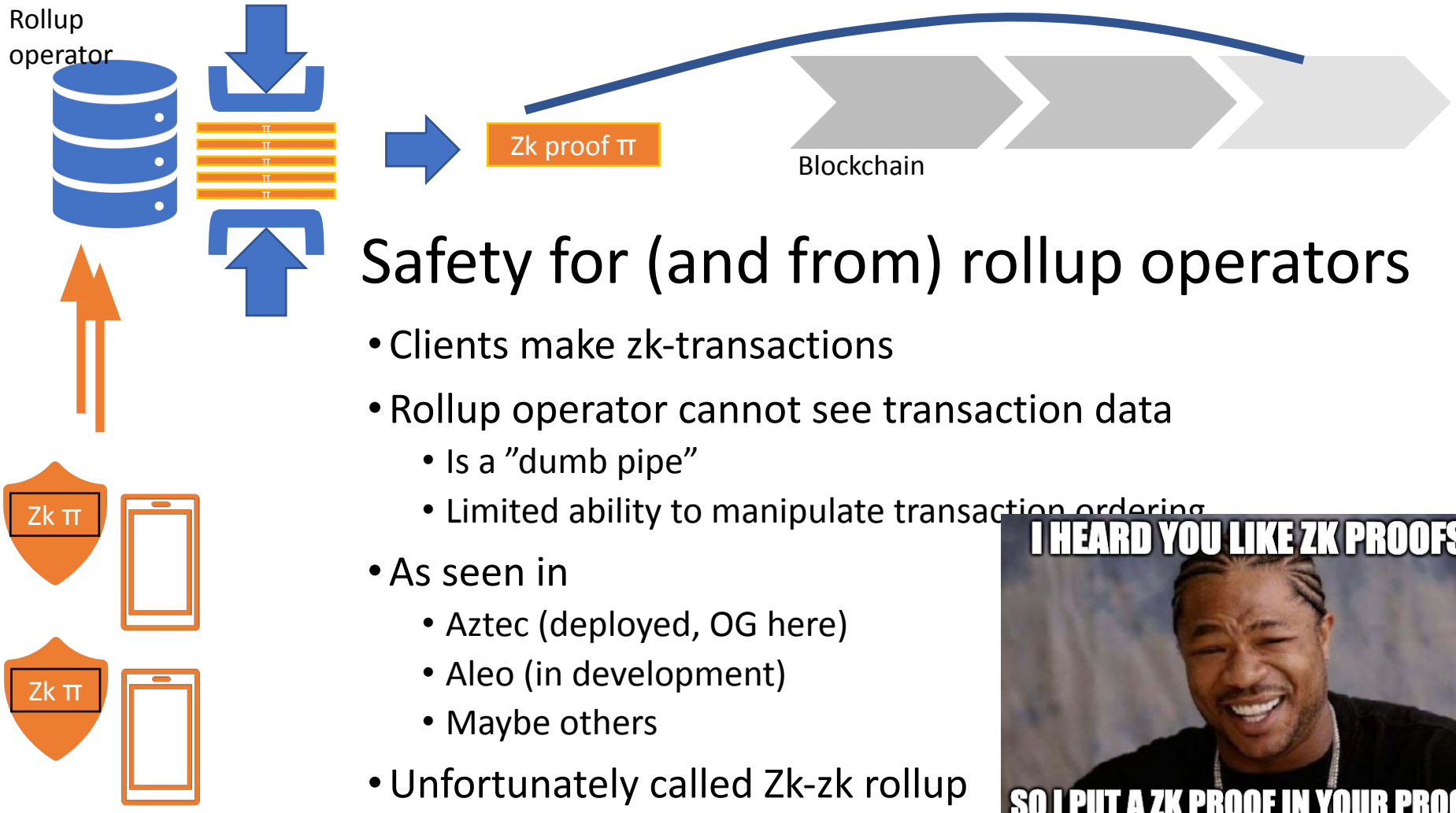


A ZKVM/rollup compresses transactions with a zk proof :

Server sees inside transactions	Server ***can*** exclude transactions	Server will be responsible for ***not*** excluding them

ZKVMs/ Rollups aren't censorship resistant

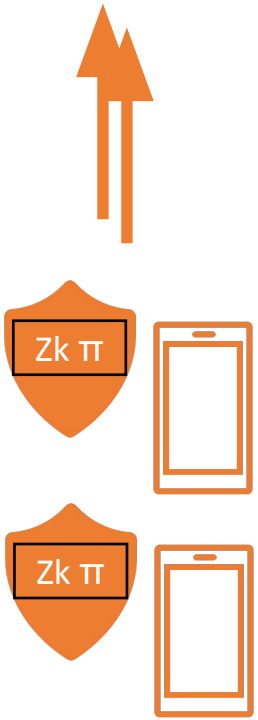
Better not mint any NFT'd memes some government hates



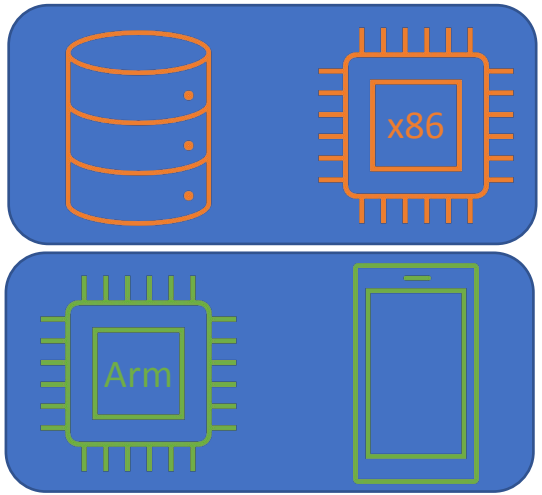
Safety for (and from) rollup operators

- Clients make zk-transactions
- Rollup operator cannot see transaction data
  - Is a ”dumb pipe”
  - Limited ability to manipulate transaction ordering
- As seen in
  - Aztec (deployed, OG here)
  - Aleo (in development)
  - Maybe others
- Unfortunately called Zk-zk rollup

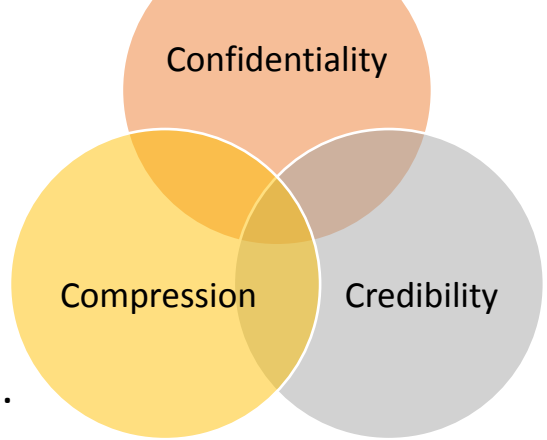
Not all zk tech will keep rollup operators safe



- Zk-zk rollups require zk proving on consumer devices
- Not all proof systems suitable
- Risk factors :
  - Provers architected for data centers
  - Proof cost must be amortized over many transactions
  - Proofs are very large
- Akin to Intel/x86 ‘s mobile challenges
- May need to add another nested zk proof system



What are ZK proofs good for?



Sure, privacy, but also …..

- Credible safety for/from rollup operators (aka censorship resistance)
- **Credibility more broadly: markets, migrated data, and money laundering prevention**
- Credible Identity, moderation, and decentralized social media

Cryptocurrency has some theft problems

HOME > NEWS > CURRENCIES

North Korea has laundered $1 billion in crypto via Tornado Cash - and the US Treasury just slammed the platform with sanctions

Phil Rosen Aug 8, 2022, 1:38 PM

Credibility: Zk chains of custody

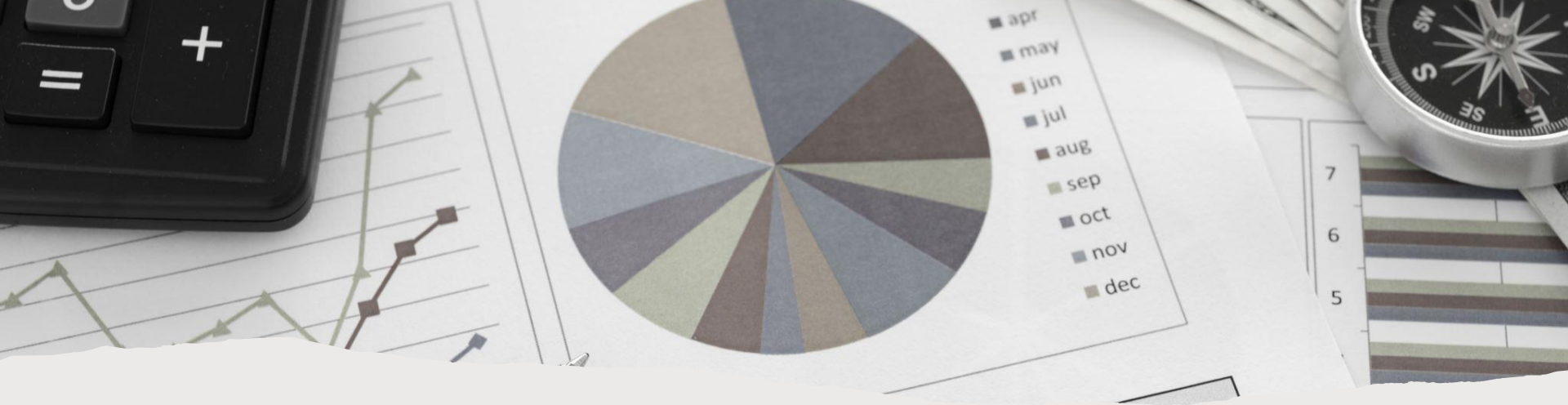
What if you could prove your money was not stolen?

And who you got it from didn't steal it

- And ….

Impossible by just asking questions, checking data, etc….

Zk proofs compose recursively



Credible compliance and money laundering prevention

- Abide by currency transaction reports (CTRs) for large payments (GG**M**16)
- Show you are not on a sanction list

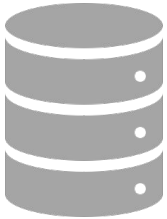
Credibility more broadly

Prove:

- Data is correct when migrating between competing services
- Auctions weren't tampered with
- Matching markets (like Uber) weren't manipulated
- News feed weren't manipulated

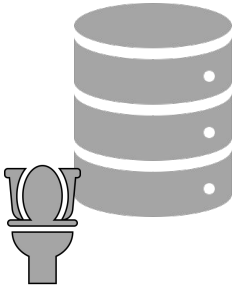
Not just is credibility nice, if we want to decentralize existing services, organizations and institutions, its essential. And we can't just publish everythong

Credibility: portability for online gaming



- Awesome game, server, + community

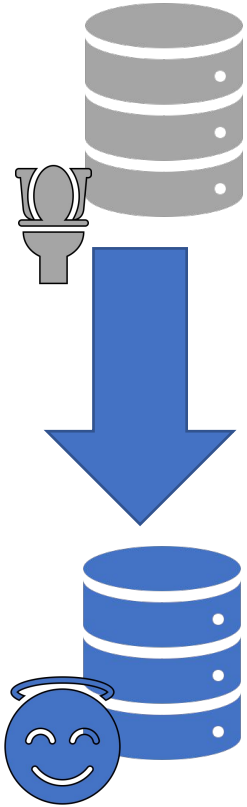
Credibility: portability for online gaming



- Awesome game, server, + community
- Devs get bought/greed -> ruin the game

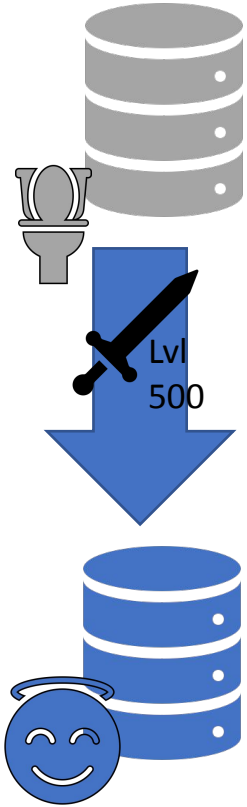
Credibility: portability for online gaming

- Awesome game, server, + community
- Devs get bought/greed -> ruin the game
- Lets take game state/ items to a new server, better server



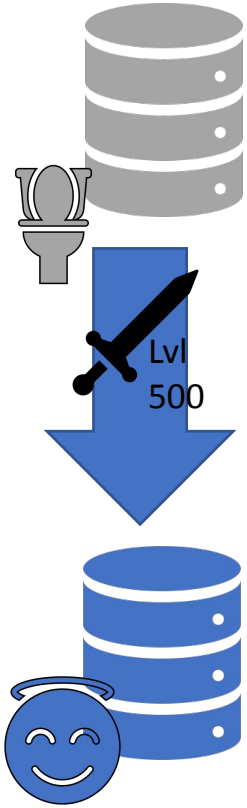
Credibility: portability for online gaming

- Awesome game, server, + community
- Devs get bought/greed -> ruin the game
- Lets take game state/ items to a new server, better server
- Credibility for users:
  - Is that level 500 sword real?



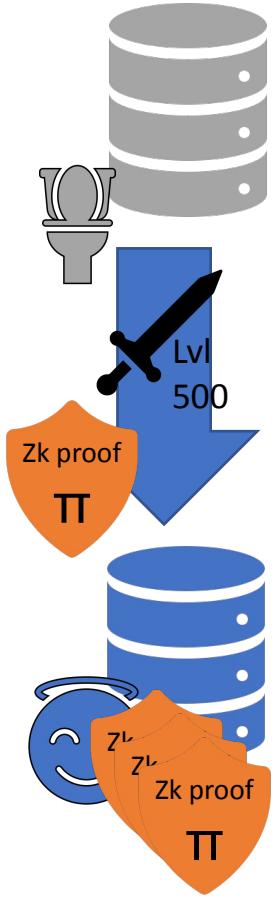
Credibility: portability for online gaming

- Awesome game, server, + community
- Devs get bought/greed -> ruin the game
- Lets take game state/ items to a new server, better server
- Credibility for users:
  - Is that level 500 sword real?
- Credibility for the server:
  - Prove items aren’t pay to play
  - In game economy was correct



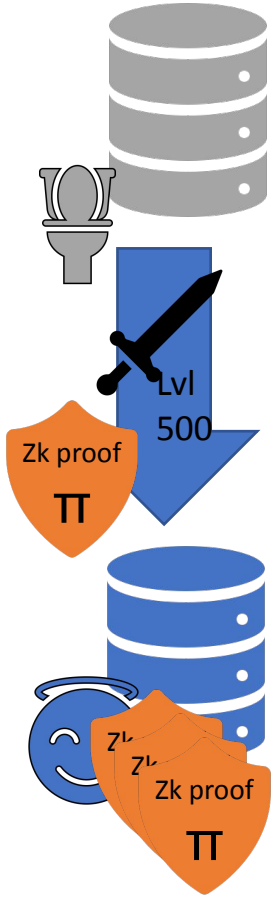
Credibility: portability for online gaming

- Awesome game, server, + community
- Devs get bought/greed -> ruin the game
- Lets take game state/ items to a new server, better server
- Credibility for users:
  - Is that level 500 sword real?
- Credibility for the server:
  - Prove items aren't pay to play
  - In game economy was correct



Credibility: portability for online gaming

- Awesome game, server, + community
- Devs get bought/greed -> ruin the game
- Lets take game state/ items to a new server, better server
- Credibility for users:
  - Is that level 500 sword real?
- Credibility for the server:
  - Prove items aren't pay to play
  - In game economy was correct
- Not feasible with current tech, but a tractable goal
- Broadly applicable to data portability +market competition



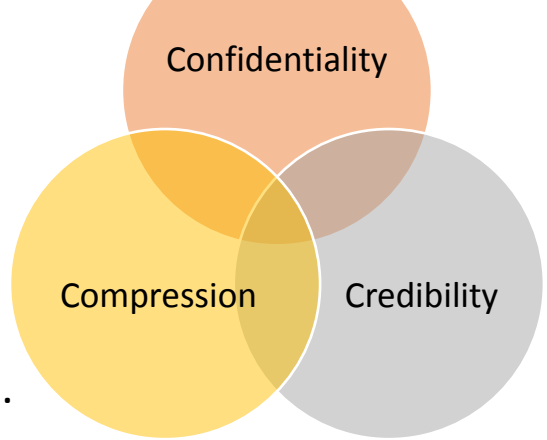
Thinking even bigger: Credible institutions

- What would it take to know the IRS is credible?
- Need to commit to
  - Audit policy
  - All tax returns for that year
- Show correct process was applied
- Can’t reveal anything publicly
- With zk proofs + blockchains of committed data, its (maybe)(eventually) possible

Verification enables cooperation

- US and the USSR want less nukes
- Verifying compliance with agreements is hard
- Technical advances enabled verification and more cooperation
- But for many applications, simple transparency isn't viable, we need zk proofs

What are ZK proofs good for?



Sure, privacy, but also …..

- Credible safety for/from rollup operators (aka censorship resistance)
- Credibility more broadly: markets, migrated data, and money laundering prevention
- **Credible Identity, moderation, and decentralized social media**

Identity

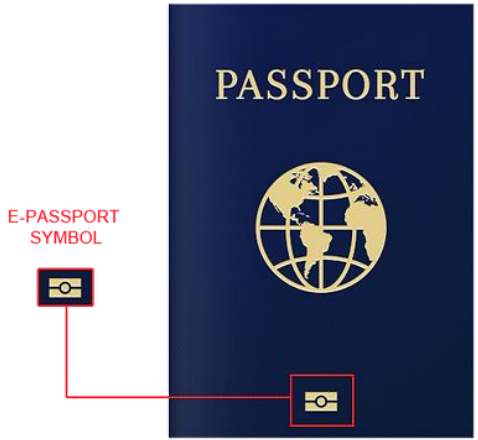
We are required to prove many things about ourselves

- not a North Korean Money launderer
- not a bot
- Over 18 to view a video

Zkcreds:Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure

Michael Rosenberg, Jacob White, Christina Garman, and Ian Miers

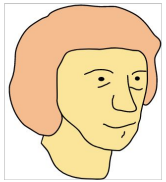
- Zk proof identity framework
- No new trusted issuers or keys, just a list
  - List can be on a blockchain
- Example application: > 18 years old
  - Zk proof to convert passport to credential
  - Zk proof to show you your over 18
- Supports
  - cloning resistant credentials
  - Arbitrary identity credicats



Snarkblock (IEEE S&P 2022): decentralized blocklisting of annoying anonymous users

- You have a sybil resistant account
- You can post anonymously across the internet
- If one of your posts is on a blocklist, you can't post on any service that uses that list
  - Even though the service has no idea who you are
- Blocklists can be managed by anyone, and mixed and matched
- For every post, you prove the pseudo-random tags for your previous posts aren't on the block list

k_A

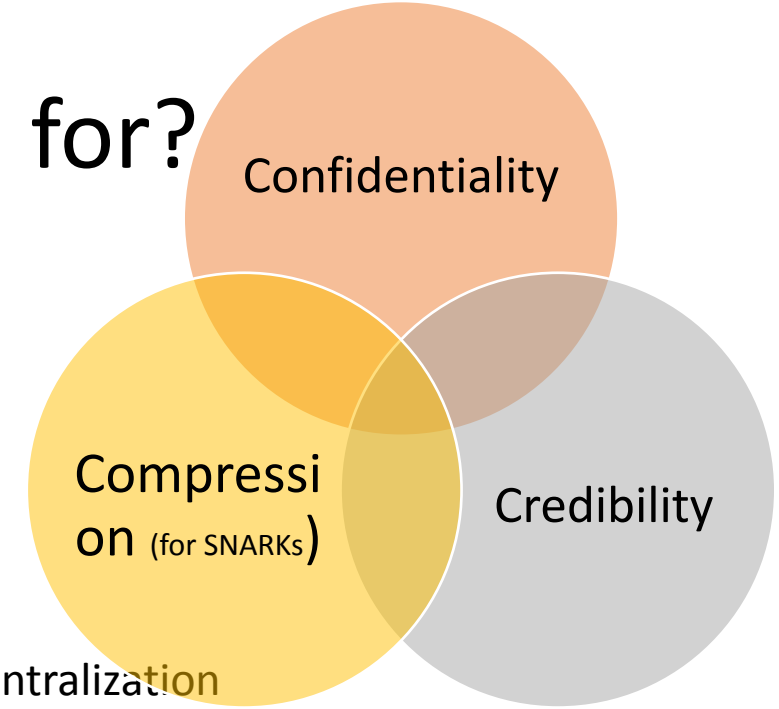


$\text{nonce}' \leftarrow \mathbb{F}$

$\text{tag}' = \text{PRF}_{k_A}(\text{nonce}')$

$\pi =$ "I know k_A such that
$\text{tag}' = \text{PRF}_{k_A}(\text{nonce}')$
AND
$\text{tag}_1 \neq \text{PRF}_{k_A}(\text{nonce}_1)$ ...
AND $\text{tag}_N \neq \text{PRF}_{k_A}(\text{nonce}_N)$"

What are zk proofs good for?



Takeaways

- ZKVMs/rollups aren't zk
  - Wont need zk for scale:
  - Won't provide it: like publishing your password hash + a proof about it.
- We need zk-zk rollups for safety/censorship resistance
- We can use zk proofs for so much more:
  - Supporting data portable/ completion/ decentralization
  - Identity and distributed social media
- Zk proofs+ blockchains give us credibility carrying data
  - The right thing was done, with the right data, and the right things kept secret