Efficient Zero-Knowledge Proofs: Theory and Practice

Jiaheng Zhang

jiahengzhang1996@gmail.com

Verification

Verify Account

Verify Your Email Address

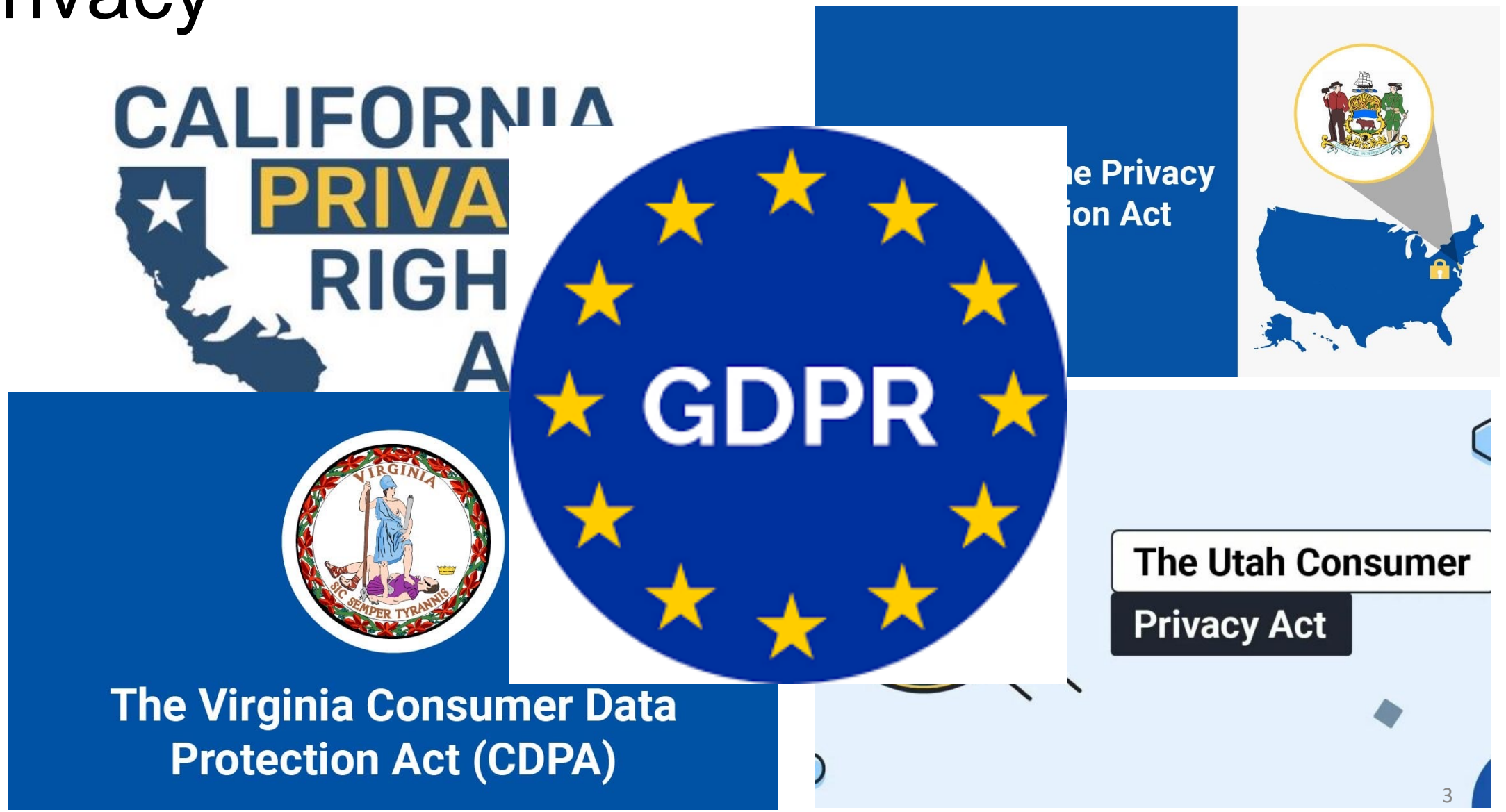
To continue using Brazen, please verify your email address:

alexa+needstoverify@brazen.com

SEND VERIFICATION EMAIL

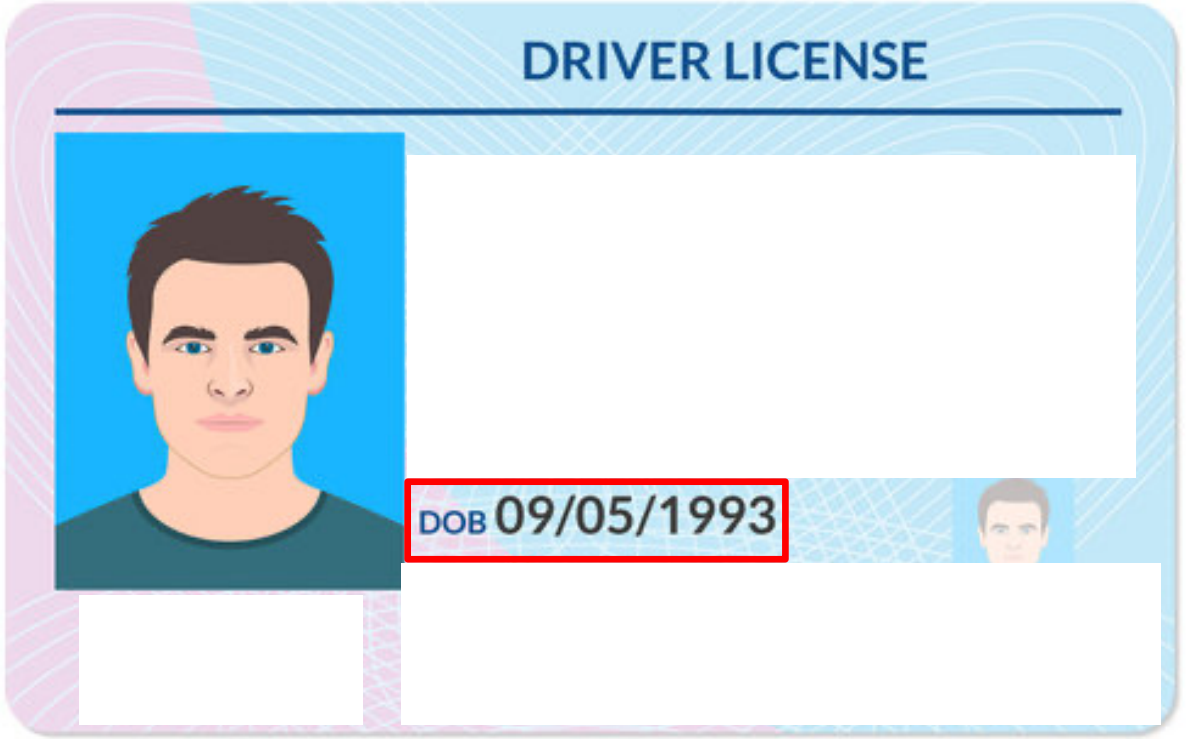
Trouble Verifying?

Privacy

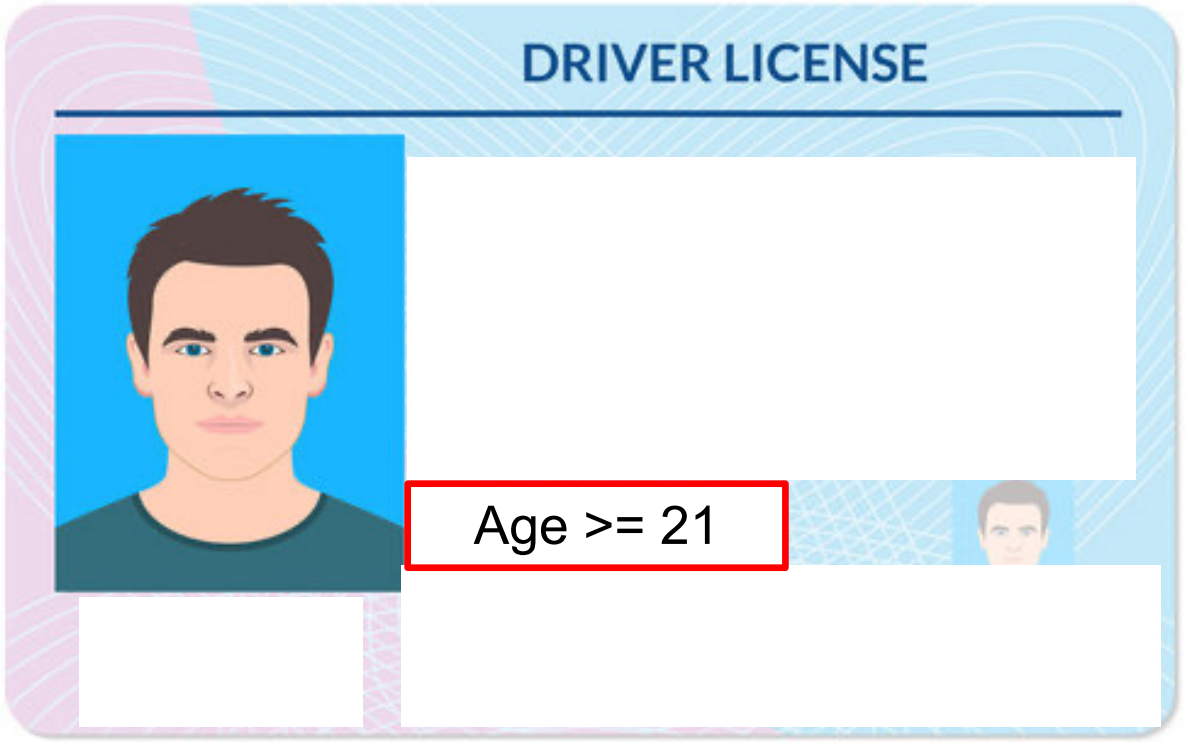

CALIFORNIA
PRIVA
RIGH
A
GDPR
e Privacy
ion Act
VIRGINIA
SIC SEMPER TYRANNIS
The Virginia Consumer Data Protection Act (CDPA)
The Utah Consumer
Privacy Act

Verification and Privacy

Verification and Privacy



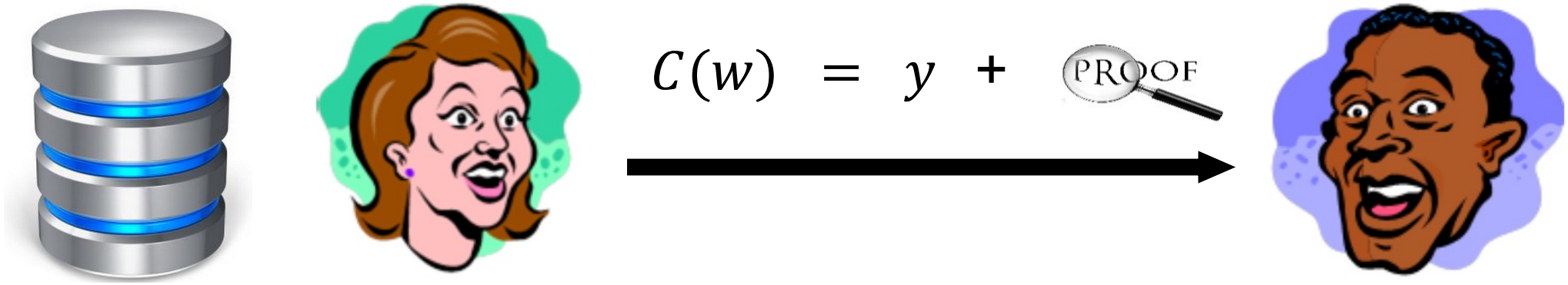
Verification and Privacy



Verification + Privacy = Zero-Knowledge Proof

Zero-Knowledge Proof (ZKP) [GMR 85]

Verification: ✓ **or** ✘



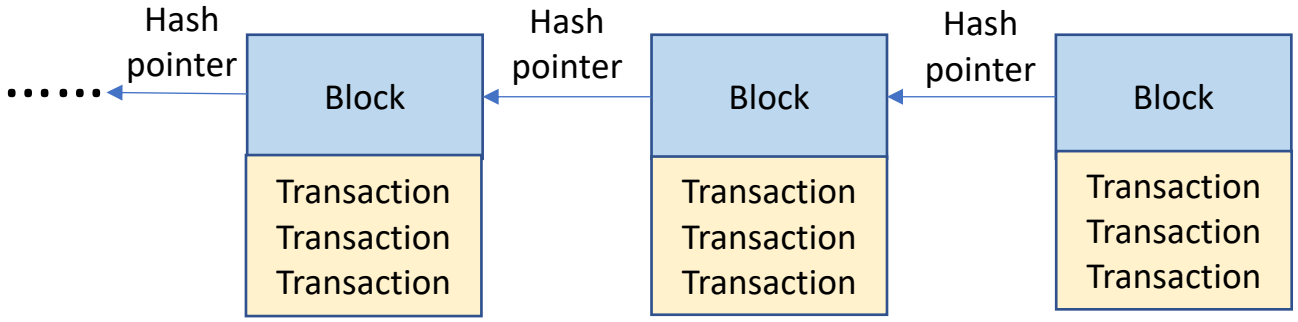
Witness: w Prover Verifier

- Completeness: if $C(w) = y$ then verification is ✓
- Soundness: if $C(w) \neq y$ then verification is ✘

} Verification

- Zero knowledge: proof leaks no information about w → Privacy

Applications on Blockchain and Cryptocurrency



Issues:

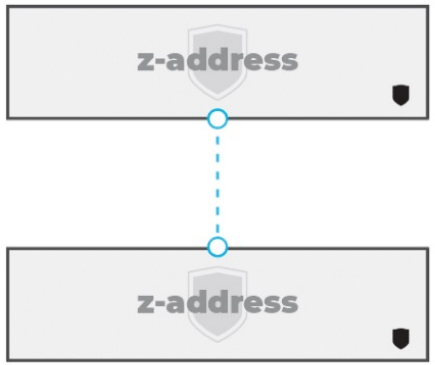
Privacy. Transparent data on blockchain.

Scalability. Bitcoin 7TX/s v.s. Visa 24,000TX/s

Solution: Zero-knowledge proof

Privacy-preserving transaction

Zcash

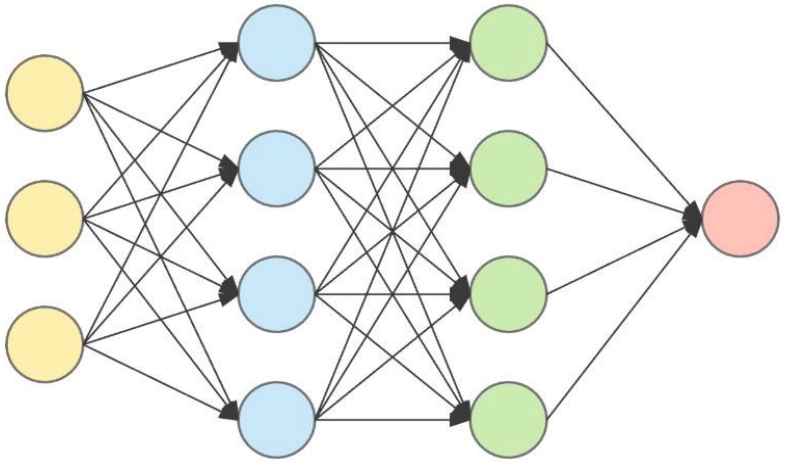


ZKRollup

1. Generate *proof* for transaction execution.
2. Others check *proof* instead of validating one-by-one.

Applications on Machine Learning

Secret ML Model



Prover

PROOF

Model property

• Accuracy

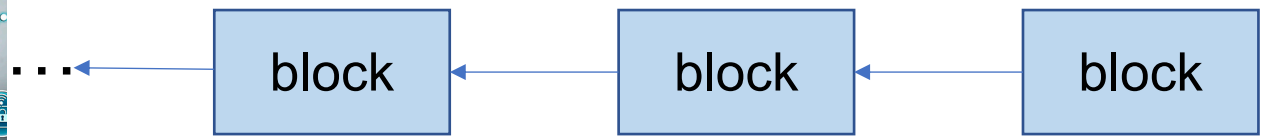
Verifier

Stock prediction

Healthcare with ML

Marketplace on blockchain

PROOF



Popularity of ZKP

True internet privacy could finally become possible thanks to a new tool that can—for instance—let you prove you're over 18 without revealing your date of birth, or prove you have enough money in the bank for a financial transaction without revealing your balance or other details. That limits the risk of a privacy breach or identity theft.

The tool is an emerging cryptographic protocol called a zero-knowledge proof. Though researchers have worked on it for decades, interest has exploded in the past year, thanks in part to the growing obsession with cryptocurrencies, most of which aren't private.

Perfect Online Privacy

Breakthrough

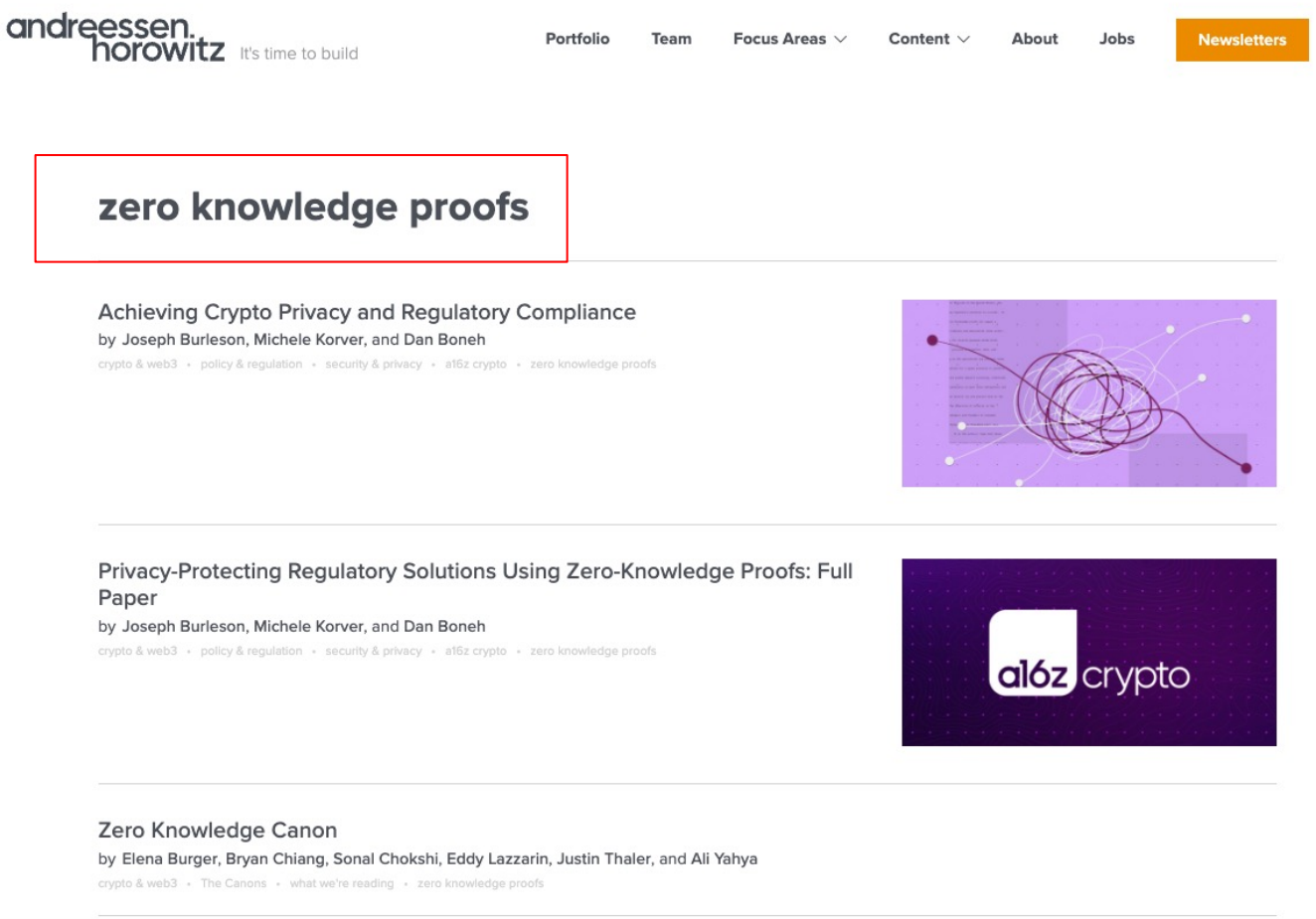
Computer scientists are perfecting a cryptographic tool for proving something without revealing the information underlying the proof.

Why it matters

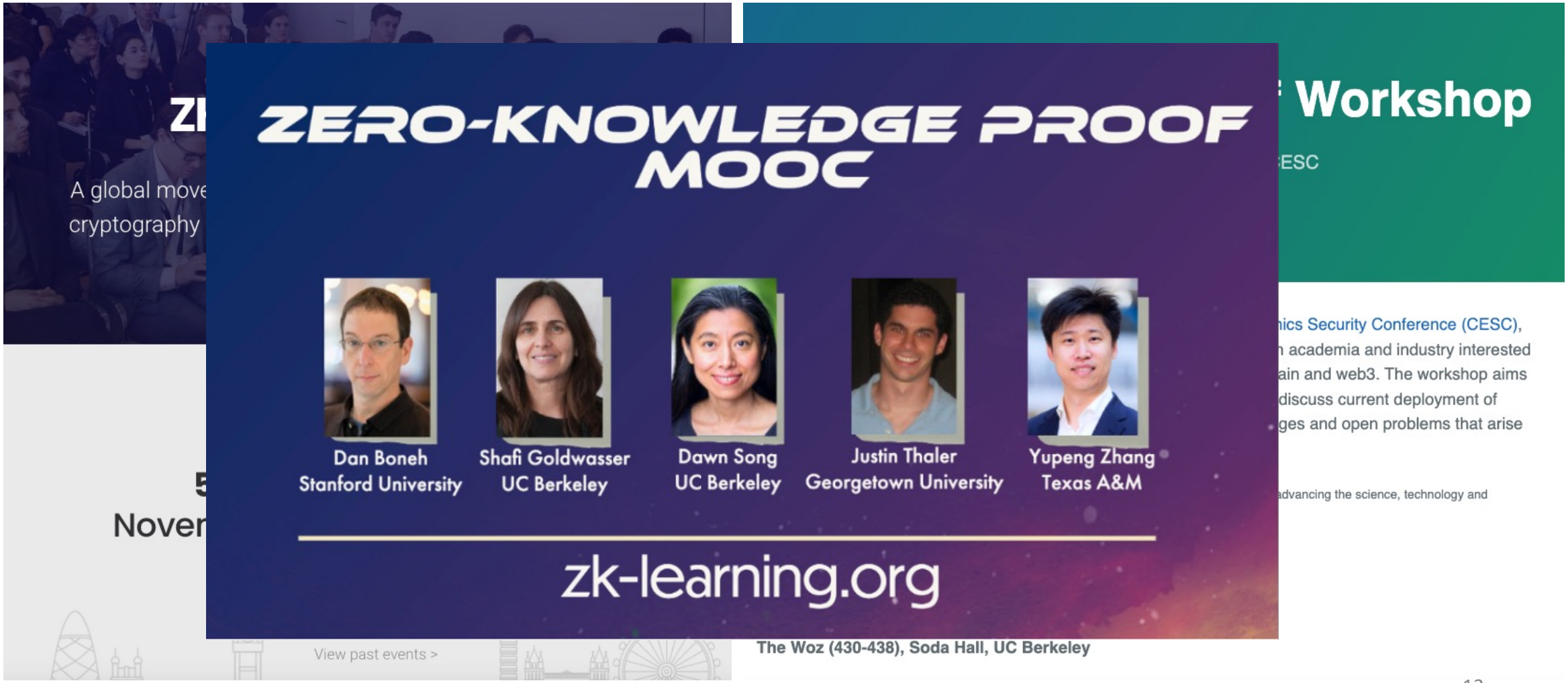
If you need to disclose personal information to get something done online, it will be easier to do so without risking your privacy or exposing yourself to identity theft.

Key players

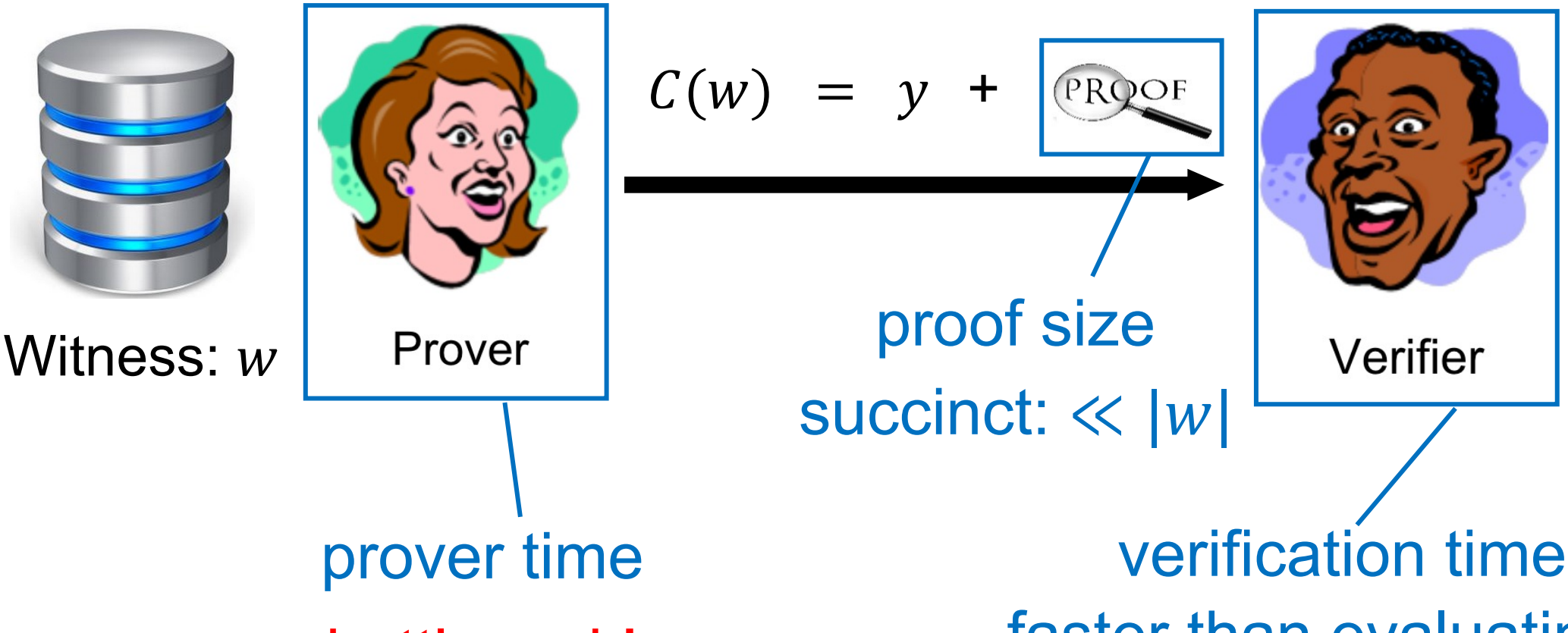
Zcash; JPMorgan Chase; ING



Workshops and MOOC of ZKP



What is a Good ZKP?



Example: Matrix Multiplication

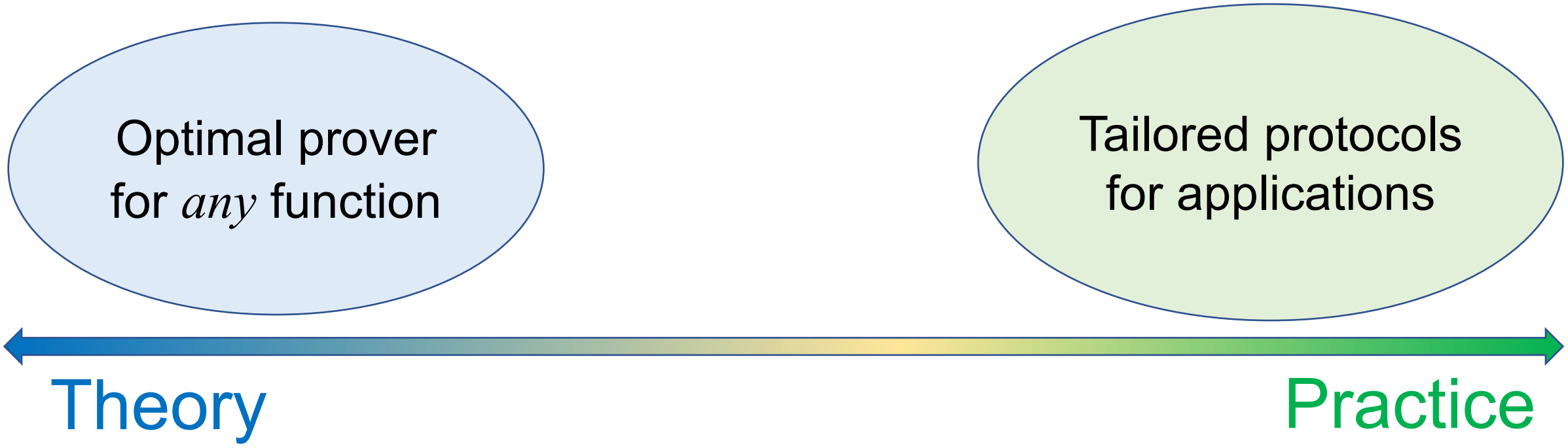
$C(w) = w \cdot w = y$
w is a 256 x 256 matrix

Generate ZKP by Groth16 [protocol used in Zcash]

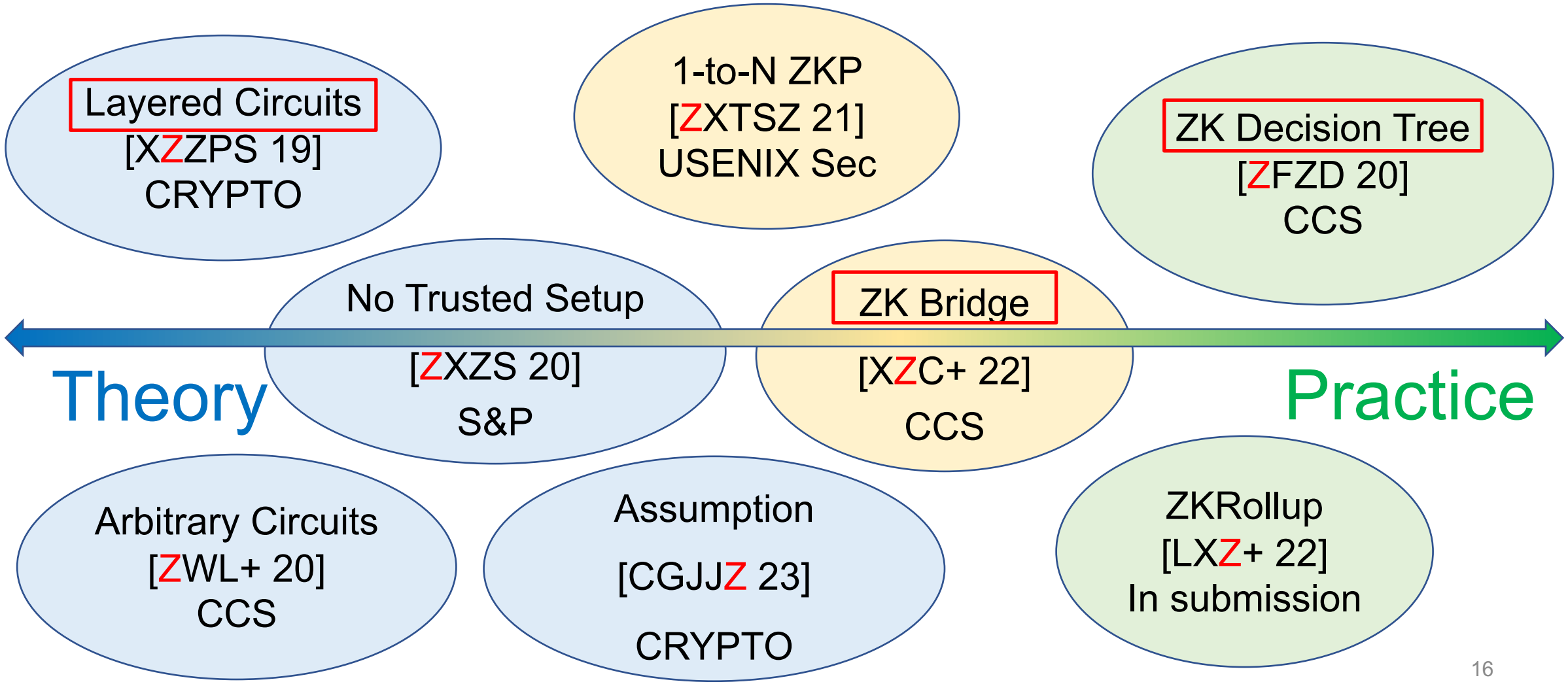
- Proof size: 192 bytes
- Verification time: 3ms
- Prover time: >1000s

*Data from https://github.com/ConsenSys/gnark

My Work on ZKP



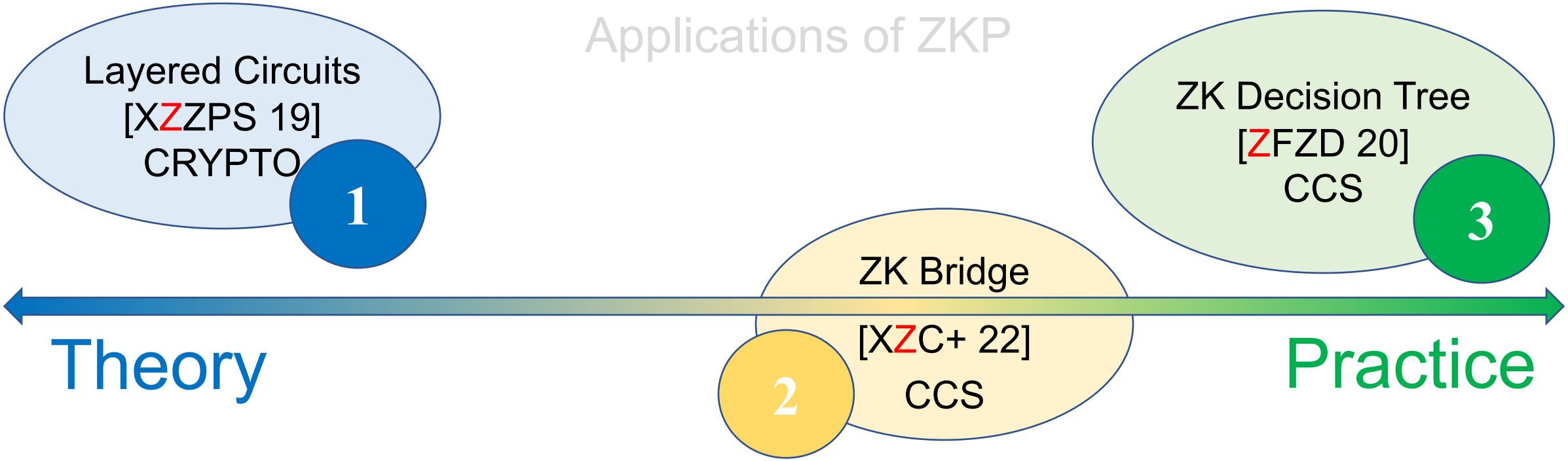
My Work on ZKP



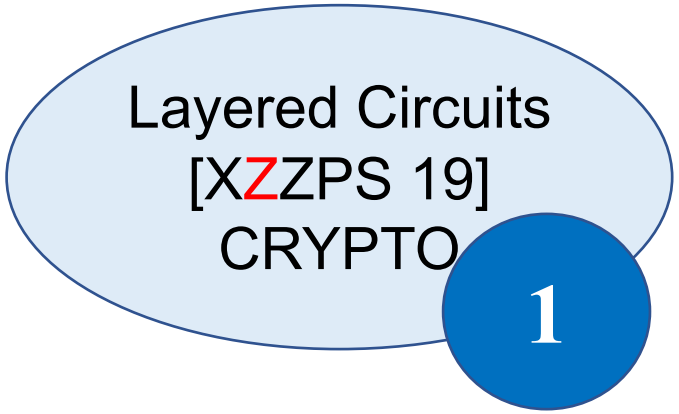
Outline

What is ZKP

Applications of ZKP



Future Work



Libra: Succinct Zero Knowledge Proofs with Optimal Prover Computation

Theory

Practice

GKR protocol [GKR 08]

Layered Arithmetic Circuit C

w

Prover

$C(w) = y$

Verifier

w

No zero-knowledge

Sumcheck Protocol [LNFK 92]

$$H = \sum_{b \in [n]} f(b) = f(0) + \cdots + f(n-1)$$

Prover

proof, $f(r)$

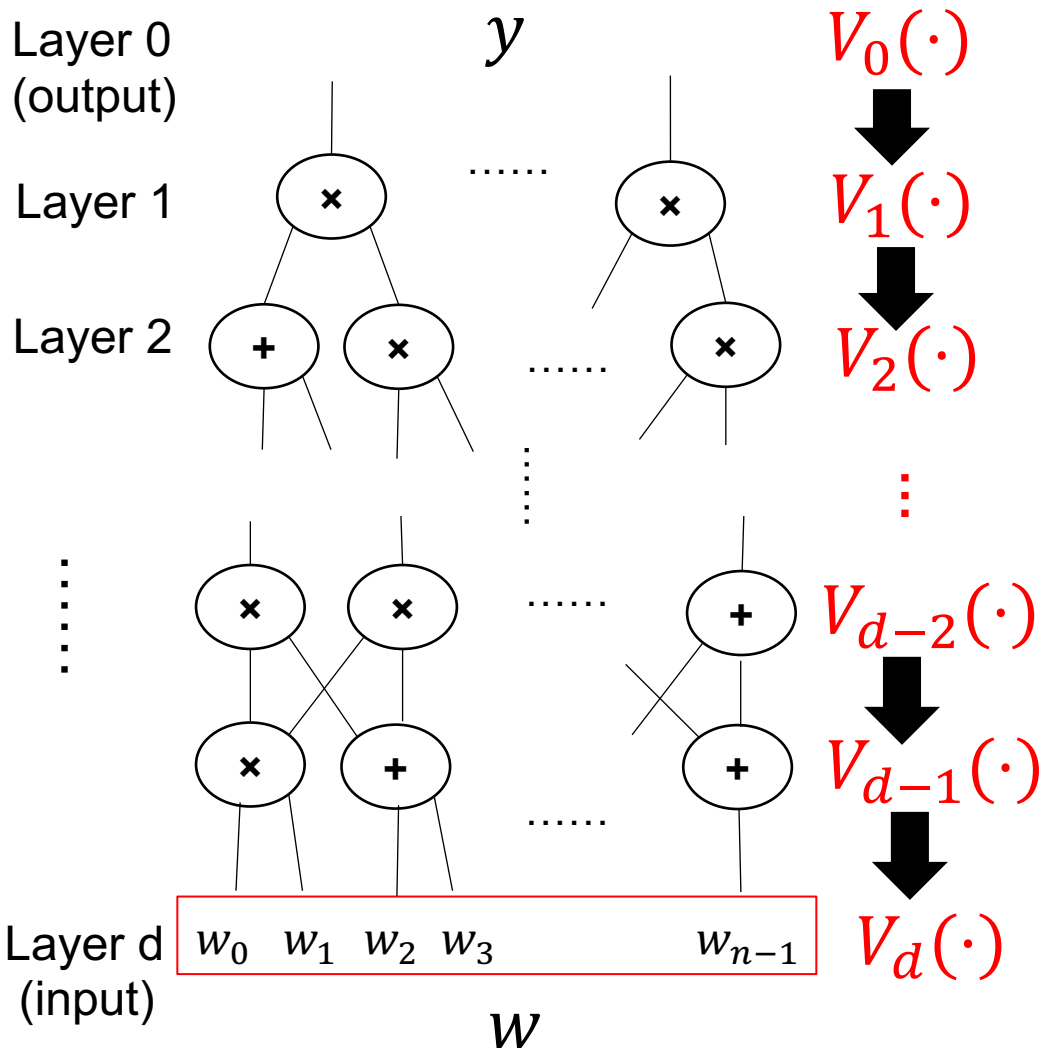
Verifier

Succinct proof size: $O(\log n)$

Fast verifier time: $O(\log n)$ + $f(r)$

GKR protocol

Layered Arithmetic Circuit C



sumcheck protocol

$$V_i(r_i) = \sum_{b \in [n]} f(V_{i+1}(b))$$

$V_i(r_i) \rightarrow V_{i+1}(r_{i+1})$

Example: $n = 8$

$V_d(0) = w_0$

$V_d(1) = w_1$

$\cdots$

$V_d(7) = w_7$

Build ZKP on top of GKR protocol

✓ Light operations (addition + multiplication).
✓ Succinct proof size and fast verifier time.

× No practical prover time: $O(|C|^3)$.
× No zero-knowledge (privacy).

* $|C|$ is the number of gates in circuit C.

Contributions of Libra [XZZPS 19]

- GKR with Optimal Prover Time.

- Achieve Zero-Knowledge Efficiently.

Optimal Prover Time

$O(|C|^3)$ [GKR 08]

$O(|C| \log |C|)$ [CMT 12]

Regular circuits

$O(|C|)$ [T 13]

Circuits with N same copies

$O(|C| \log \frac{|C|}{N})$ [T 13]

$O(|C| + \frac{|C|}{N} \log \frac{|C|}{N})$ [WJB+ 17]

Circuits with N different copies

$O(|C| \log \frac{|C|}{N})$ [ZGK+ 18]

Optimal Prover Time

$O(|C|^3)$ [GKR 08]

$O(|C| \log |C|)$ [CMT 12]

Regular circuits

$O(|C|)$ [T 13]

Circuits with N same copies

$O(|C| \log \frac{|C|}{N})$ [T 13]

$O(|C| + \frac{|C|}{N} \log \frac{|C|}{N})$ [WJB+ 17]

Circuits with N different copies

$O(|C| \log \frac{|C|}{N})$ [ZGK+ 18]

$O(|C|)$ for arbitrary layered circuits [XZZPS 19]

0.41μs/gate

Technical overview

Each gate takes in two input gates

Sumcheck in GKR

$$V_i(r_i) = \sum_{b,b' \in [n]} f(V_{i+1}(b), V_{i+1}(b'))$$

$O(n^3)$ [GKR 08]

Run f for each $b \in [n], b' \in [n]$

$O(n \log n)$ [CMT 12]

Compute $O(n \log n)$ $f\left(V_{i+1}(b), V_{i+1}(b')\right) \neq 0$

$O(n)$ [XZZPS 19]

Phase 1: $O(n)$ sumcheck on b

$\sum_{b \in [n]} \left\{ \sum_{b' \in [n]} f\left(V_{i+1}(b), V_{i+1}(b')\right) \right\}$

Phase 2: $O(n)$ sumcheck on b'

$$\sum_{b' \in [n]} f(V_{i+1}(r_{i+1}), V_{i+1}(b'))$$

Technical overview

Phase 1: $\sum_{b\in[n]}\{\sum_{b'\in[n]} f(V_{i+1}(b), V_{i+1}(b'))\}$

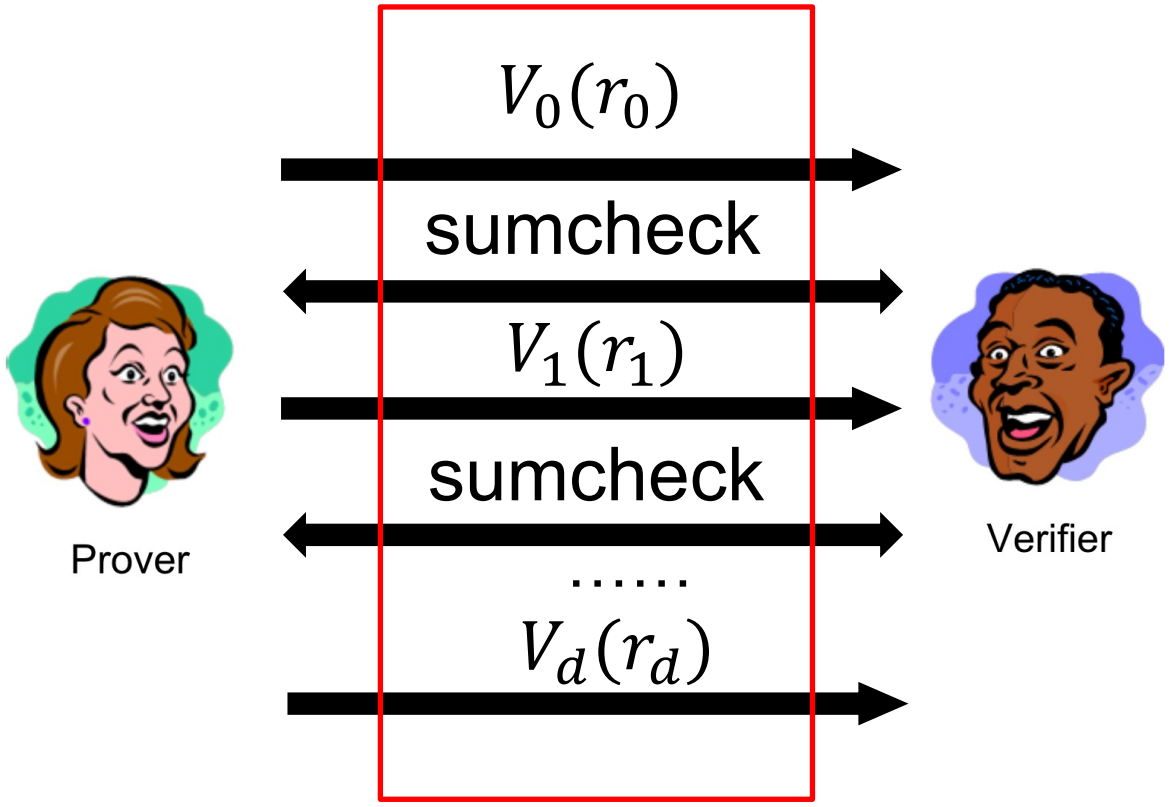
- Let $g(b) = \sum_{b'\in[n]} f(V_{i+1}(b), V_{i+1}(b'))$
- Initialize $g(0), \cdots, g(n-1)$ in $O(n)$ time
- Run sumcheck on $\sum_{b\in[n]} g(b)$ in $O(n)$ time

Phase 2: $\sum_{b'\in[n]} f(V_{i+1}(r_{i+1}), V_{i+1}(b'))$

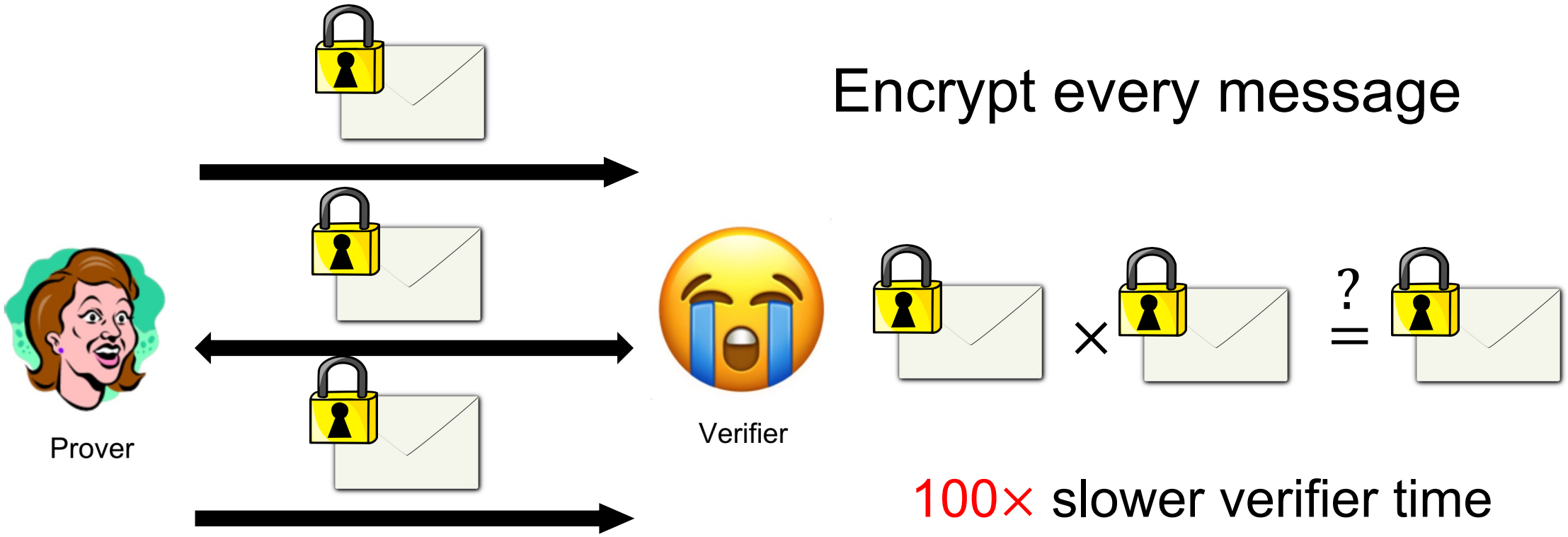
- Let $h(\mathrm{b}') = f(V_{i+1}(r_{i+1}), V_{i+1}(b'))$
- Initialize $h(0), \cdots, h(n-1)$ in $O(n)$ time
- Run sumcheck on $\sum_{b'\in[n]} h(b')$ in $O(n)$ time

$O(n)$

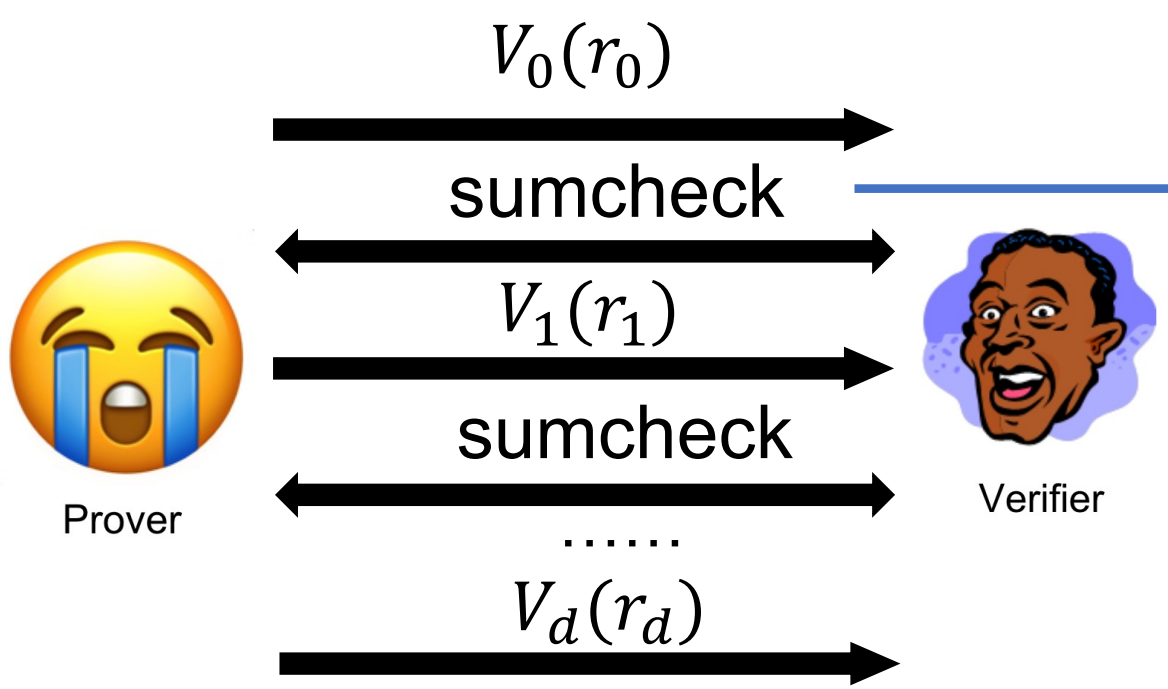
Achieve Zero-Knowledge



Previous Solution [ZGK+ 18, WTS+ 18]



Previous Solution [CFS 17]



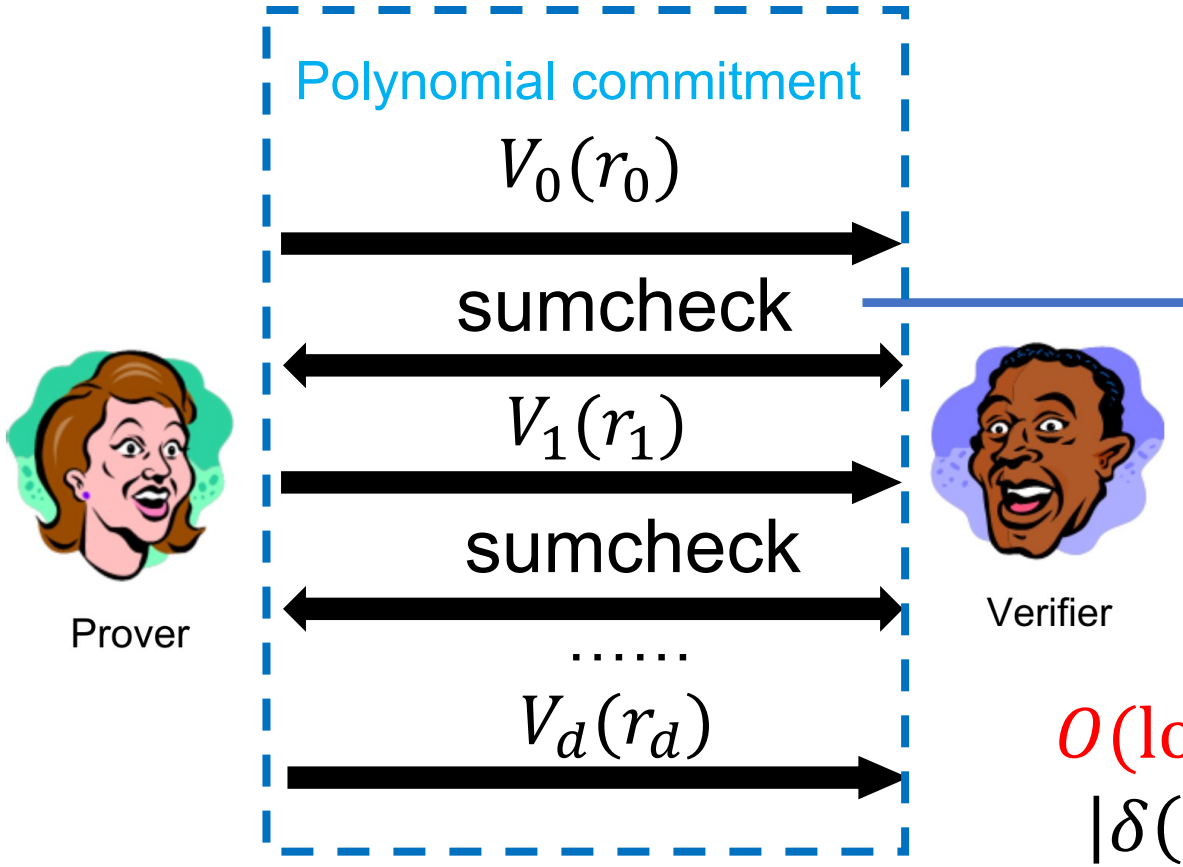
Add mask polynomial

$$H \neq \rho\Delta = \sum_{b\in[n]} f(b) \; (f(b) + \; \rho\delta(b)) - \sum_{b\in[n]}$$

$$|\delta(b)| = |f(b)| = n$$

High overhead on prover time

Our Solution



Libra [XZZPS 19]

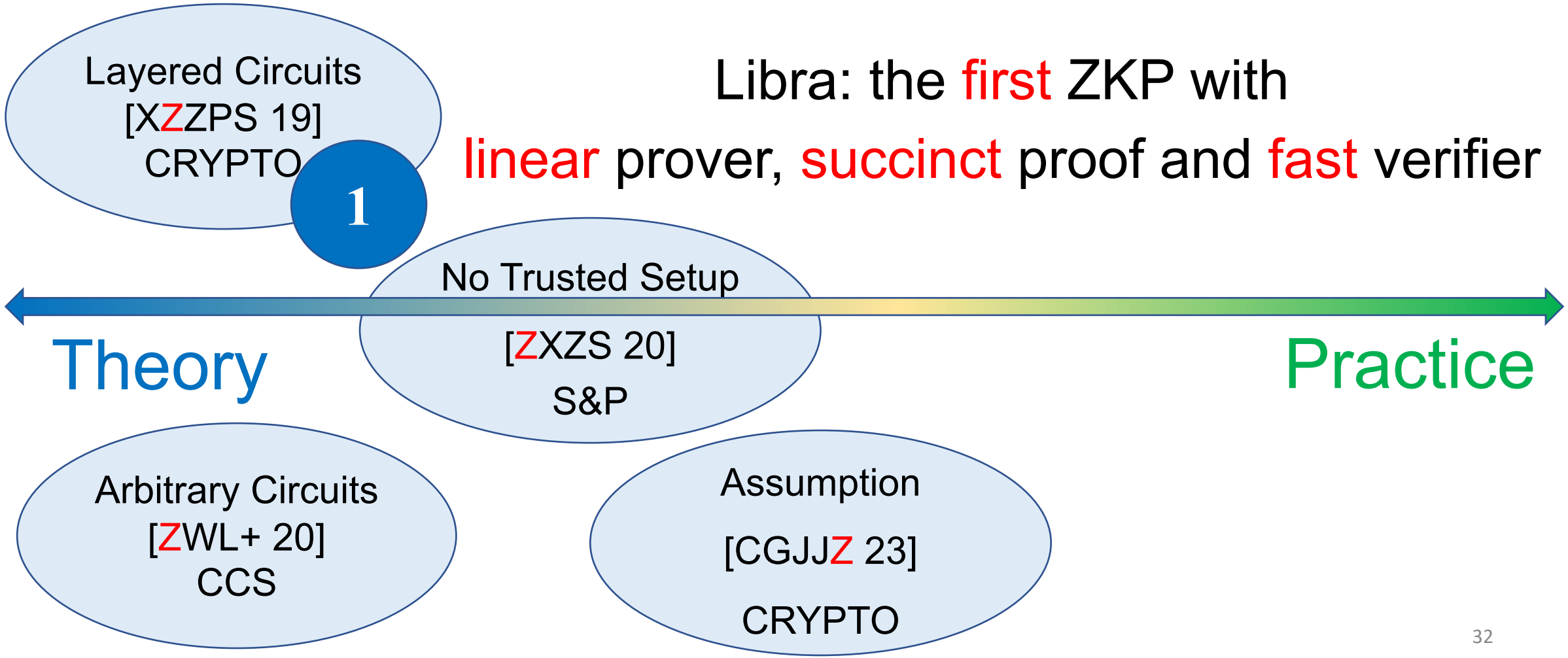
Add mask polynomial

$$H + \rho\Delta = \sum_{b\in[n]} (f(b) + \rho\delta(b))$$

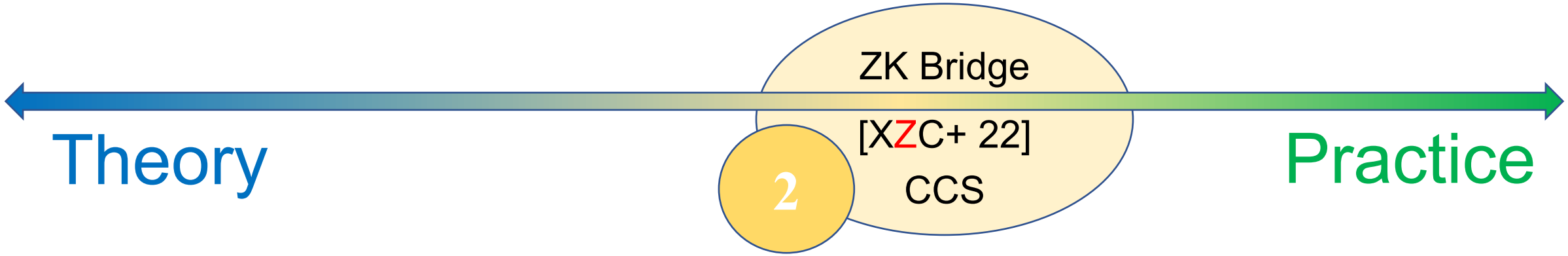
$O(\log n)$ proof size => $O(\log n)$ leakage

$|\delta(b)| = O(\log n) \ll |f(b)|$ is enough!

No overhead


Layered Circuits
[XZZPS 19]
CRYPTO
1
Libra: the first ZKP with
linear prover, succinct proof and fast verifier
No Trusted Setup
[ZXZS 20]
S&P
Theory
Practice
Arbitrary Circuits
[ZWL+ 20]
CCS
Assumption
[CGJJZ 23]
CRYPTO

zkBridge: Trustless Cross-chain Bridges Made Practical



Bridges in Blockchain

Burn 1 Bitcoin for Alice

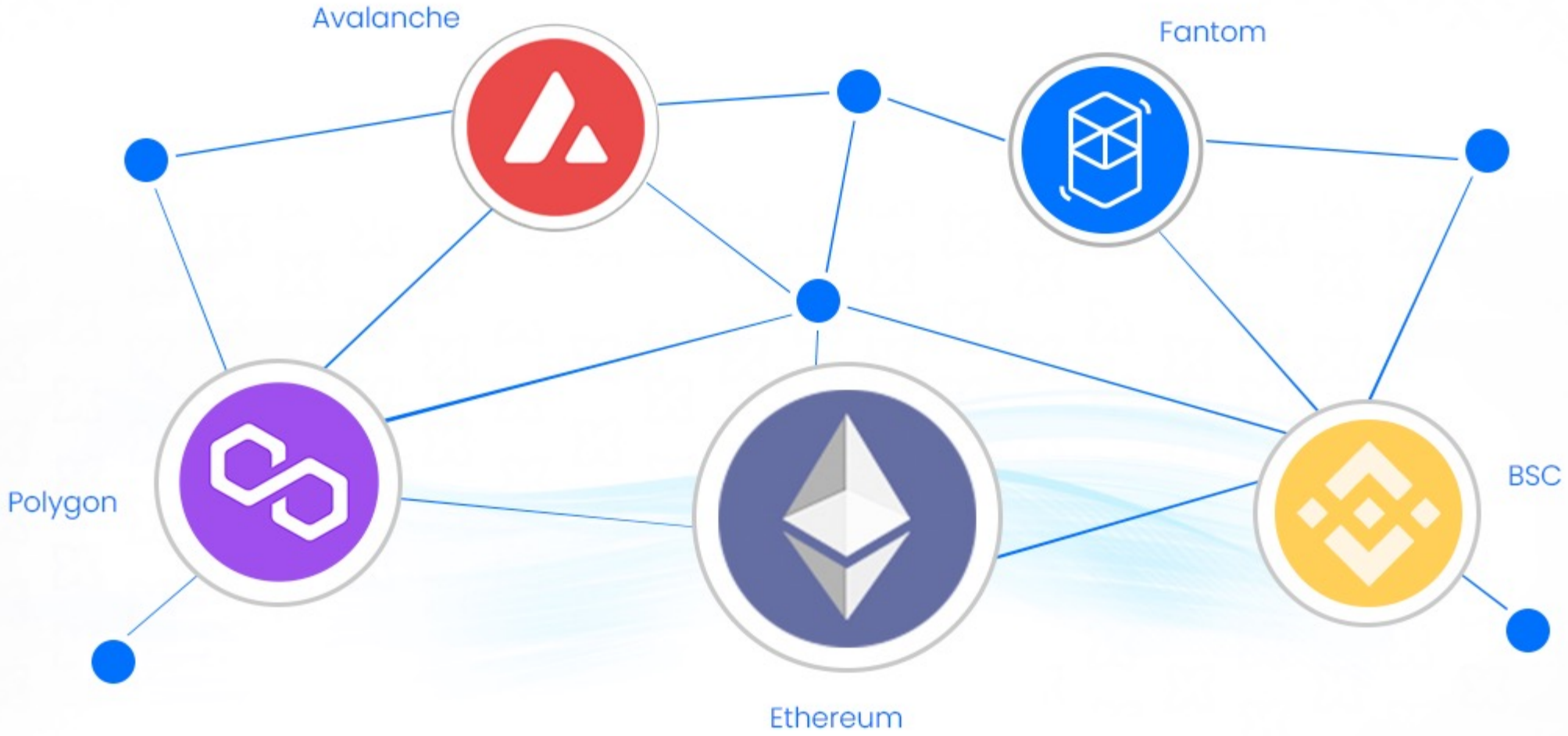
- message passing
- state changing

…

Create 1 Bitcoin for Alice

Sender Blockchain

Receiver Blockchain



CROSS-CHAIN **BRIDGE**

HACKS • AUGUST 10, 2021, 9:30AM EDT

At least $611 million stolen ...ss-chain

NEWS › CRYPTOCURRENCY NEWS

Binance Hit By $570 Million Blockchain Bridge Hack

By RAHUL NAMBIAMPURATH Published October 07, 2022

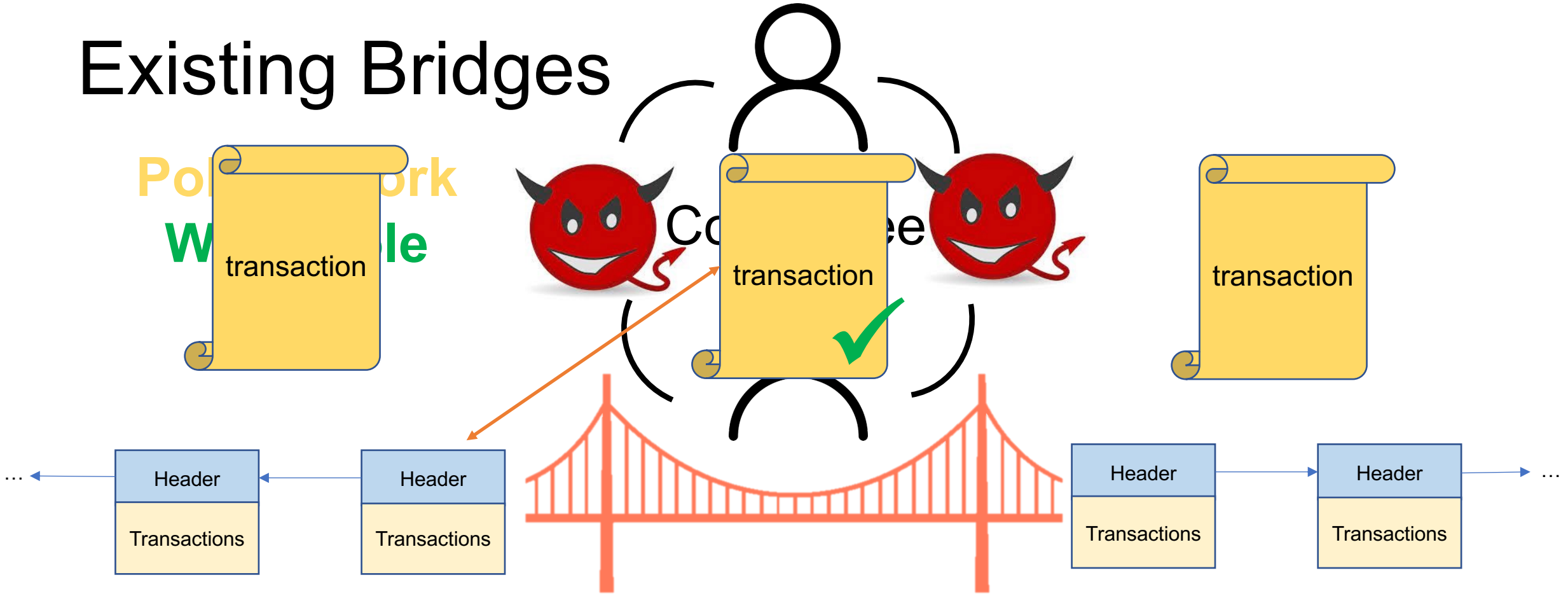
...s Possible Exploit

...e is now attempting to negotiate on-chain with the hacker.

By Andrew Thurman Feb 2, 2022 at 1:30 p.m. PST Updated Feb 3, 2022 at 6:24 a.m. PST

Blockchains need ***secure*** bridges.

Existing Bridges

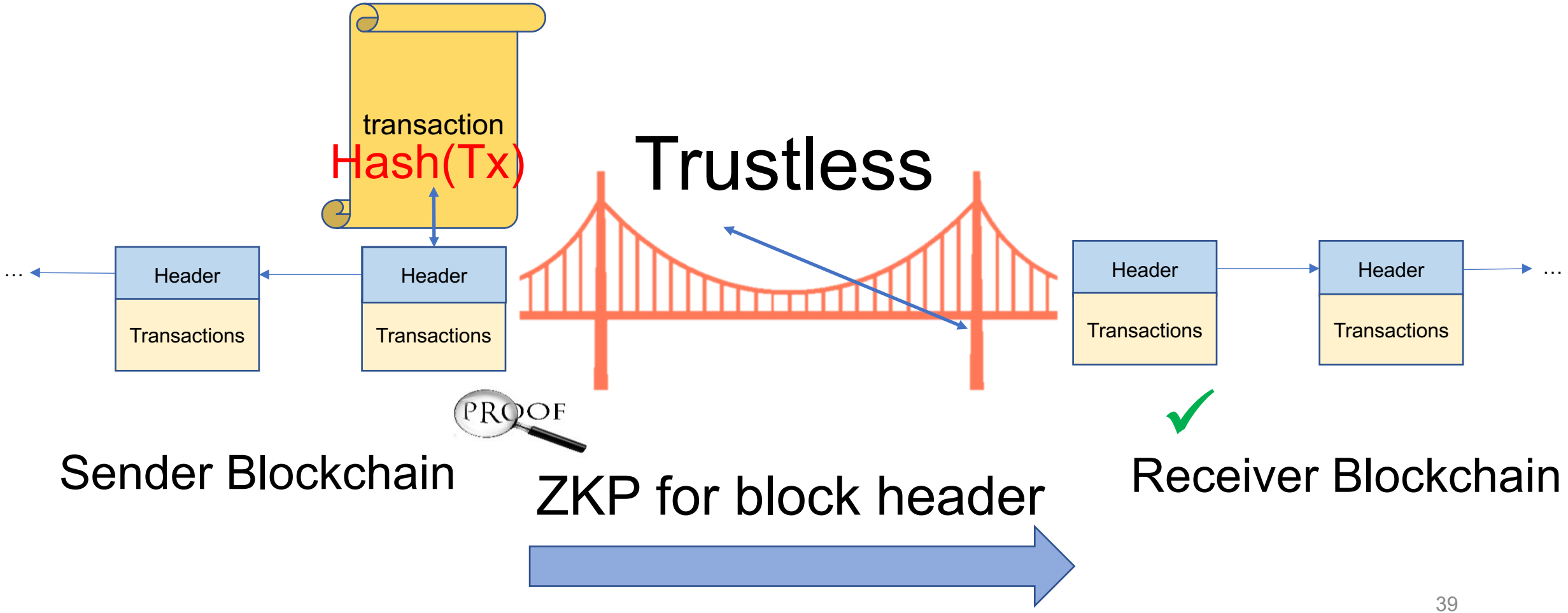


Sender Blockchain

Receiver Blockchain

Unsecure if some members are corrupted

Our Solution: zkBridge



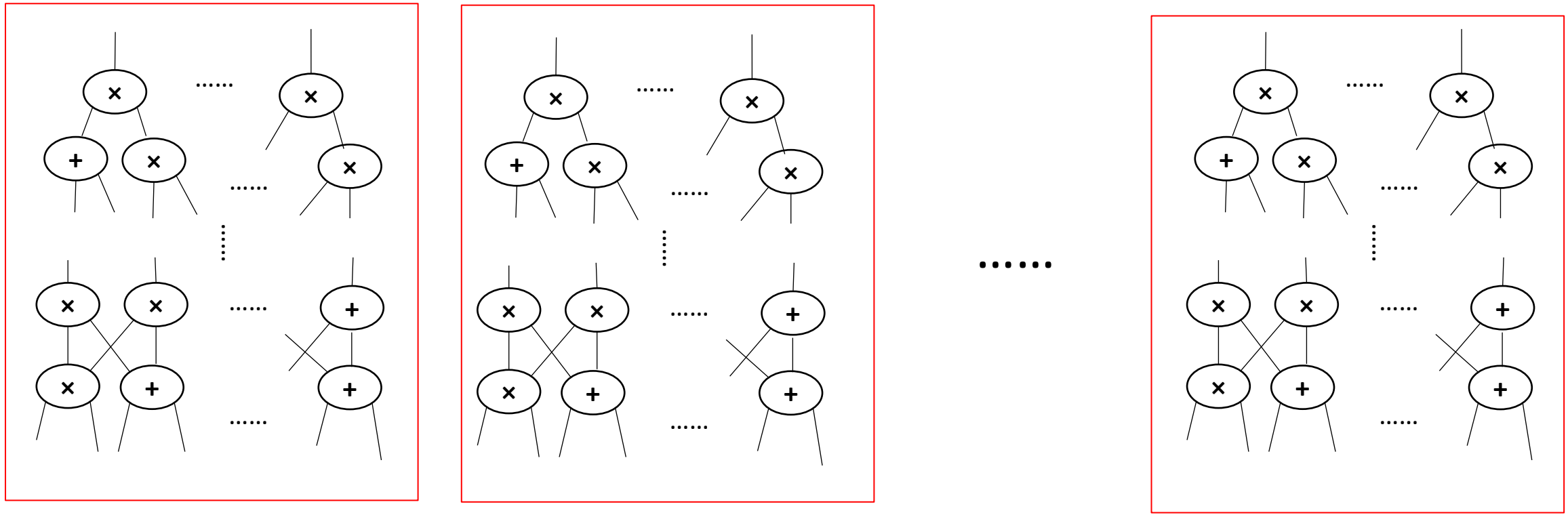
Technical Challenges

Generate ZKP for 100+ signature validations for PoS blockchains

2M gates per signature
0.2B gates in total
>1000s prover time

Data Parallel Circuits

Signature validation



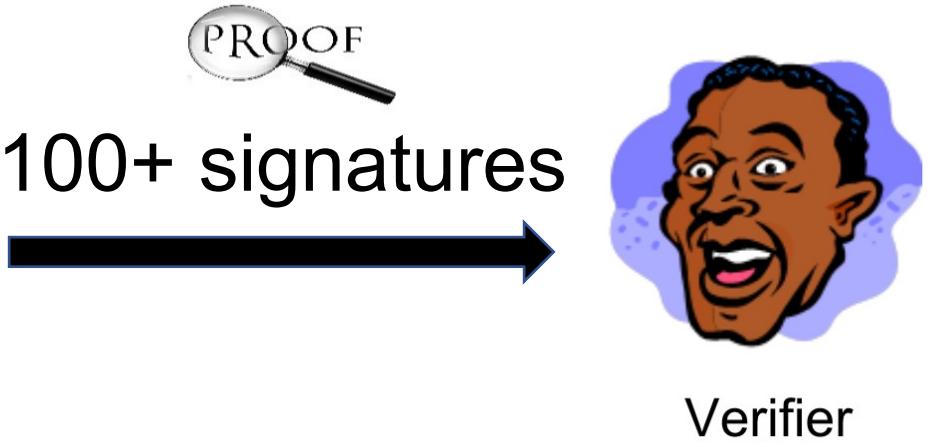
Distributed ZKP

Previous Work: DIZK [WZC+ 18]

- Distributed algorithm for Groth16 [protocol used in Zcash]
- Scale Groth16 to 100x larger circuits

- Slow for large-scale circuits
- High communication

Distributed ZKP with Perfect Scalability



Optimal: T× speedup given T machine
Minimal communication for optimal GKR for polynomial commitment in [LXZ+ 22]

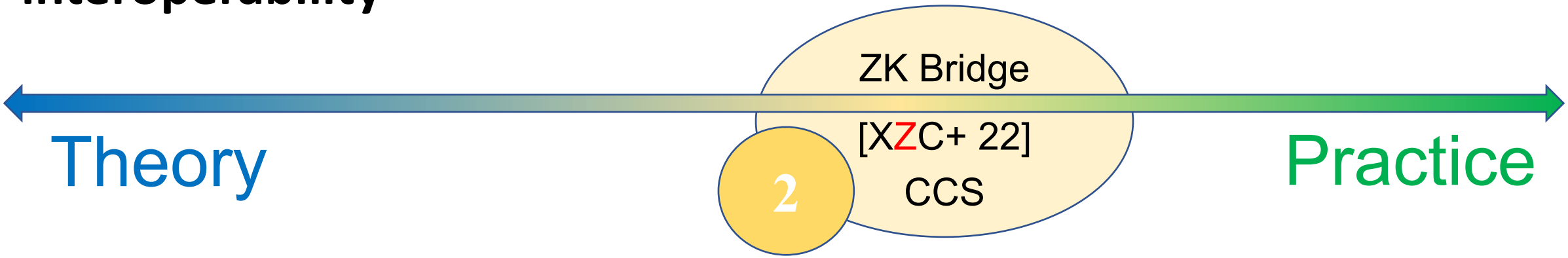
2M gates per signature
0.2B gates in total
<10s prover time

Impact of zkBridge

zkCollective:
building a **secure**, **universal foundation** for multichain **interoperability**

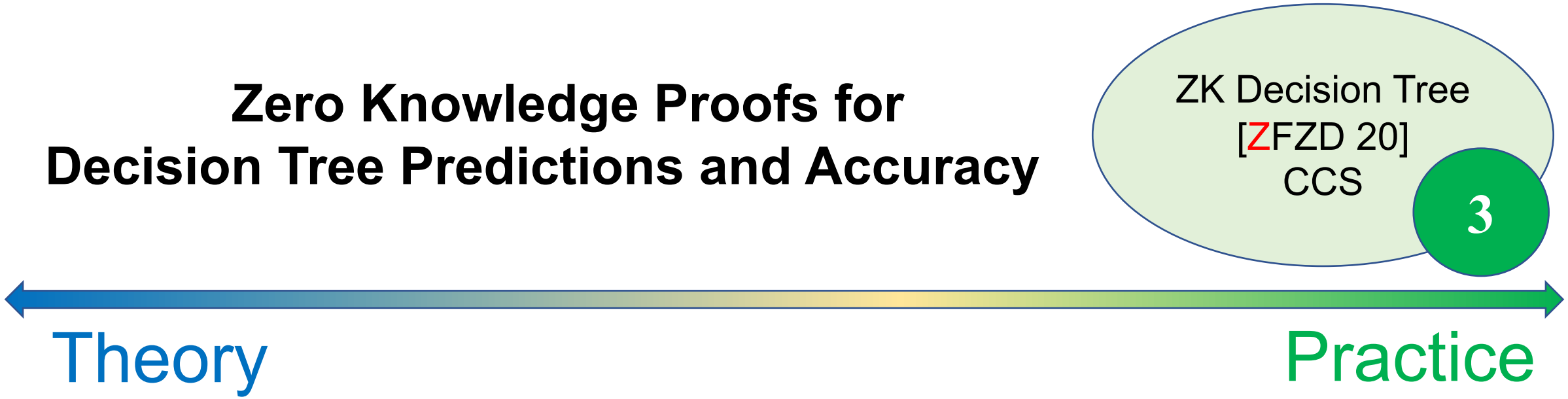
Polyhedra

Raise 25M+ USD with zkBridge



The first trustless and efficient bridge

Zero Knowledge Proofs for Decision Tree Predictions and Accuracy



Success of Machine Learning

Image processing

Speech recognition

Self-driving cars

Drug discovery

Integrity Issues in Machine Learning

- Reproducibility
- Validity

EMAILED ON JUNE 3, 2019 BY CONOR GRANT

Human-guided burrito bots raise questions about the future of robo-delivery

H **e learning**

p

Kiwibots — rolling robots that deliver burritos and smoothies — have become a fixture on UC Berkeley's campus thanks to their creepy-cute "faces" and low delivery prices.

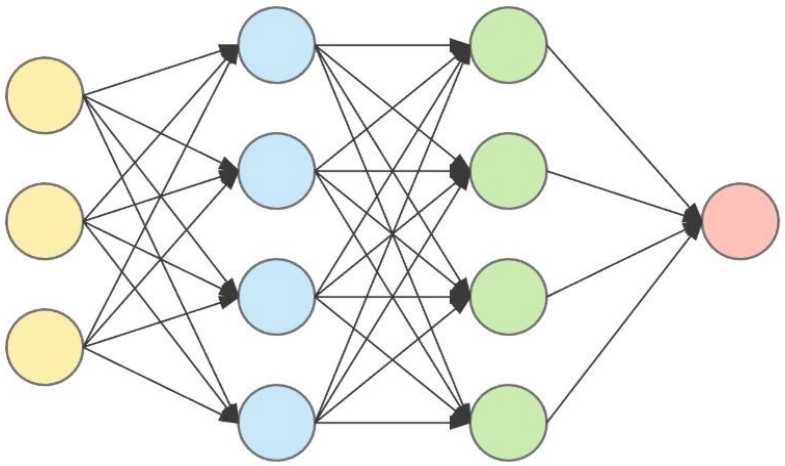
But while the robots appear to be autonomous, the *San Francisco Chronicle* reports they're actually operated by remote workers in Colombia who make $2 an hour.

The bodies behind the bots

Kiwi Campus' technology page shows several videos of Kiwibots using complex-looking computer vision to cross streets and identify obstacles

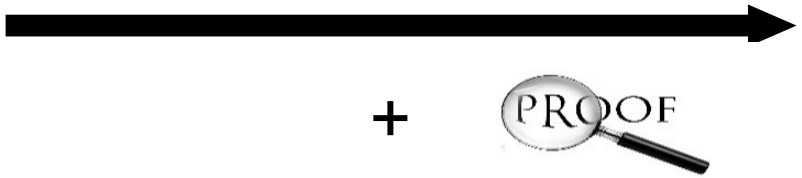
Address Issues by ZKP

Secret ML Model



Prover

$\mathrm{output}(\mathrm{data}, \mathrm{model}) = \mathrm{result}$



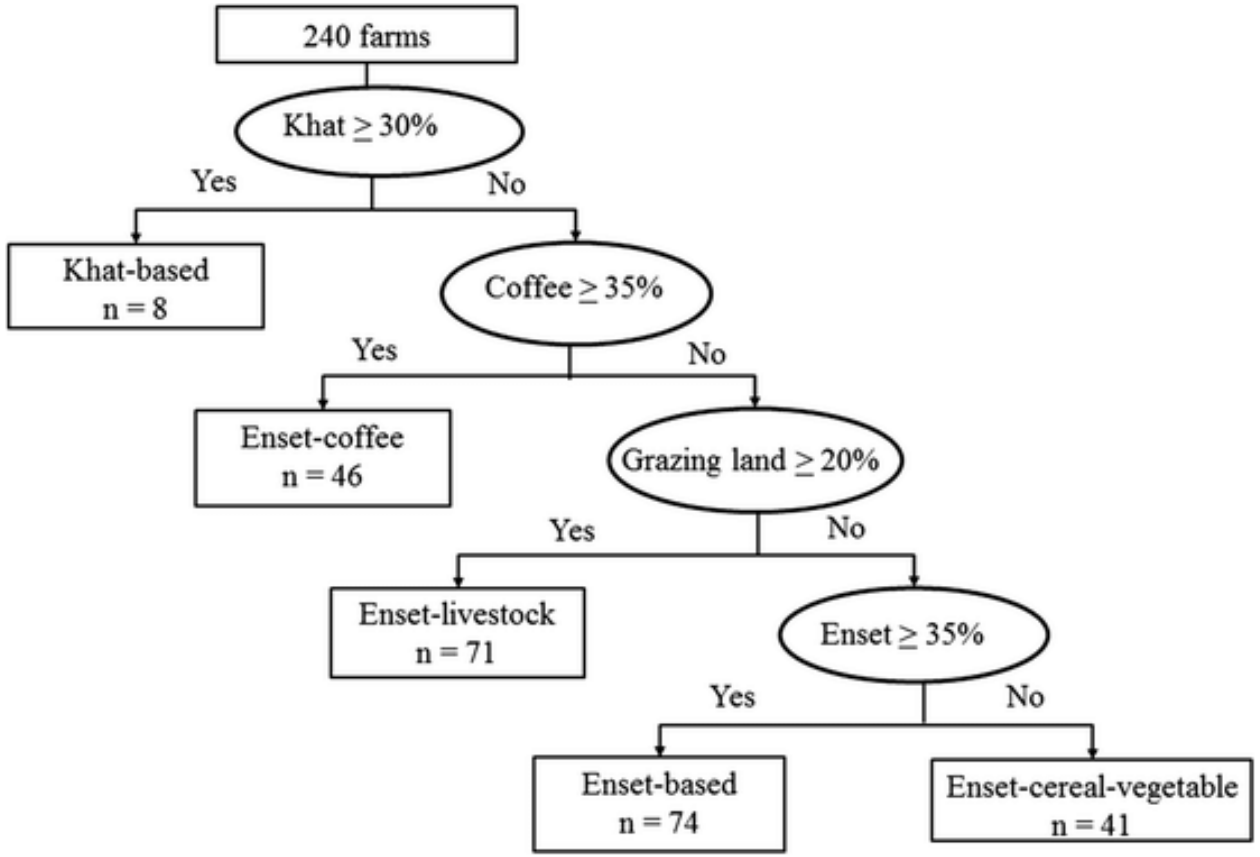
\+ PROOF

Verifier

$\mathrm{acc}(\mathrm{dataset}, \mathrm{model}) = 99\%$

\+ PROOF

Example: Decision Tree

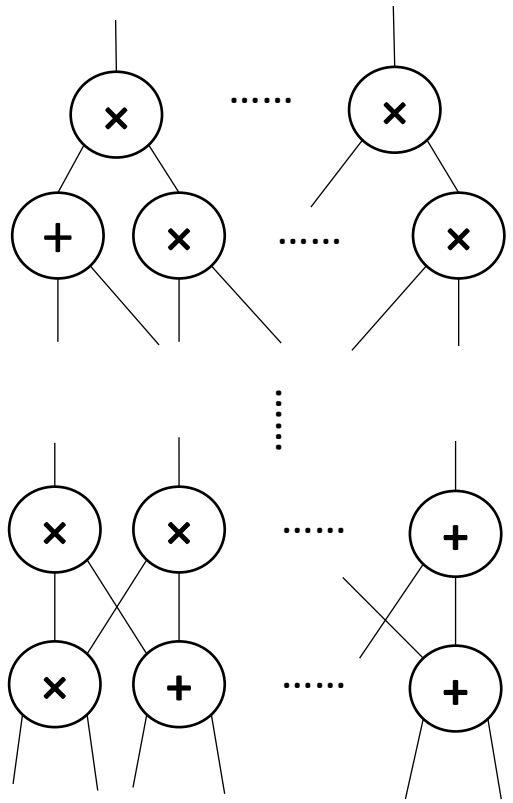


Algorithm 1 Decision Tree Prediction

Input: Decision tree $\mathcal{T}$, data sample $\mathbf{a}$
Output: classification $y_{\mathbf{a}}$

```
1: v := T.root
2: while v is not a leaf node do
3:     if a[v.att] < v.thr then
4:         v := v.left
5:     else
6:         v := v.right
7: return v.class
```

Technical Challenge



Algorithm 1 Decision Tree Prediction

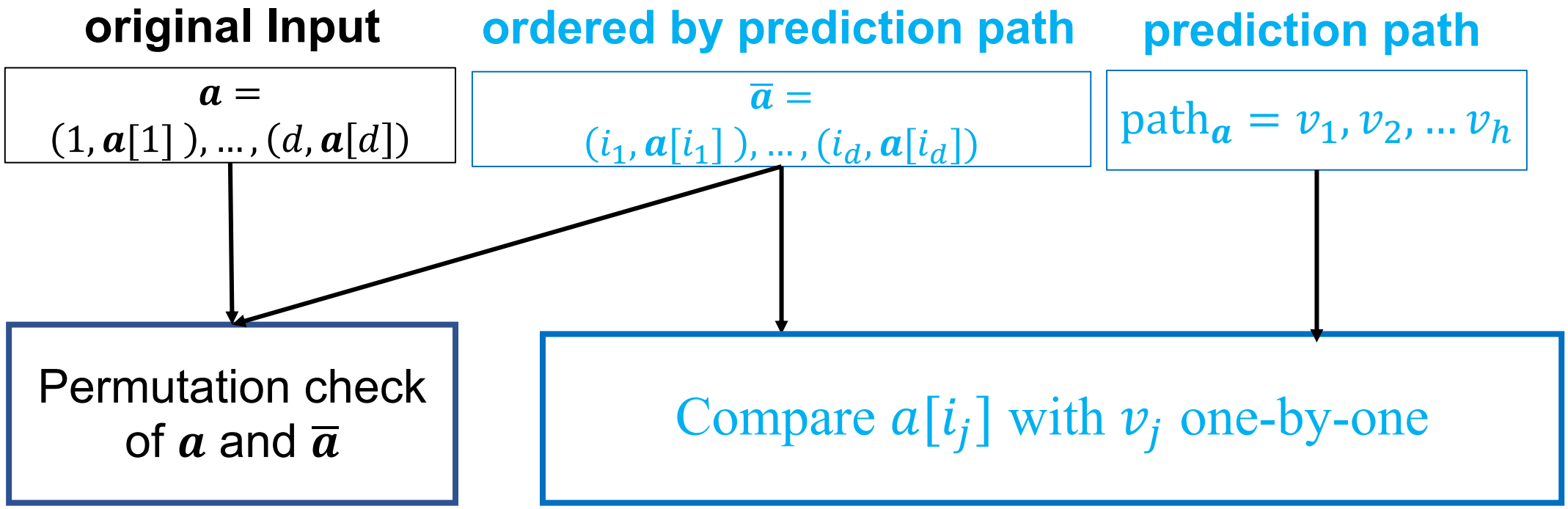
Input: Decision tree $\mathcal{T}$, data sample **a**
Output: classification $y_{\mathbf{a}}$

```
1: v := T.root
2: while v is not a leaf node do
3:     if a[v.att] < v.thr then
4:         v := v.left
5:     else
6:         v := v.right
7: return v.class
```

High overhead for conditional branching

Our Circuit for Decision Tree Prediction

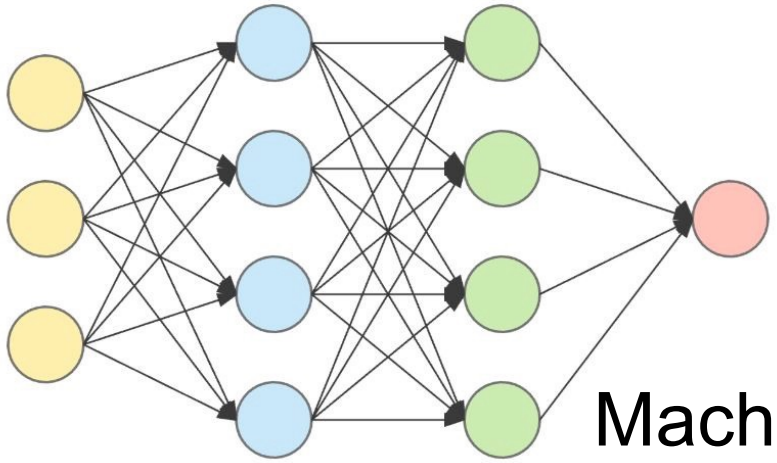
Validate the prediction instead of running the program



Optimal size: $\boldsymbol{O(d + h)} \ll O(2^h)$ naïvely

h: height of the tree; d: #attributes of the input

Build Bridge between ML and Blockchain



Machine Learning Model

Quality

Blockchain

The first work to apply ZKP to machine learning inference

ZK Decision Tree
[ZFZD 20]
CCS

3

Theory

Practice

Follow-up works

ZKCNN
[LXZ 21]
CCS

ZK-IMG
[KHSS 22]

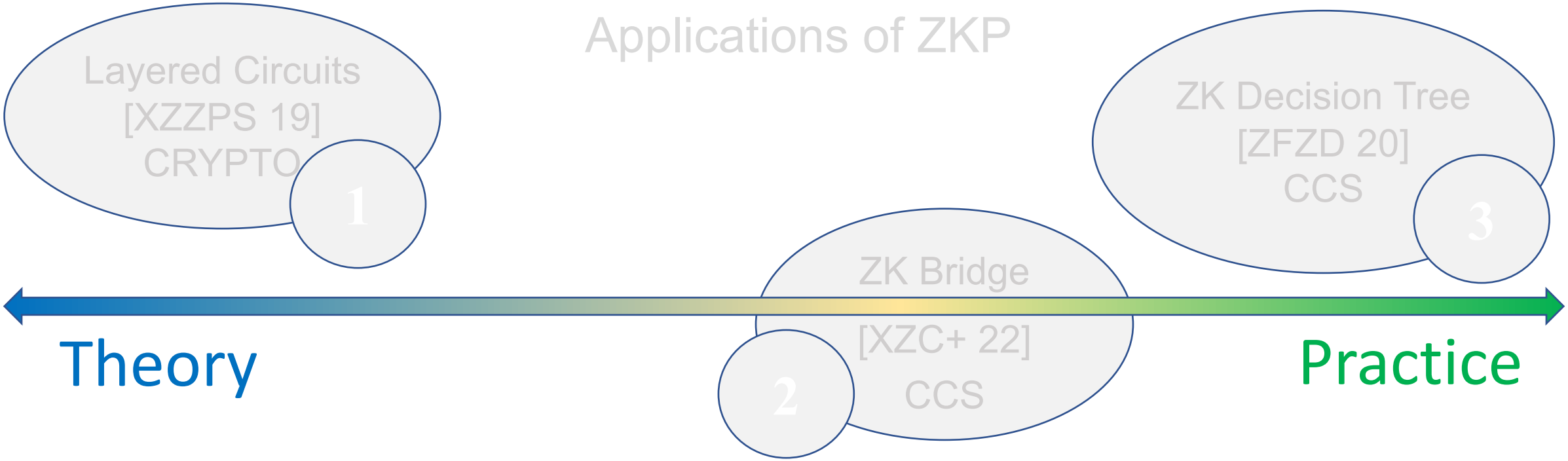
ZEN
[FQZ+ 21]

ZKDNN
[KHSS 22]

Outline

What is ZKP

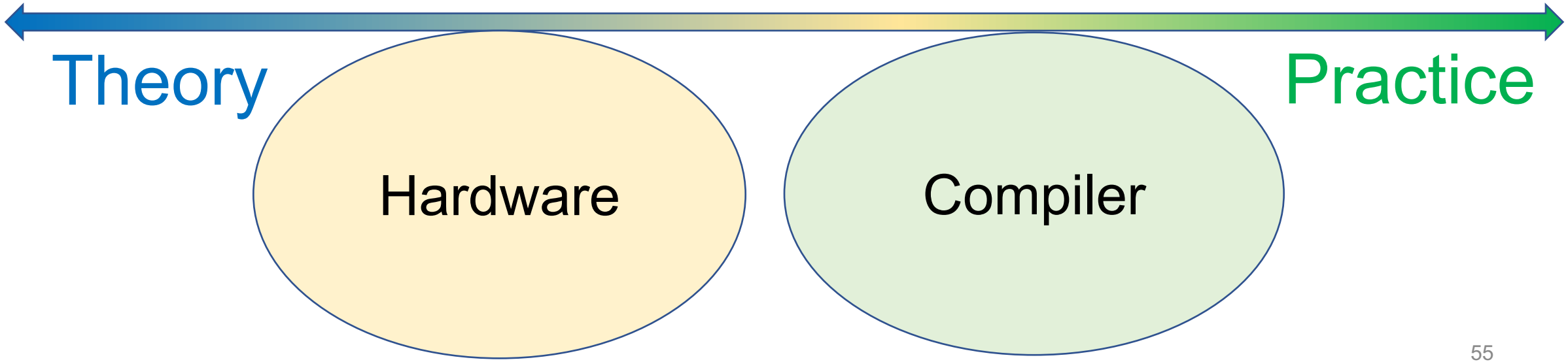
Applications of ZKP



Future Work

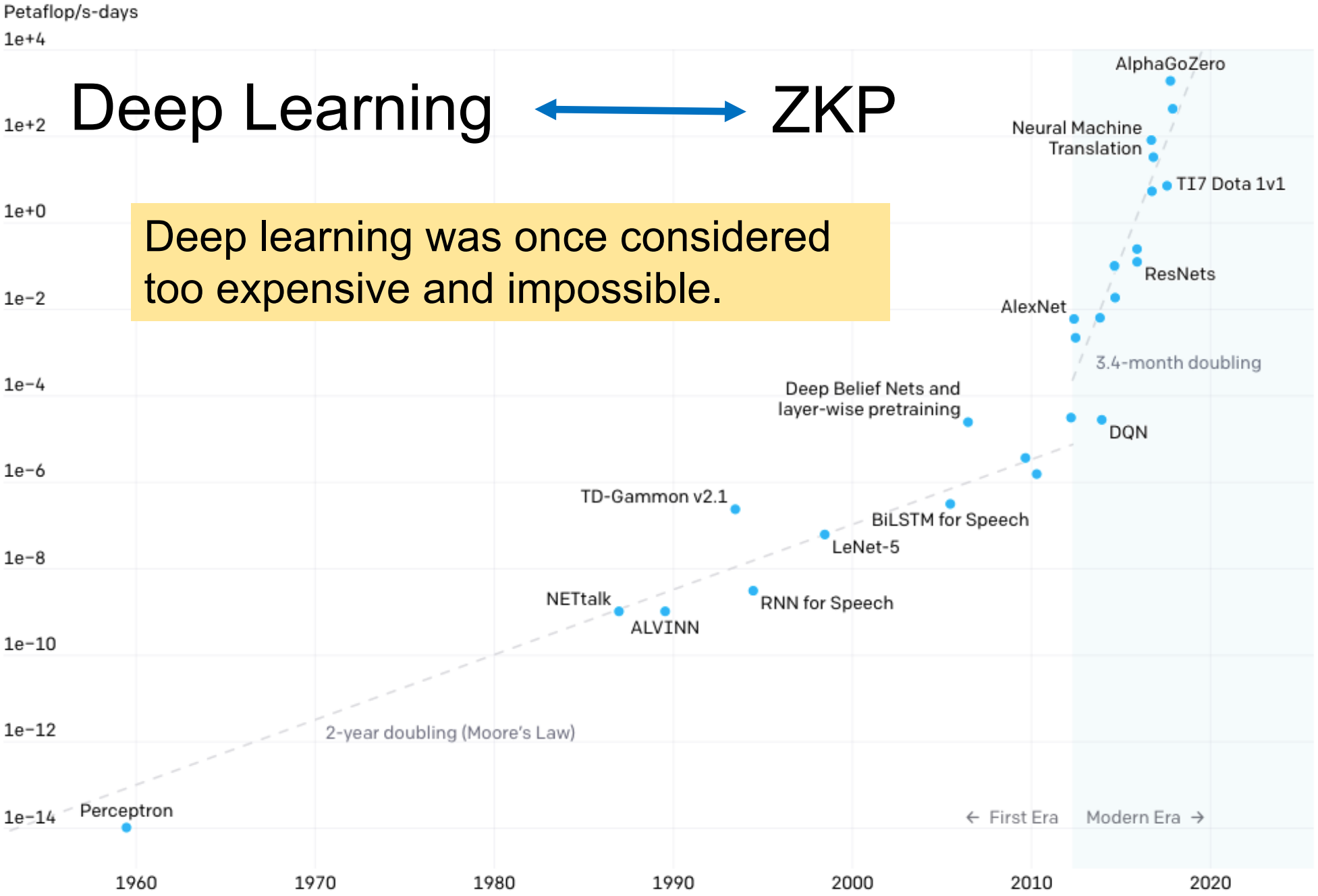
Future Work

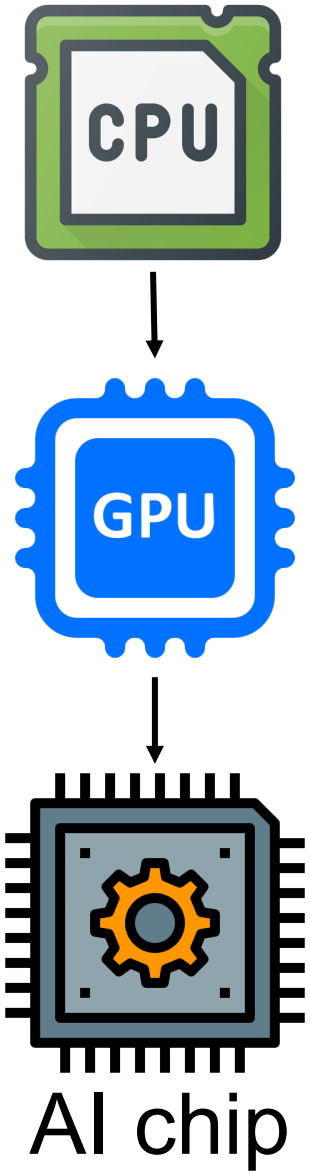
How to fill in the gap between
ZKP and local computation?



Deep Learning ⟷ ZKP

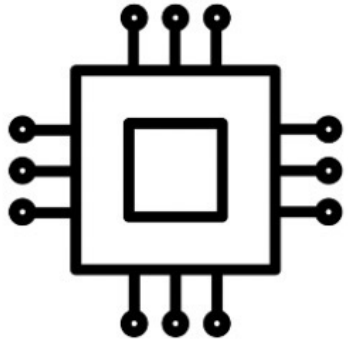
Deep learning was once considered too expensive and impossible.

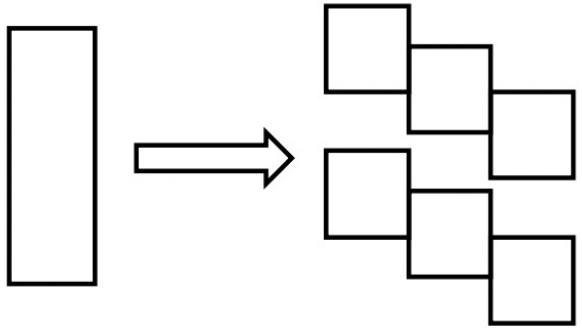


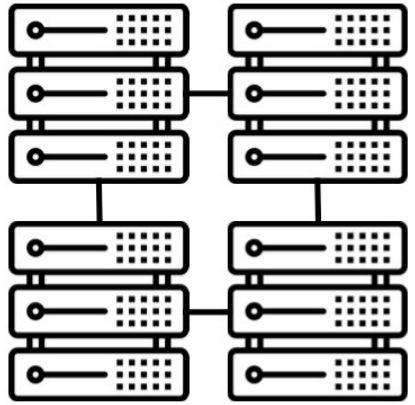


AI chip

Hardware-software Co-design for ZKP







Hardware acceleration

ZKP-friendly hardware

Software optimization

Hardware-friendly ZKP

System-level optimization

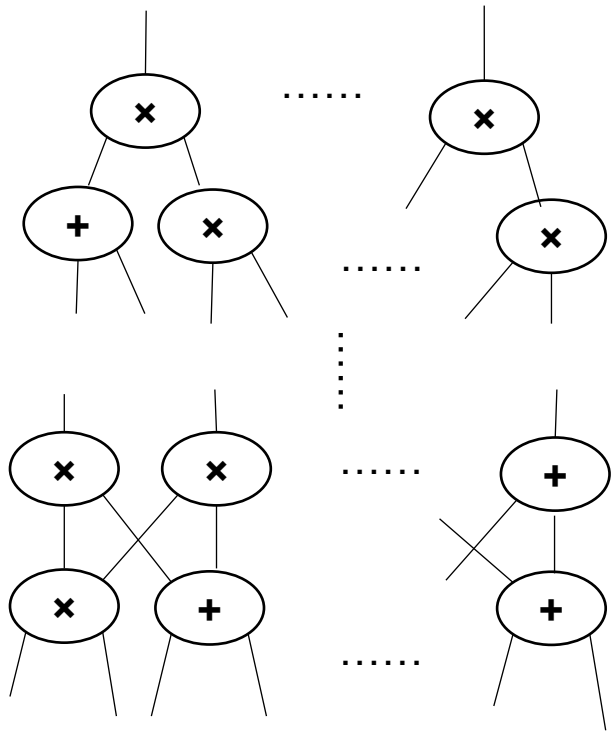
Adaptive resource allocation

Compile to ZKP Circuits

```
#include <exception>
#include <fstream>
#include <string>

void f(const std::string &fileName) {
  std::fstream file(fileName);
  if (!file.is_open()) {
    // Handle error
    return;
  }
  // ...
  file.close();
  if (file.fail()) {
    // Handle error
  }
  std::terminate();
}
```

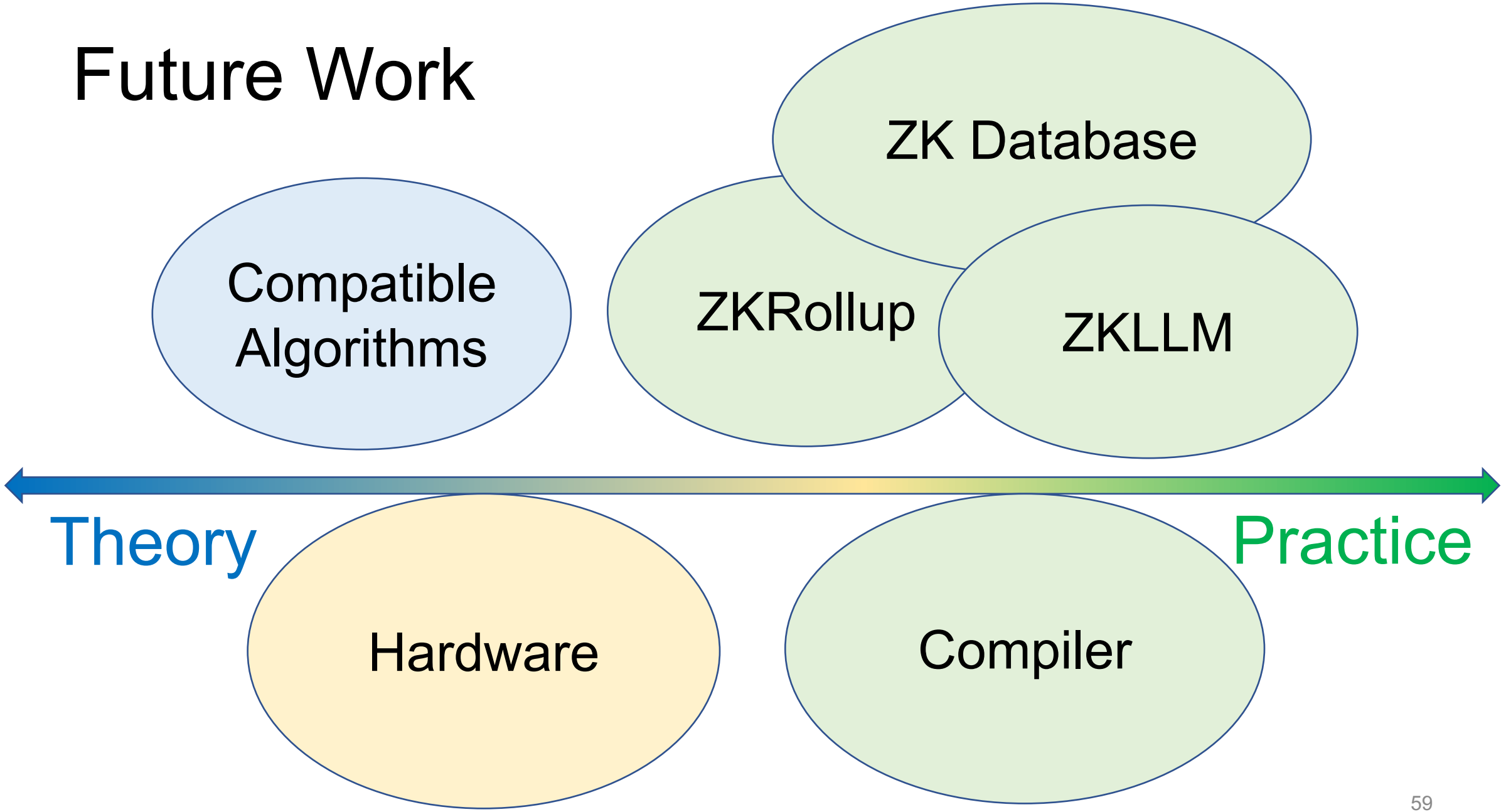
compiler



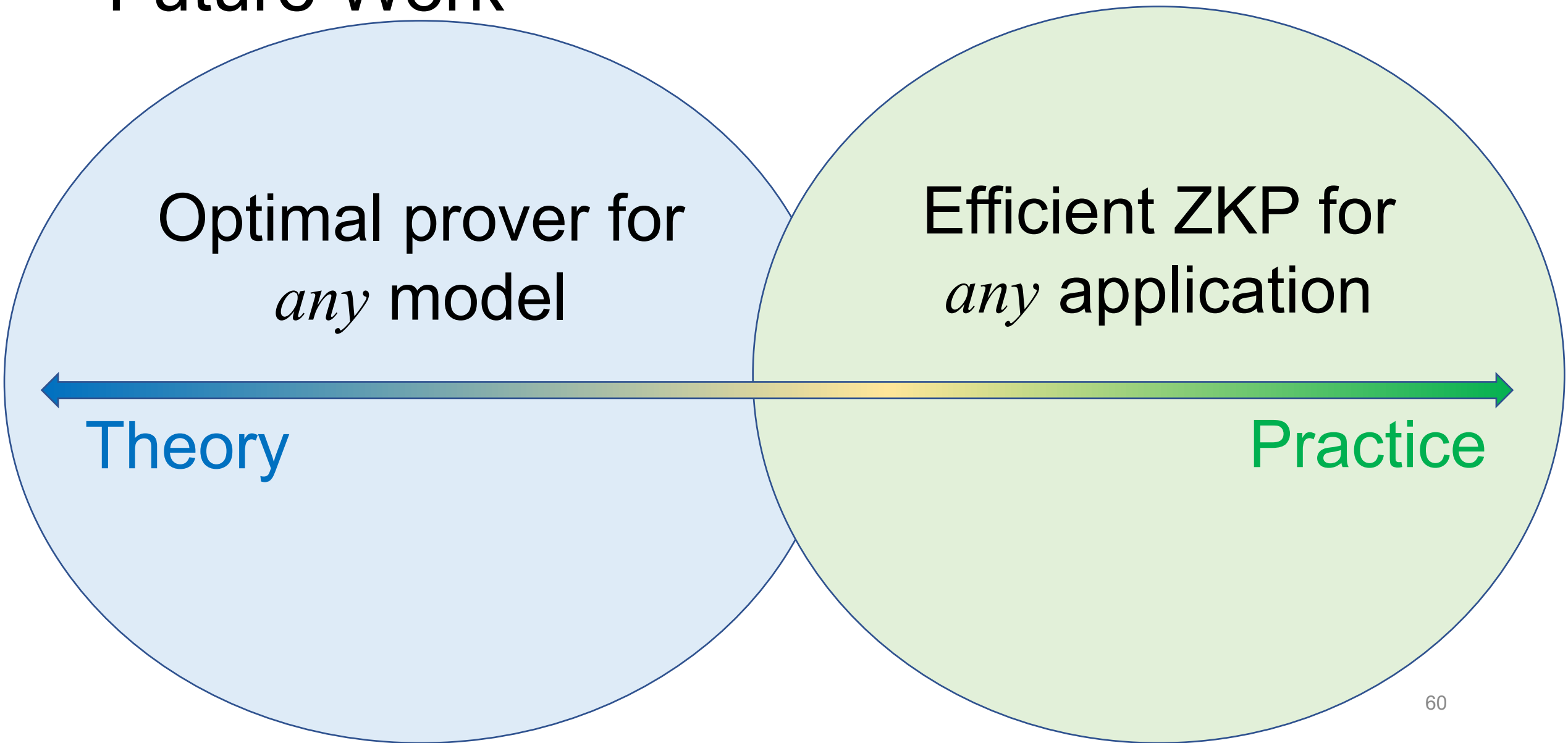
High level
programming language

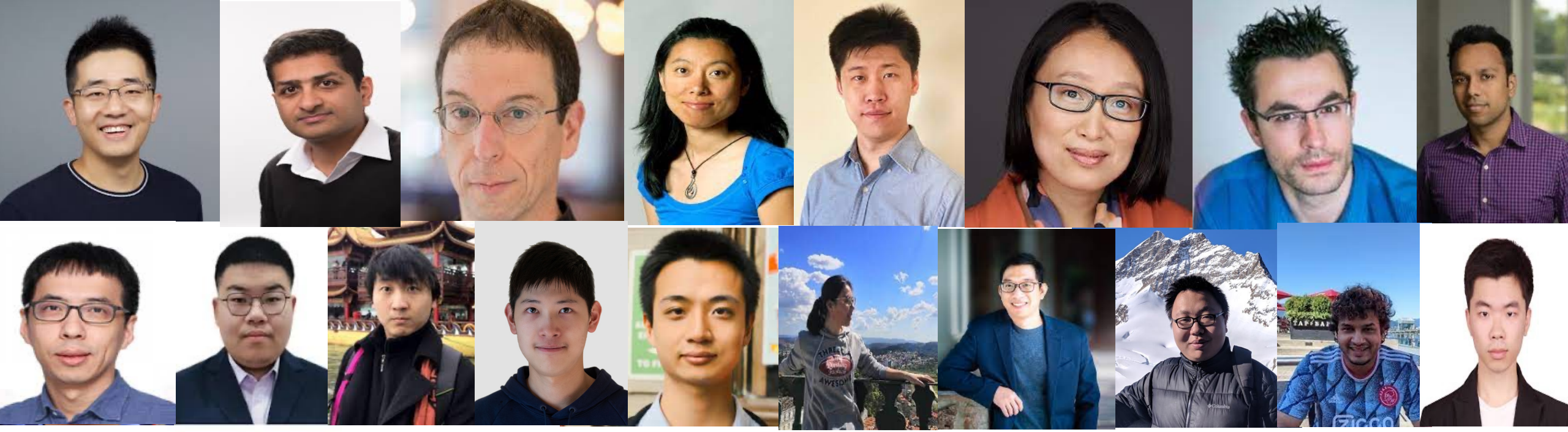
Arithmetic circuit

Future Work


ZK Database
Compatible Algorithms
ZKRollup
ZKLLM
Theory
Practice
Hardware
Compiler

Future Work


Optimal prover for
any model
Efficient ZKP for
any application
Theory
Practice



Thank you!

Efficient Zero-Knowledge Proof: Theory and Practice