

Democratizing the Cryptocurrency Ecosystem by Just-In-Time Transformation of Mining Programs

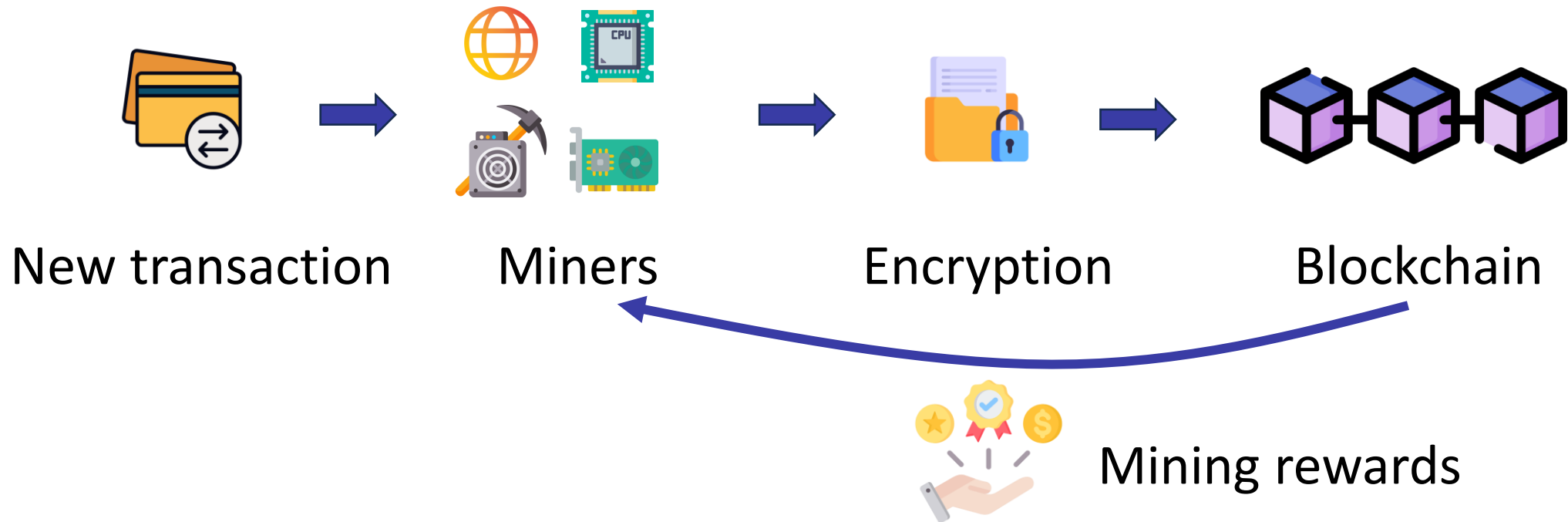
Wei Liu , Zhenhua Li, Feng Qian, Feiyu Jin, Hao Lin
Yannan Zheng, Bo Xiao, Xiaokang Qin, Tianyin Xu



1. Background

□ Cryptomining is an important pillar for cryptocurrencies

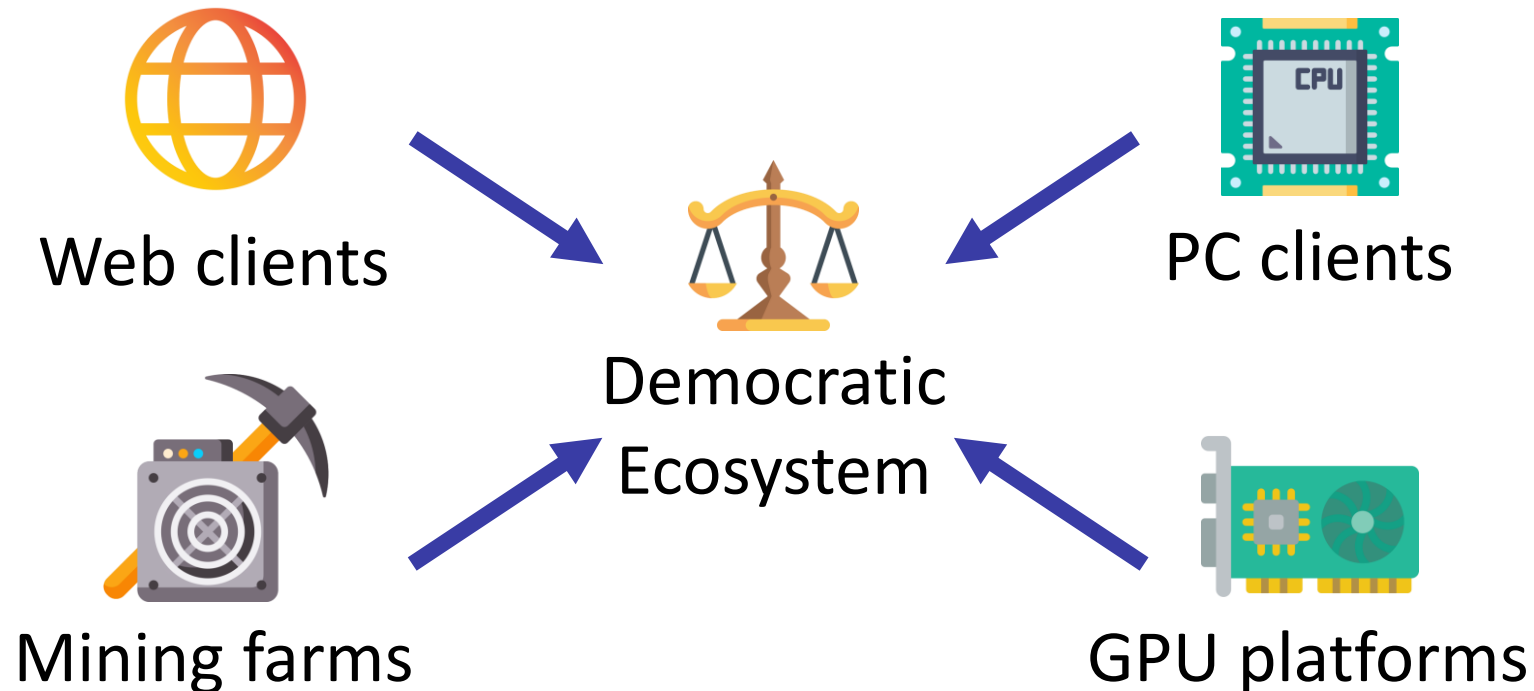
- Miners solve **computationally difficult puzzles** for new transactions
- These puzzles make transactions to be **securely** added to blockchains
- The first miner to solve the puzzle is paid in cryptocurrency



1. Background

□ Democracy is crucial to cryptocurrency

- Cryptomining is **decentralized** to keep the **credibility** of cryptocurrency
- Supporting a variety of miners: **mining farms, PC, web clients, etc.**
- No individual entity can dominate the computation power



2. Motivation

❑ Democracy is threatened by dedicated mining hardware

■ ASICs and FPGAs

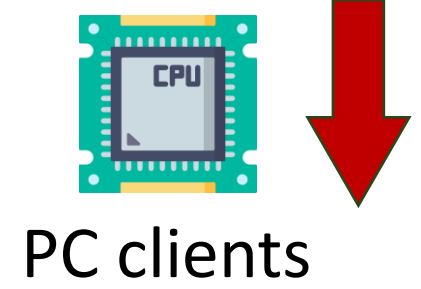
■ Web-based mining dropped from **50M+** to **<0.1M**

■ PC-based mining scaled down to **~0.8M**

■ Renders common users' cryptomining less **profitable** or **unprofitable**



ASICs in mining farms



Common users

2. Motivation

□ Breaking the monopoly

- Cryptocurrencies adopted new mining algorithms

- Monero: **RandomX**



- Scala: **Panthera**

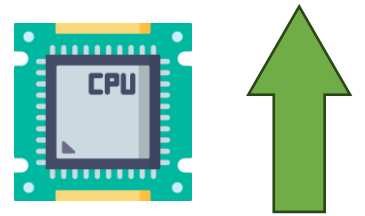


- Rely on the architectural of **general-purpose hardware**

1. Dynamic **instruction execution**

2. Instruction **vectorizations**

- Reducing the efficiency of dedicated mining hardware



PC clients

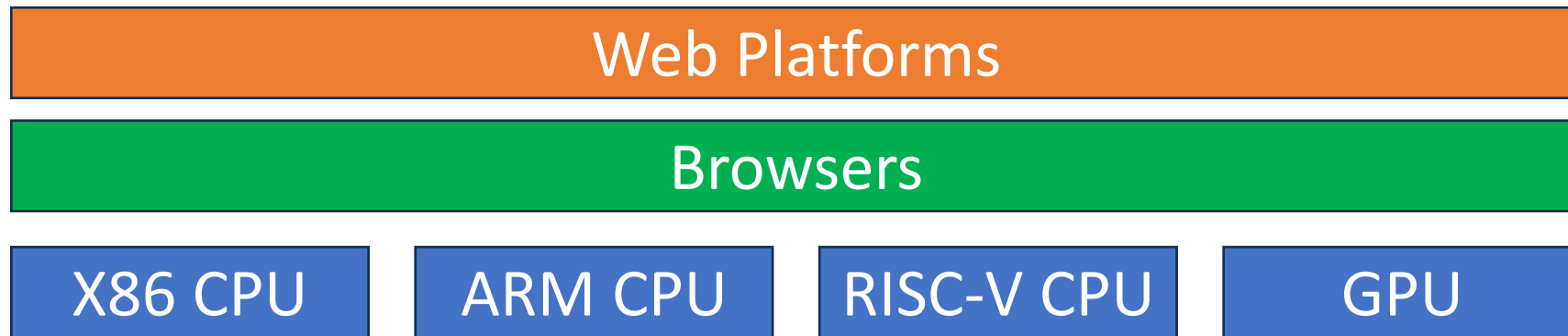


Mining farms

2. Motivation

□ However...

- New mining algorithms further **impair web cryptomining** 😞
- Web is designed to **hide hardware details** for platform independence



- Have to **emulate** hardware features of general-purpose CPUs
 - Directed rounding of floating points
 - Diverse SIMD data types

2. Motivation

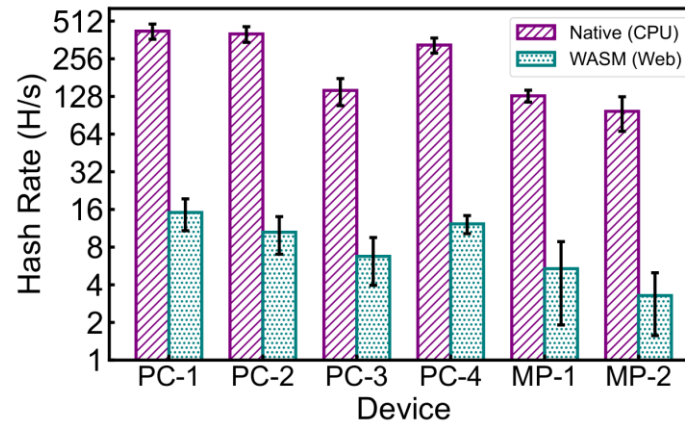
❑ So, the democracy has not been fully recovered

- Web cryptomining is **severely slowed down**
- Coinhive asserted

Discontinuation of Coinhive

Some of you might have anticipated this, some of you will be surprised. The decision has been made. We will discontinue our service on March 8, 2019. It has been a blast working on this project over the past 18

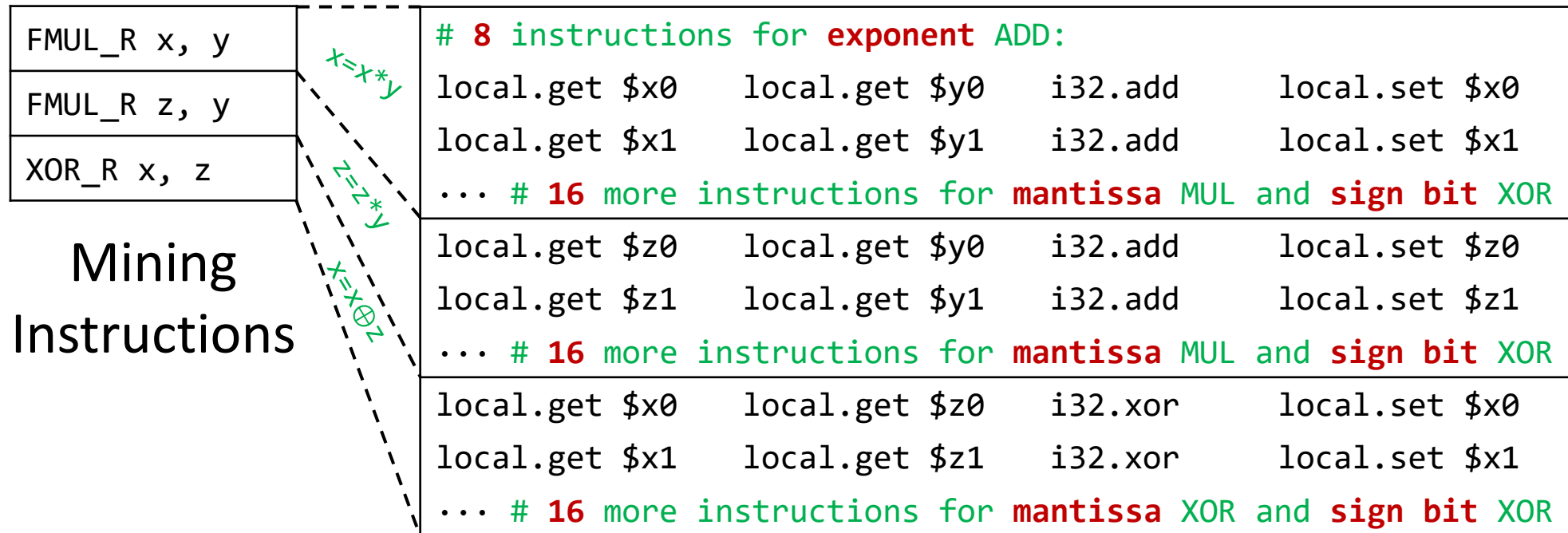
To be completely honest, it isn't economically viable anymore.



3. Analysis

❑ Inefficiency of web cryptomining—a RandomX example

- ① New Monero Transaction → Dynamic Mining Program (RandomX ISA)
- ② Dynamic Mining Program (RandomX ISA) → WASM Emulations

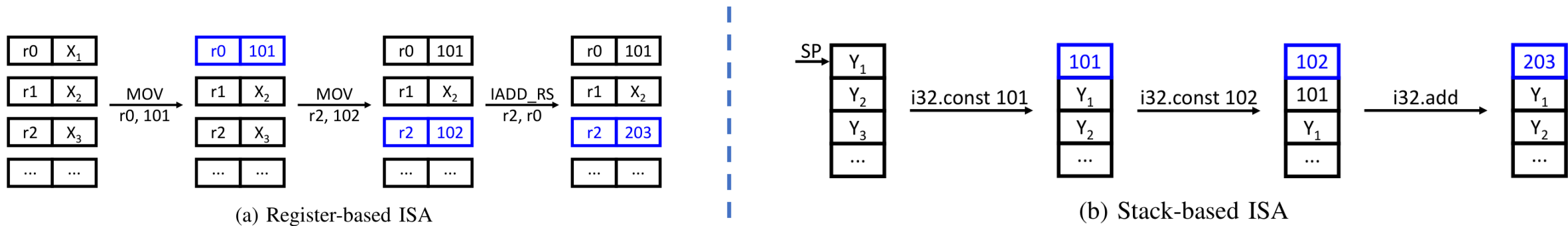


Emulated WASM Instructions

3. Analysis

□ Why dynamic mining programs are emulated in WASM

- Common CPU ISAs: **register-based**
- WASM ISA: **stack-based** for better portability across the web
 1. No special registers for state maintenance
 2. Limited data types



ISA Incompatibilities

3. Design of Vectra

Just-in-time transformation of mining programs

Element propagation graph (EPG) modeling

8 instructions for exponent ADD:

local.get $\$x0$ local.get $\$y0$ i32.add local.set $\$x0$

local.get $\$x1$ local.get $\$y1$ i32.add local.set $\$x1$

... # 16 more instructions for mantissa MUL and sign bit XOR

local.get $\$z0$ local.get $\$y0$ i32.add local.set $\$z0$

local.get $\$z1$ local.get $\$y1$ i32.add local.set $\$z1$

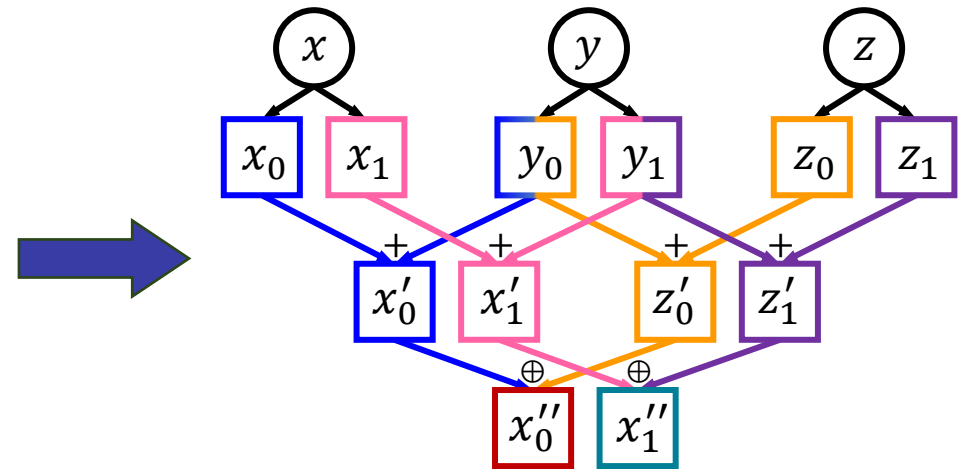
... # 16 more instructions for mantissa MUL and sign bit XOR

local.get $\$x0$ local.get $\$z0$ i32.xor local.set $\$x0$

local.get $\$x1$ local.get $\$z1$ i32.xor local.set $\$x1$

... # 16 more instructions for mantissa XOR and sign bit XOR

Emulated WASM instructions

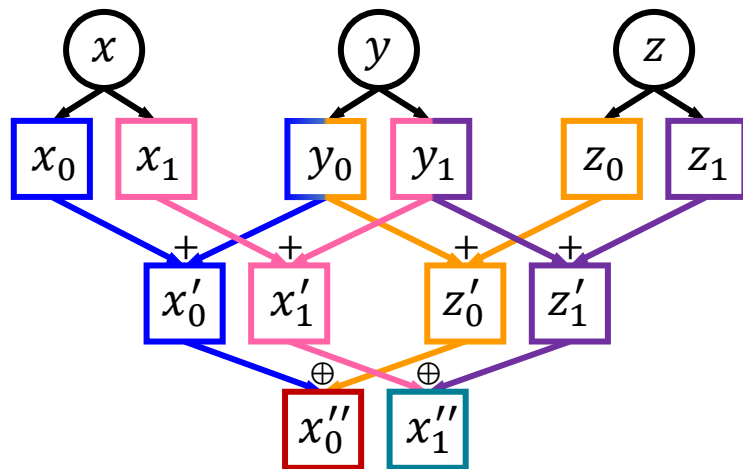


Element propagation graph

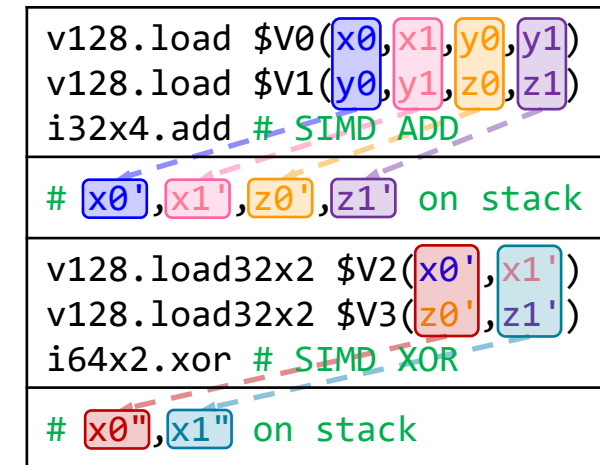
3. Design of Vectra

Just-in-time transformation of mining programs

- Merge instructions in **isomorphic** element propagations
- **ISA-compatible efficient** SIMD instructions



Element propagation graph

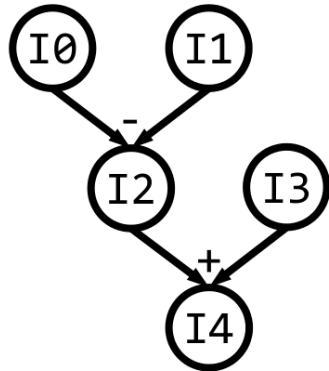


Merged WASM SIMD instructions

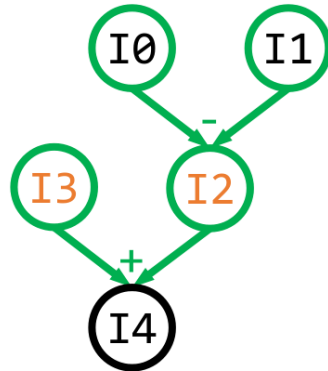
3. Design of Vectra

□ Finding optimal EGP components that are isomorphic

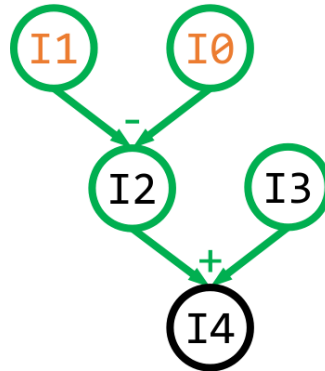
■ Graph isomorphisms



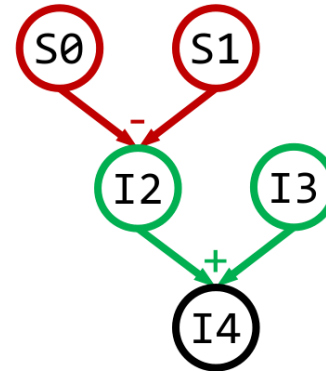
(a)



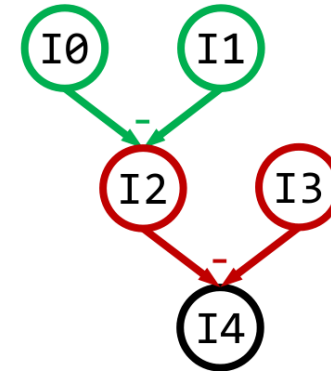
(b)



(c)



(d)



(e)

■ High time complexity of $O(n!)$

3. Design of Vectra

□ Finding optimal EGP components that are isomorphic

- Key idea: use locality of **data dependencies** to bound searching process
- Locality metric:

$$L(x, y) = L_{intra}(x, y) \cdot L_{inter}(x, y)$$

$$L_{intra}(x, y) = |D(x, r) - D(y, r)| + 1$$

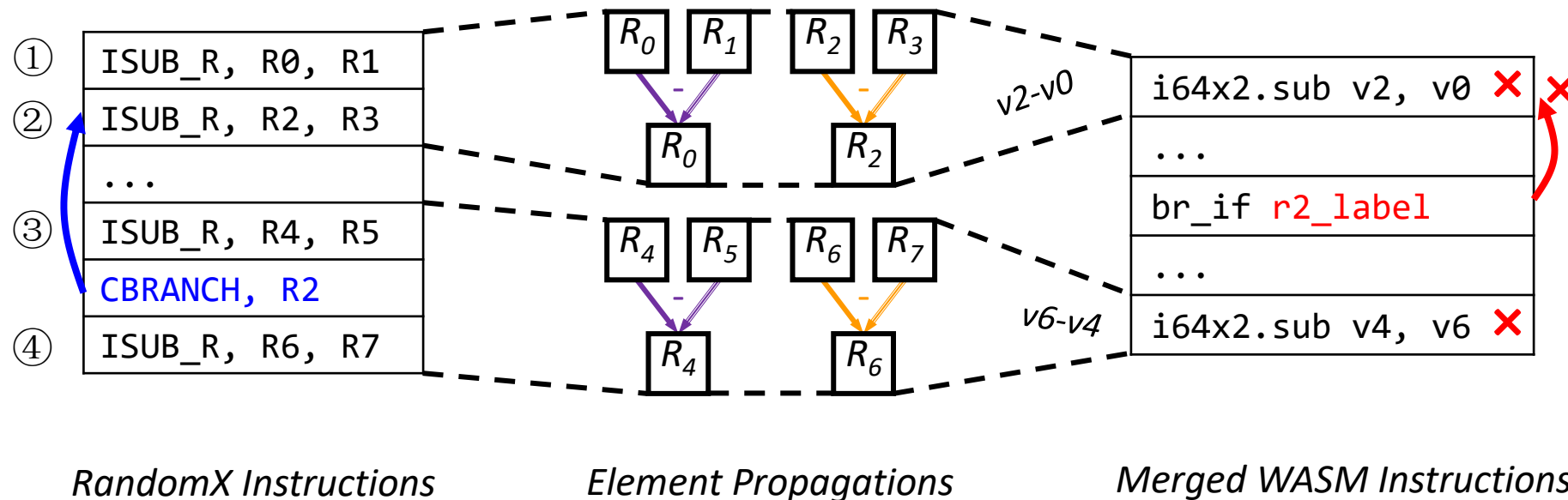
$$L_{inter}(x, y) = I(x, y) + 1$$

- Group graph nodes based on $L(x, y)$
- Search happens **only in each group** ↓99% search time reduction

3. Design of Vectra

□ Ensuring correct program transformation

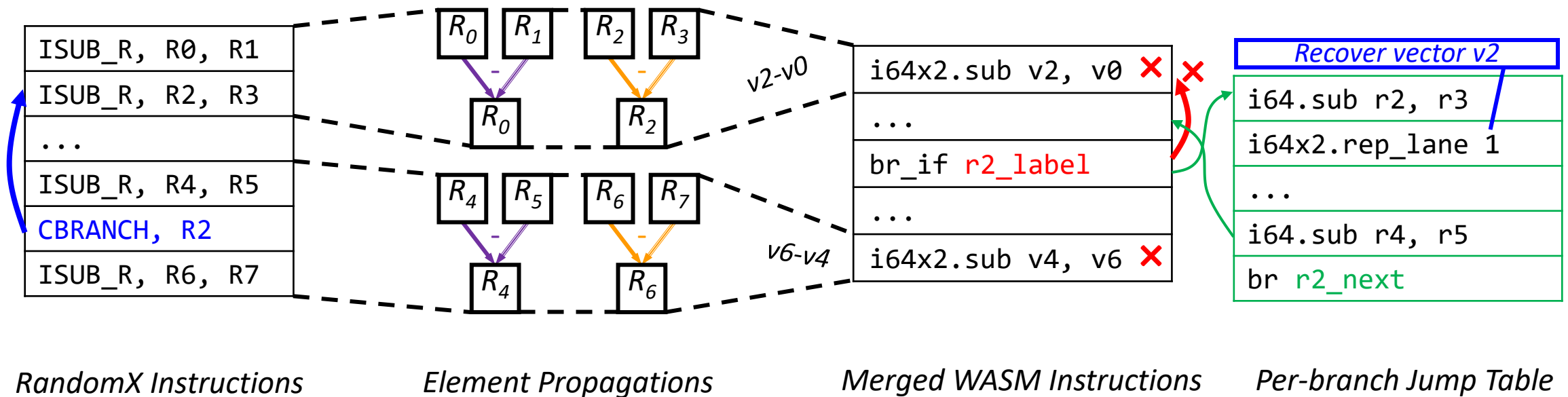
- Instruction merging is **risky**



3. Design of Vectra

□ Ensuring correct program transformation

- Symbolic constraints on branching instructions
- Jump table recovery



4. Evaluation

□ Evaluation setups

■ Devices used for testing

Device	CPU	RAM	OS
PC-1	Intel i9-10980HK (2.90 GHz)	64 GB	Windows 11
PC-2	Intel i7-10700F (2.90 GHz)	64 GB	Windows 11
PC-3	Intel E5-2420 (1.90 GHz)	64 GB	Ubuntu 22.04
PC-4	Apple M2 Pro (3.49 GHz)	16 GB	MacOS 13.4
MP-1	Snapdragon 888 (2.84 GHz)	12 GB	Android 13
MP-2	Kirin 990 (2.86 GHz)	6 GB	Android 10

■ Compared solutions

□ RandomX Compiler-Optimized

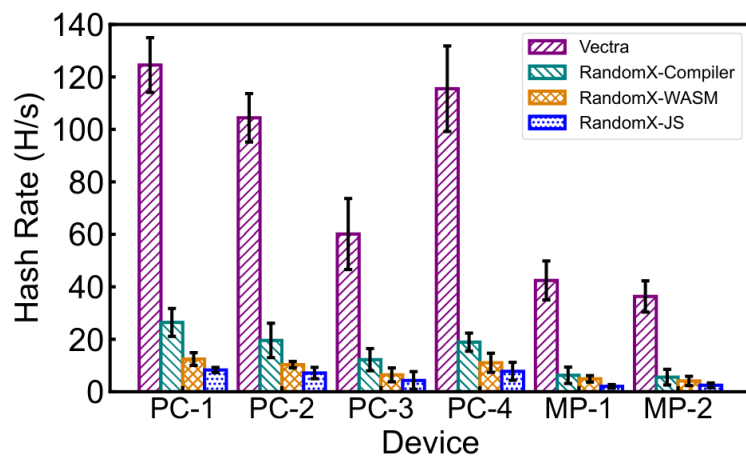
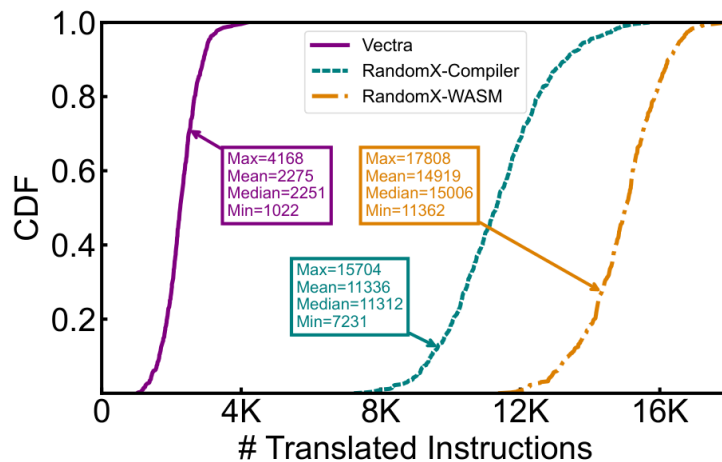
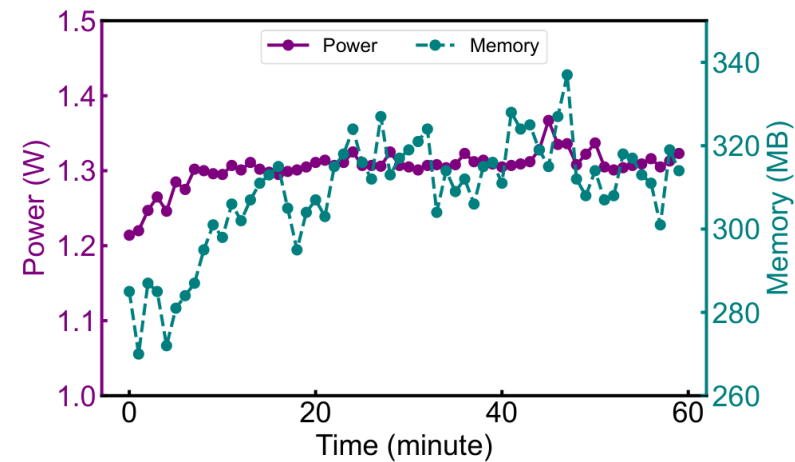
□ RandomX WASM

□ RandomX-JS

4. Evaluation

□ End-to-end performance

- **3X-16X** faster at mining Monero
- **7X** instruction reduction
- Negligible resource consumptions even on mobile devices

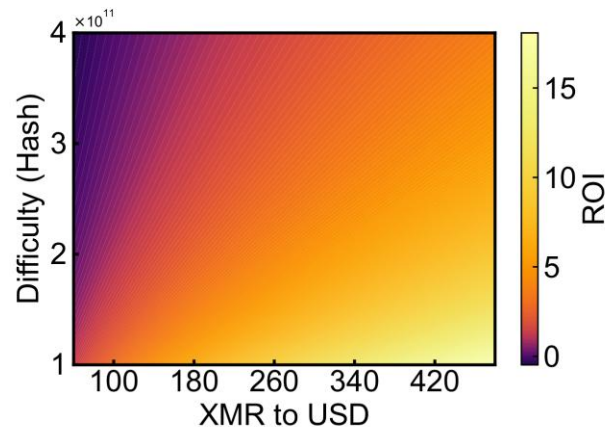


4. Evaluation

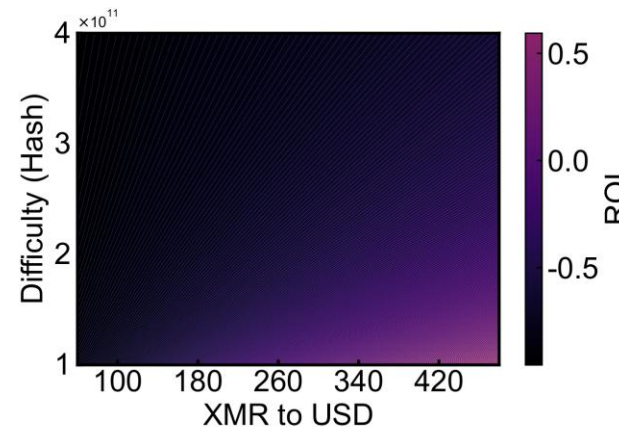
□ Real-world economic benefits

- Vetra provides **a return-on-investment (ROI) of 69% — 274%** to users
- H: hash rate, D: mining difficulty
- P: CPU power consumption
- E: Electricity price, R: exchange rate

$$ROI = \frac{Revenue - Cost}{Cost} = R \times \frac{H/D}{P/E + N/t} - 1$$



(a) Vectra



(b) RandomX-WASM

5. Conclusion

- We conduct an in-depth study on **the democracy of the cryptocurrency ecosystem**, and show how **program analysis** can benefit web cryptomining with new mining algorithms.
- We reveal the root cause of inefficient web cryptomining — the gap between **the ISAs of WASM** (a high-level, portable language for web) and the native CPU.
- We develop Vetra, a **just-in-time program transformation technique** to close the gap and enable profitable web cryptomining. It speeds up web cryptomining by 3X—16X and provides an ROI of 69% — 274% to users.

Thanks!

Q & A