REM: Resource Efficient Mining for Blockchains

Fan Zhang, Ittay Eyal, Robert Escriva,
Ari Juels, Robbert van Renesse

Vancouver, Canada

The Cryptocurrency Vision

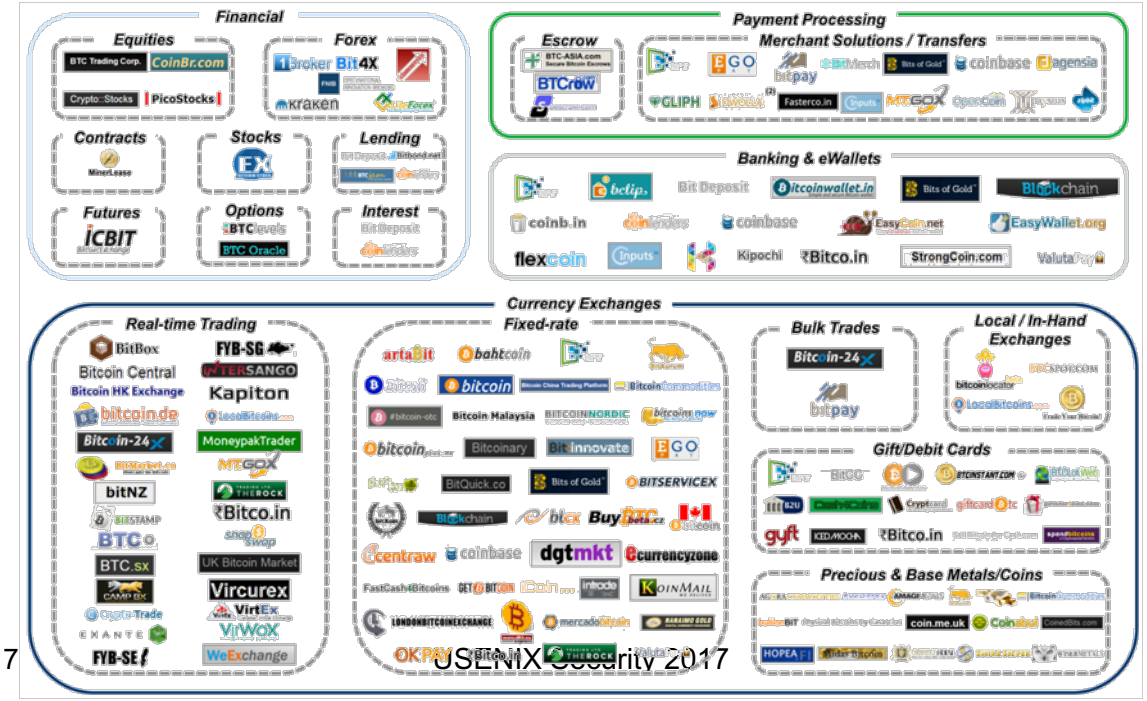
Originally

- Satoshi Nakamoto's Bitcoin ('08-'09)
- Decentralized currency

The Cryptocurrency Vision

Originally

- Satoshi Nakamoto's Bitcoin ('08-'09)
- Decentralized currency



Fintech Blockchain / DLT Vision

- Bank to bank transactions (money, securities)
- Smart contracts infrastructure
- Security structuring
- Insurance
- Provenance (supply chain, art, fair trade)
- IoT micropayments

Towards a Fintech blockchain

Reality	Fintech
Probabilistic guarantees	Hard requirements
Handful tx/sec	Thousands tx/sec
Minutes/hours for confirmation	Seconds for confirmation
Problematic resource consumption	No “waste”

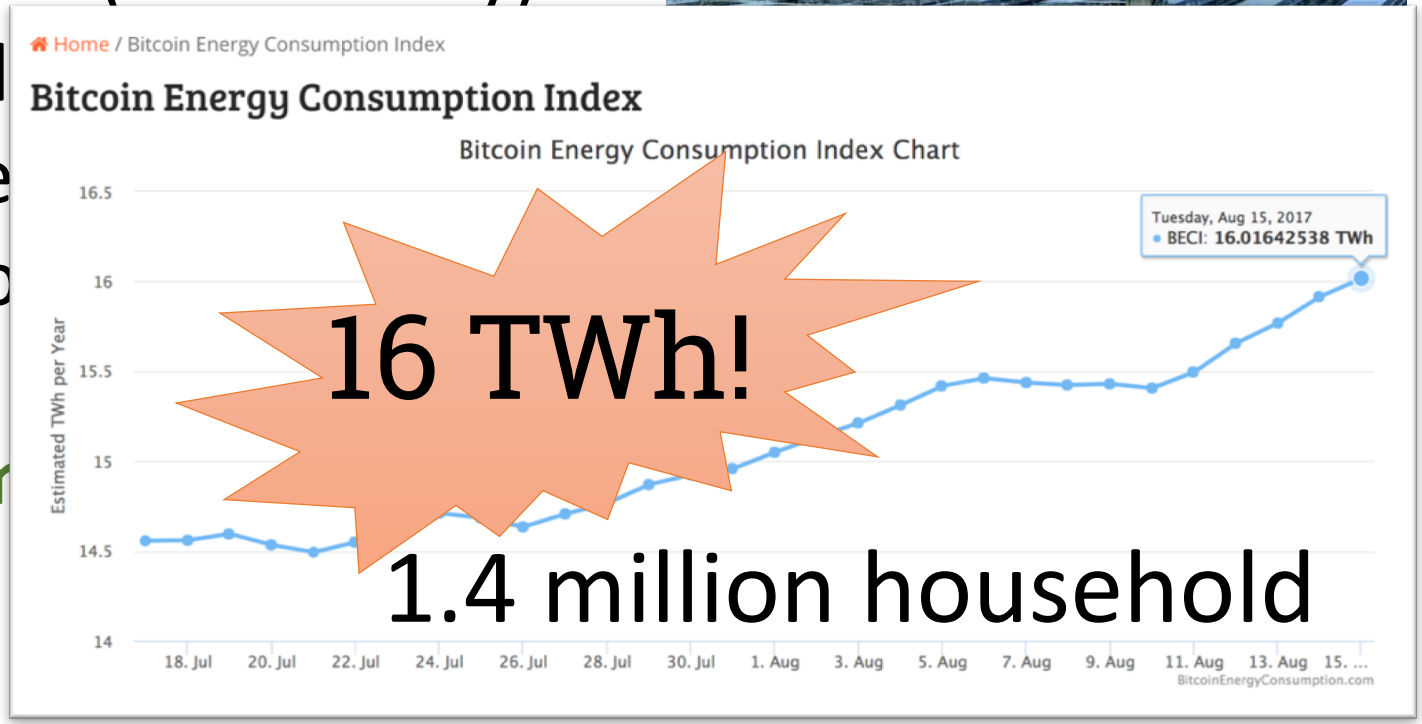
PoW: Proof of Waste?

Block proves (statistically)

real-world

- Capital e
- Operatio

Attacker m



https://digiconomist.net/bitcoin-energy-consumption

Environment-Friendly Alternatives in other settings

Permissioned system (BFT)

- Centralized

Proof of Stake

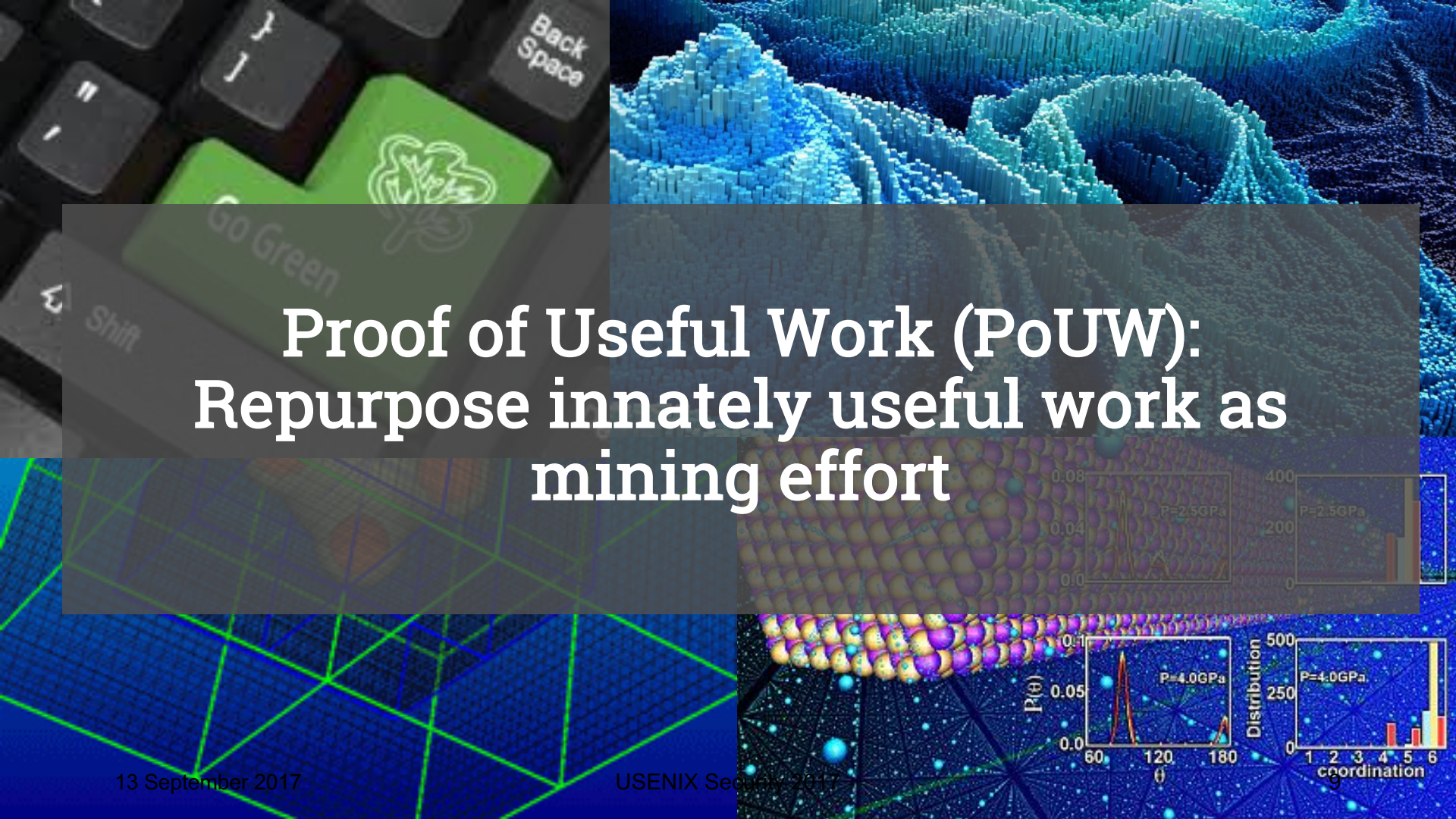
- needs a good solution for “nothing-at-stake”

Proof of Storage (Space)

- consumes storage instead of computation

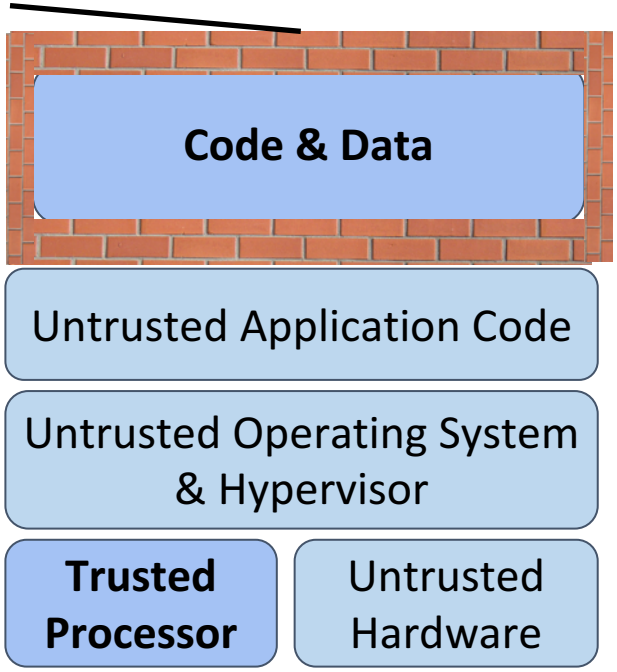

Achieve the robustness of PoW without the waste?
VOLVO
FRANKENMINT
FRANKENMINT

Proof of Useful Work (PoUW): Repurpose innately useful work as mining effort



Software Guard eXtension

"Enclave"



Integrity

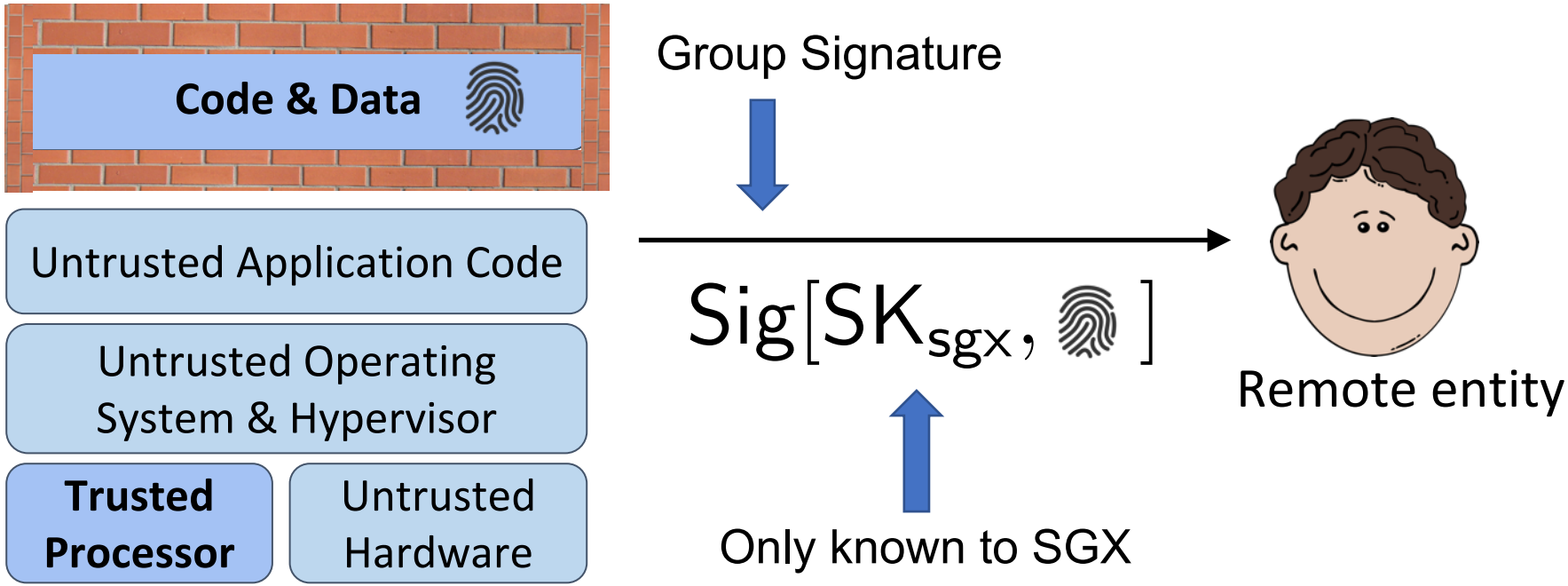
Other software and even OS cannot tamper with control flow.

Confidentiality

Other sofware and even OS can learn nothing about the interal state*.

* Modulo side channels

SGX: remote attestation

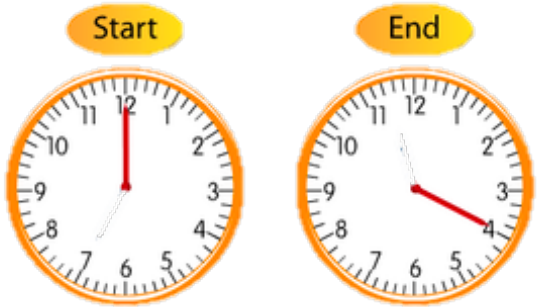


SGX-backed blockchain: A new security model

- ***Permissionless***
  - Anyone can join
- ***Partially decentralized***
  - SGX works as advertised
  - Intel manages the group signature

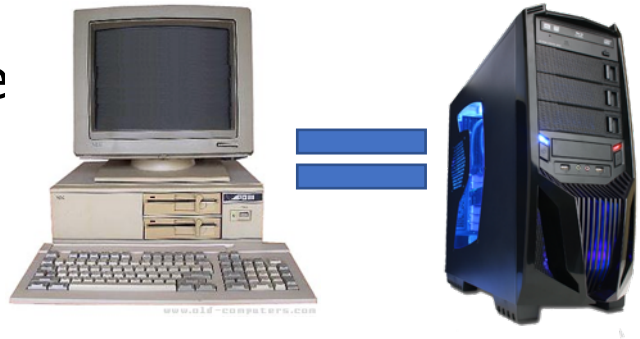
Related: Proof of Elapsed Time (PoET)

- Simulate PoW by sleeping 😴.
- Consensus in partially decentralized model
- (ideally) low mining cost + offhand mining



Unaddressed challenges in PoET

Mining power not proportional to CPU value



⇩

The ***Stale Chips Problem***:

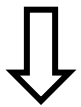
- The equilibrium is to mine using old, useless devices
- Build dedicated farms

⇩

High mining cost (contrary to the original intent)

Intel's PoET

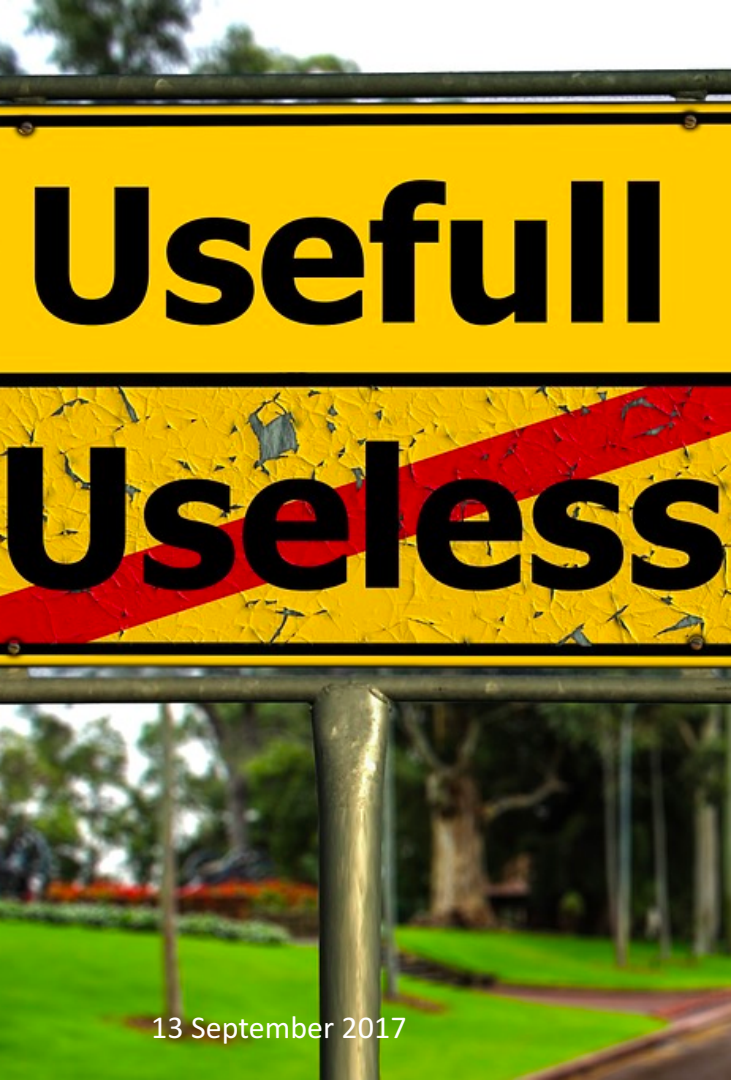
Individual CPUs can be compromised



The ***Broken Chips Problem***

Intel proposes a simple statistical test. But

1. What is the adversary's advantage?
2. What is the cost of this test?



Proof of Useful Work

- Replace the hash calculation in PoW with "useful" mining work
- Each unit of useful work grants a Bernoulli test
- Similar exponential block time

Meter the useful work

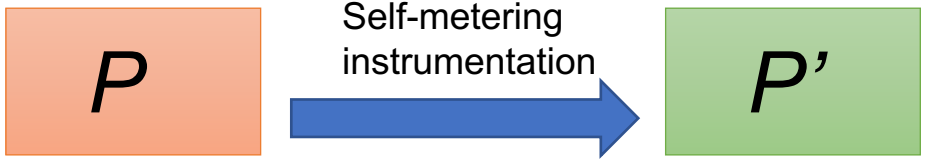
- Count CPU instructions
- Why?
  - A representative (although not perfect) metric
  - Can be done in a trustworthy way (i.e. w/o trusting OS etc.)
  - Switching to better options (if any) doesn't change REM.

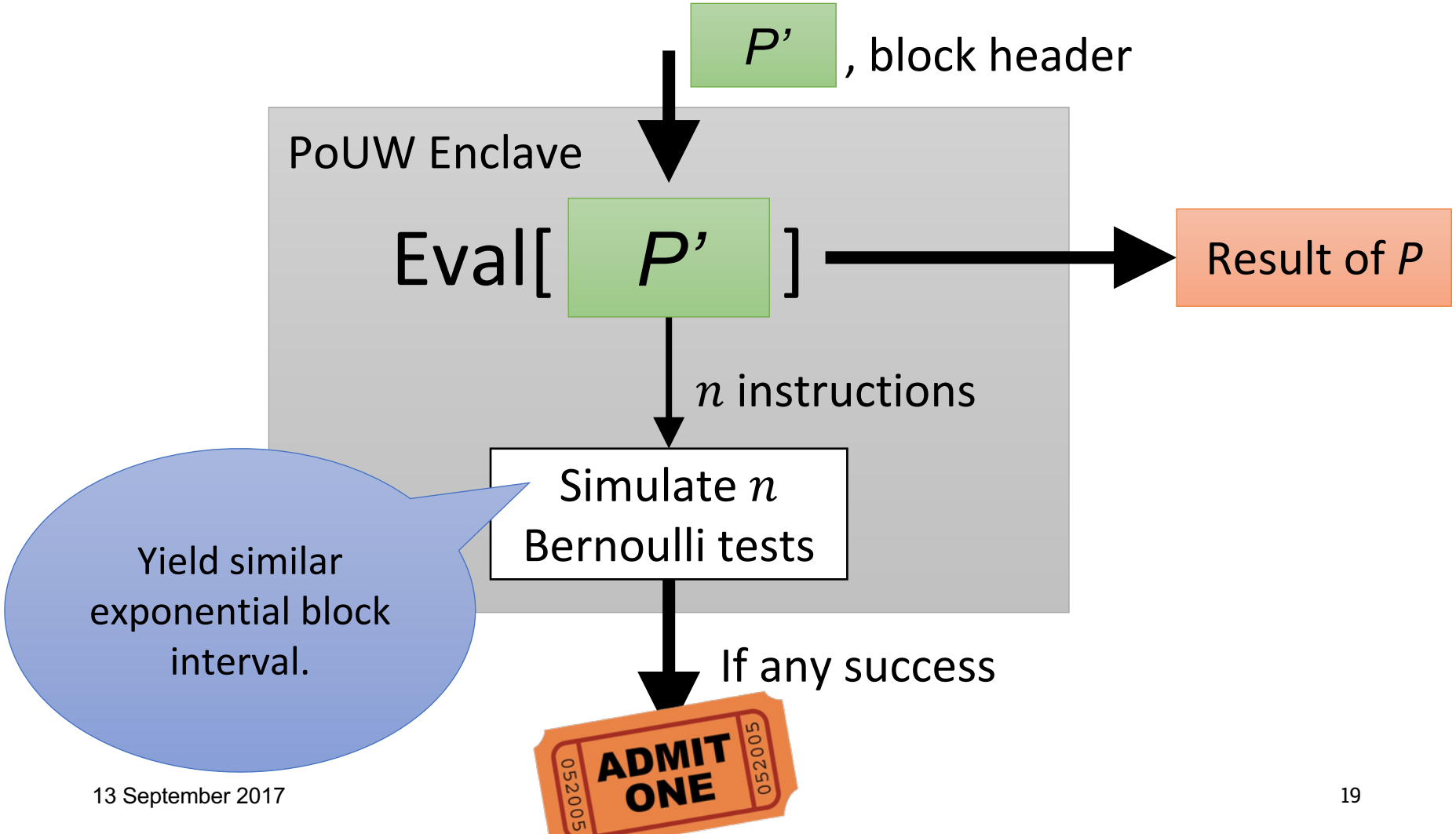
Secure Instruction Counting

- Arbitrary (malicious) programs
- Publicly verifiable
- Dynamic + static program analysis

- Enforcing W⊕X code permission
- Enforcing single-threaded enclaves
- Details in the paper

Dynamic analysis



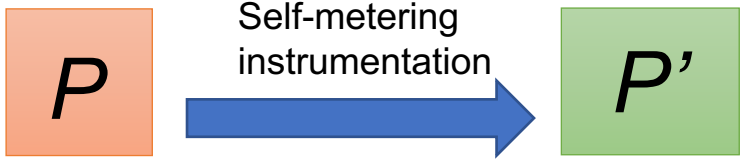

P'
, block header
PoUW Enclave
Eval[P']
Result of P
n instructions
Simulate n Bernoulli tests
Yield similar exponential block interval.
If any success
ADMIT ONE
052005
052005

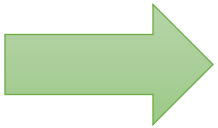
Public Verifiability

Two things to verify:

- Validity of PoUW

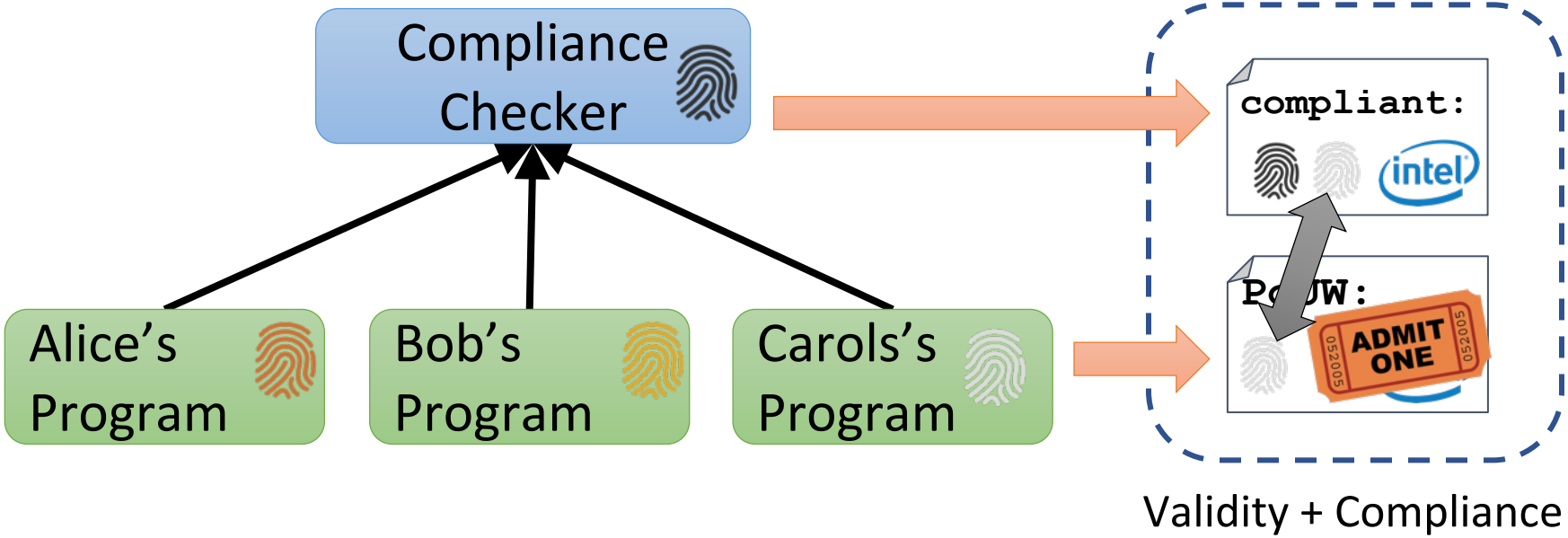
- Compliance
  - i.e. ***P'*** is correctly instrumented
  - Requires the code of ***P'***





- ❌ Put code on chain
- ❌ Predefined ***P'***
- ✅ Arbitrary ***P'***

Hierarchical Attestation



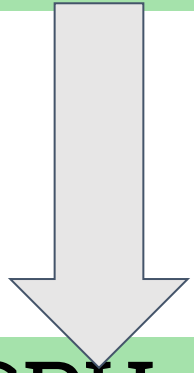
SGX might not be perfect!

- Individual CPU might be broken
- -> Can forge PoUW at will
- “Broken chip problem”

Picture source: https://www.forbes.com/sites/susanadams/2015/12/02/how-to-get-paid-to-do-nothing-5/#3fbbe0b14eaa

Implicit PKI in SGX

Intel manages the signature group

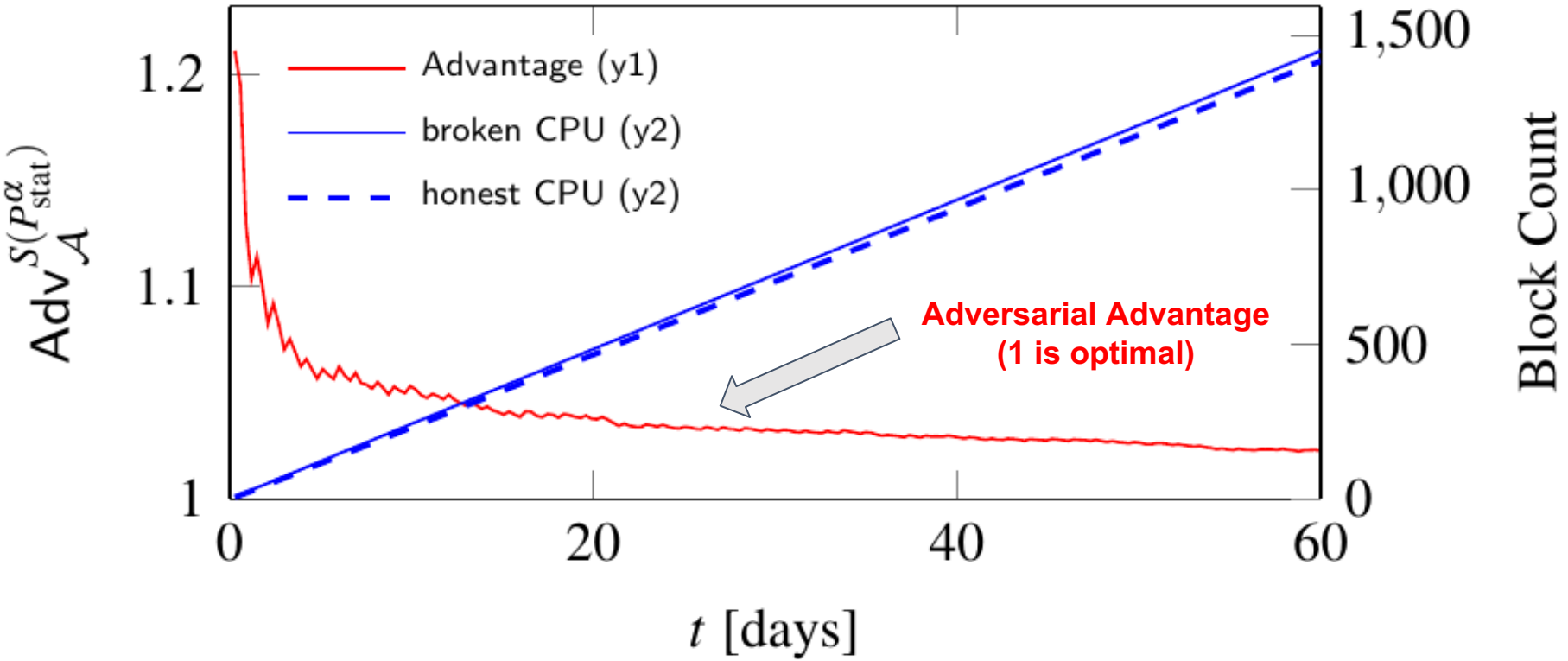


Broken SGX CPUs cannot forge identities

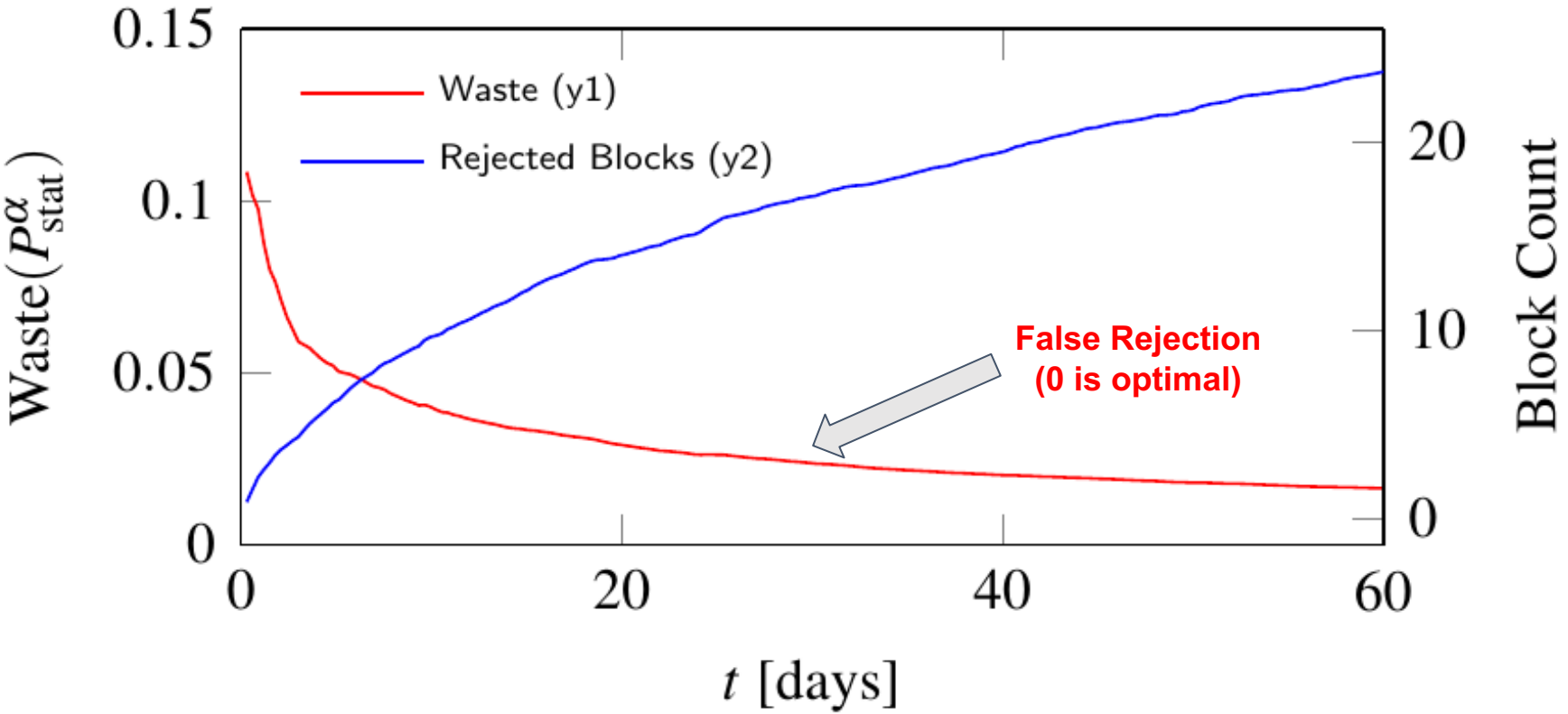
Tolerating Compromised SGX CPUs

- Adversarial Model:
  - may forge PoUW at will
  - can not forge identities
- Mitigation: statistical test
  - “If a miner is way too lucky, her block shall not be accepted.”
  - Devised rigorous framework

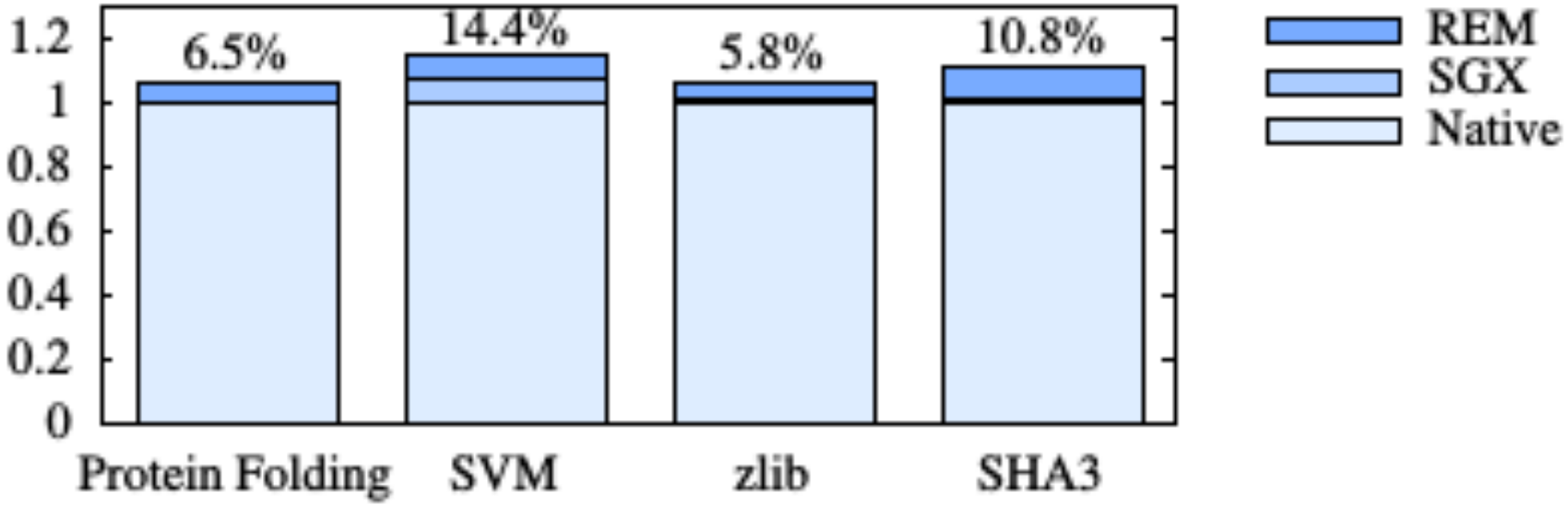
Advantage: adv revenue / honest revenue



Cost: probability of false rejection



Performance of REM



Conclusion

- PoUW: a **proof of useful work** scheme that avoids waste
- REM: a PoUW-based blockchain
  - Efficient: up to 15% overhead relative to native linux programs
- **Broken chip problem**: rigorous framework and effective policies.