KACHINA: Foundations of Private Smart Contracts

Thomas Kerber
papers@tkerber.org

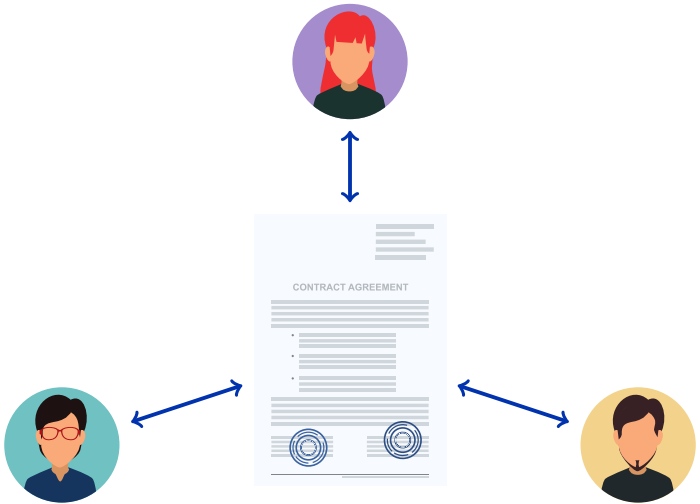
Aggelos Kiayias
akiayias@ed.ac.uk

Markulf Kohlweiss
mkohlwei@ed.ac.uk

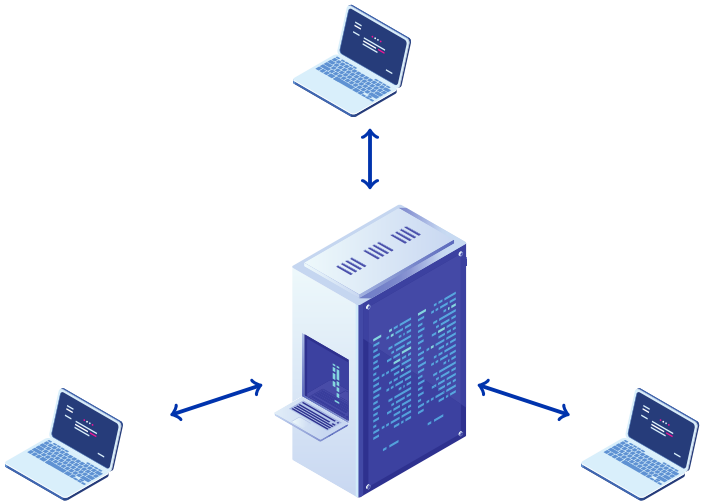
The University of Edinburgh & IOHK

June 8, 2021

Reactive State Machines



Relation to Client/Server Model

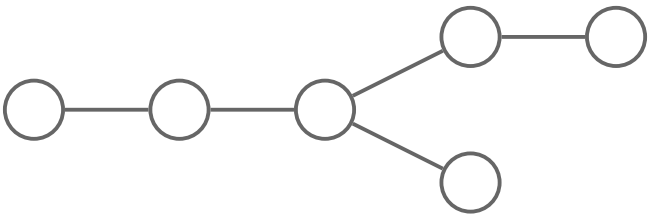



ebay

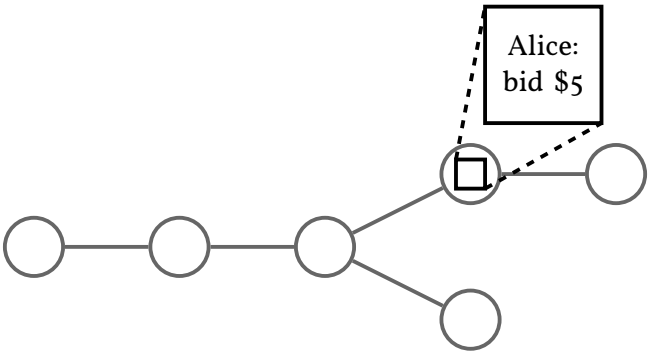

facebook

Centralised privacy relies on trust

Blockchains and Smart Contracts



Blockchains and Smart Contracts

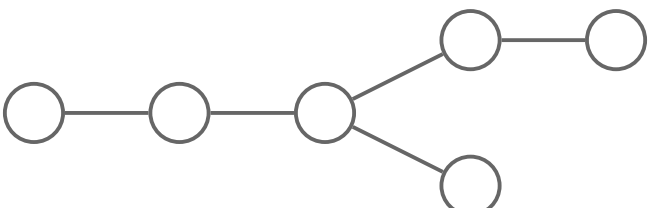


Perfect Privacy

- The same reactive state machine
- No leakage
- Decentralised implementation

- Multi-party computation (MPC) achieves this!
- Run a committee-based chain (e.g. Algorand)
- Have the same committee run MPC for each contract call
- Prohibitively expensive

Decentralisation?



This setting limits privacy

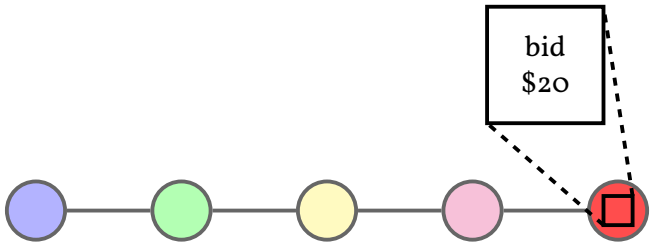
Example: The King of Ether

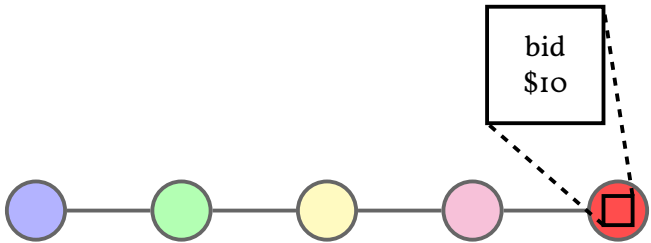
- The “throne” can be bought
- The price increases exponentially
- The previous king gets the proceeds
- A fee is paid for each attempt

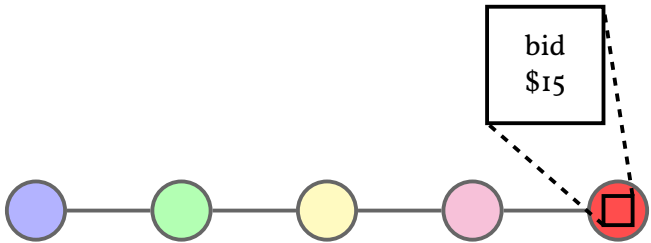
A private variant would hide:

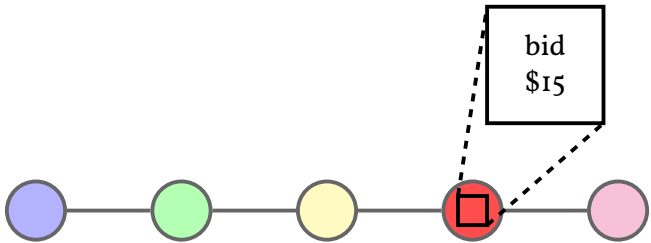
- The value of the throne
- Who holds it
- When it was obtained

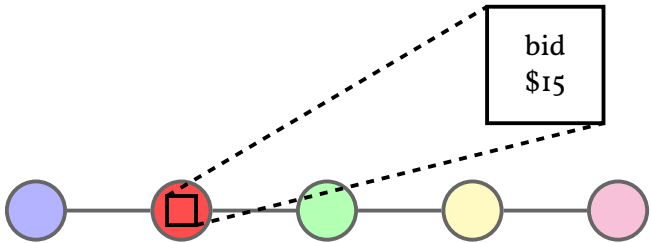
It cannot


bid
$20

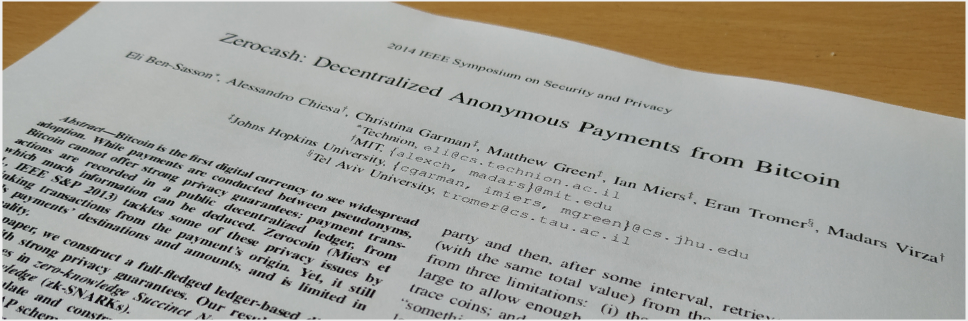

bid
$10


bid
$15

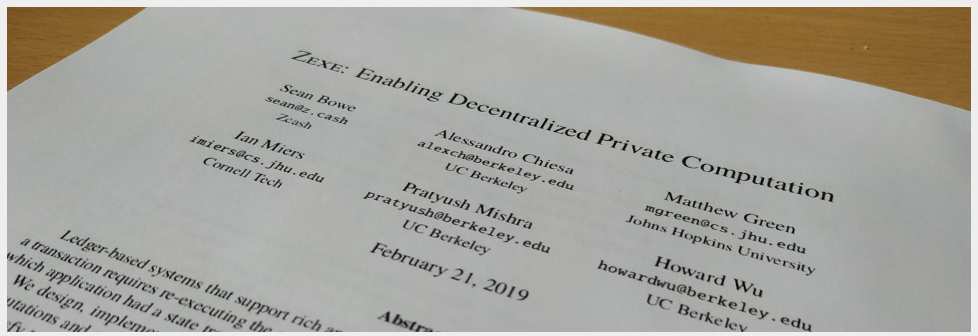

bid
$15


bid
$15

There is Hope!



There is Hope!



ZEXE: Enabling Decentralized Private Computation

Sean Bowe
sean@z.cash
Zcash

Ian Miers
imiers@cs.jhu.edu
Cornell Tech

Alessandro Chiesa
alexch@berkeley.edu
UC Berkeley

Pratyush Mishra
pratyush@berkeley.edu
UC Berkeley

Matthew Green
mgreen@cs.jhu.edu
Johns Hopkins University

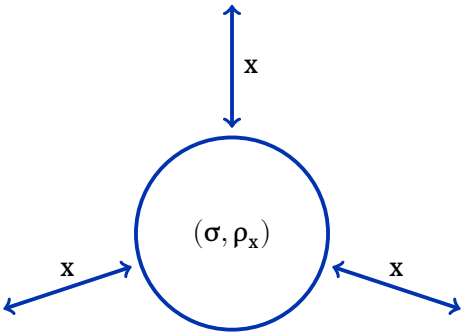
Howard Wu
howardwu@berkeley.edu
UC Berkeley

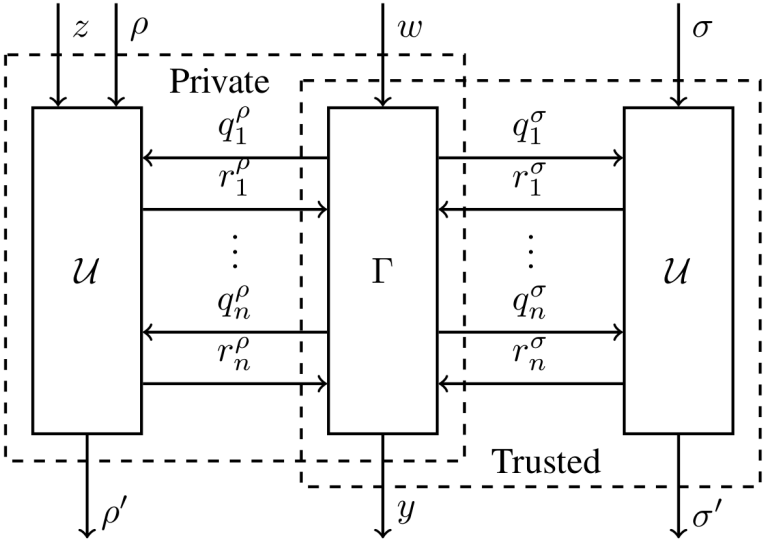
February 21, 2019

Ledger-based systems that support rich
a transaction requires re-executing the
which application had a state
We design, implem
tations and

There are perfect solutions
for individual problems

Back to State Machines




z
ρ
w
σ
Private
q_1^ρ
r_1^ρ
q_1^σ
r_1^σ
$\mathcal{U}$
Γ
$\mathcal{U}$
q_n^ρ
r_n^ρ
q_n^σ
r_n^σ
Trusted
ρ′
y
σ′


ZEROCASH

≈


PRIVATE
PAYMENTS

Thank you!

Please see `https://drwx.org/2020-07-03-copyright.txt` for copyrights and attribution of used images.