



Modern key distribution with *ClaimChains*

A decentralized Public Key Infrastructure that supports privacy-friendly social verification

NEXTLEAP

Bogdan Kulynych
Carmela Troncoso

Marios Isaakidis
George Danezis

photo by lisa cee

BLOCKCHAINS

A background image featuring Woody and Buzz Lightyear from the Toy Story franchise. Woody is on the left, looking slightly concerned. Buzz is on the right, in his iconic green and purple space suit, holding a small yellow star in his right hand.

HIGH-INTEGRITY

Tamper proof
Authenticity

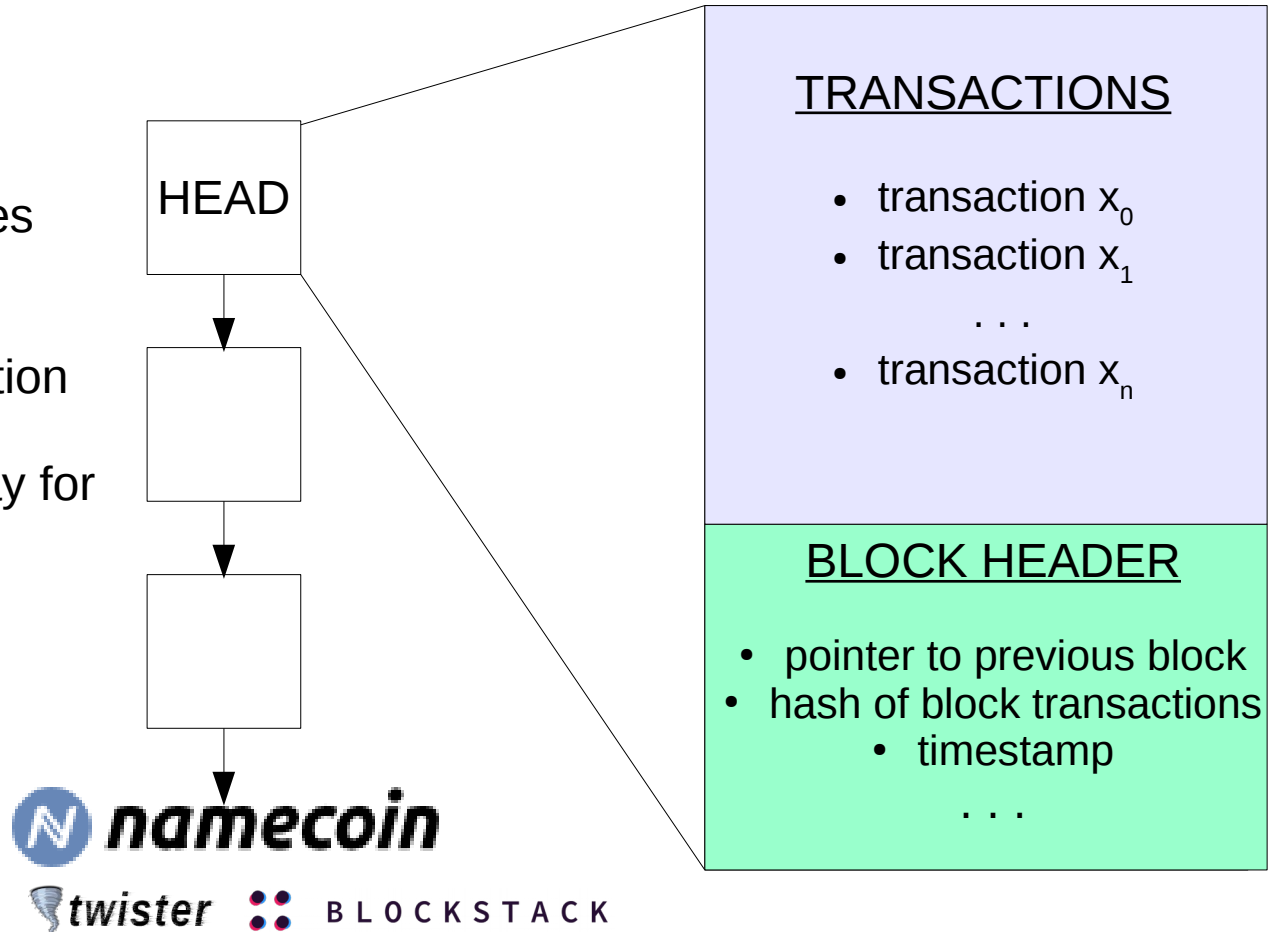
DECENTRALIZATION

Availability
Censorship-resistant
Global consensus

BLOCKCHAINS EVERYWHERE

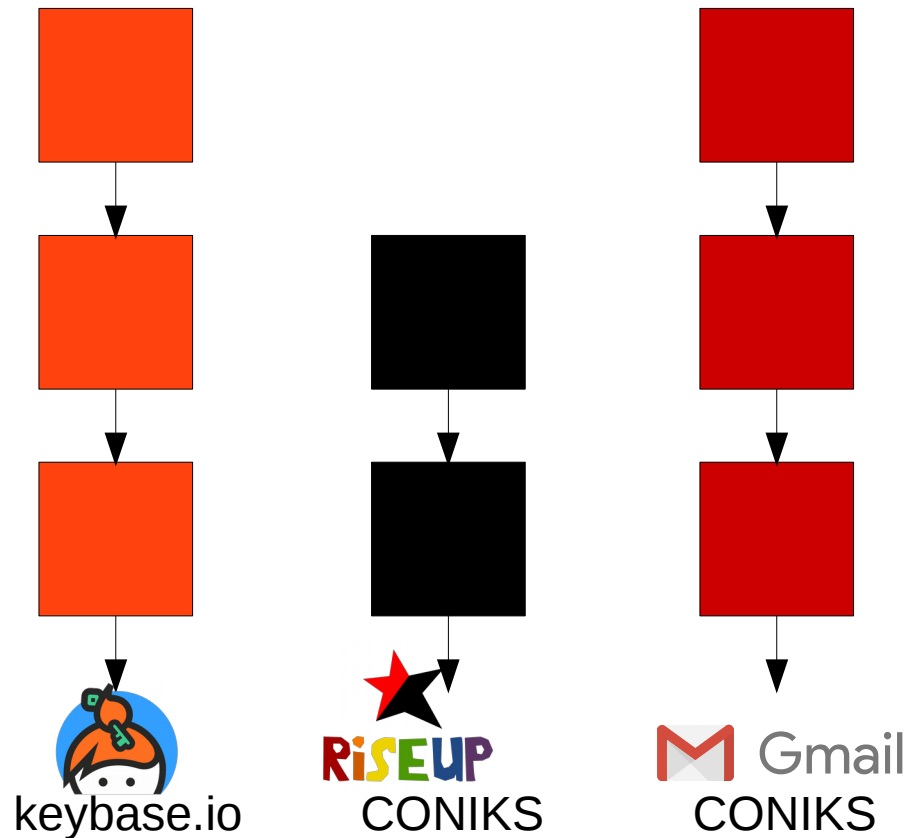
Cryptocurrency chains

- ✓ Powerful abstraction for identities
- ✓ Global namespace
- ✗ No mechanism for social validation
- ✗ All transactions are public
- ✗ Users need to buy coins and pay for transaction fees
- ✗ Resource expensive



Federated “Merkle prefix tree” chains

- ✓ Accountability
- ✓ Easy discovery
- ✓ Efficient
- ✗ Do not prevent equivocation
- ✗ Centralization
 - Single point of failure
 - Surveillance



Merkle binary prefix trees

Leaf nodes are ordered using
a Verifiable Random Function

ROOT

0

1

0

1

0

1

$H(\text{child}_0, \text{child}_1)$

0

1

0

1

0

1

0

1

$i = 000\dots$
 $v = \text{value}_Y$

$i = 001\dots$
 $v = \text{value}_X$

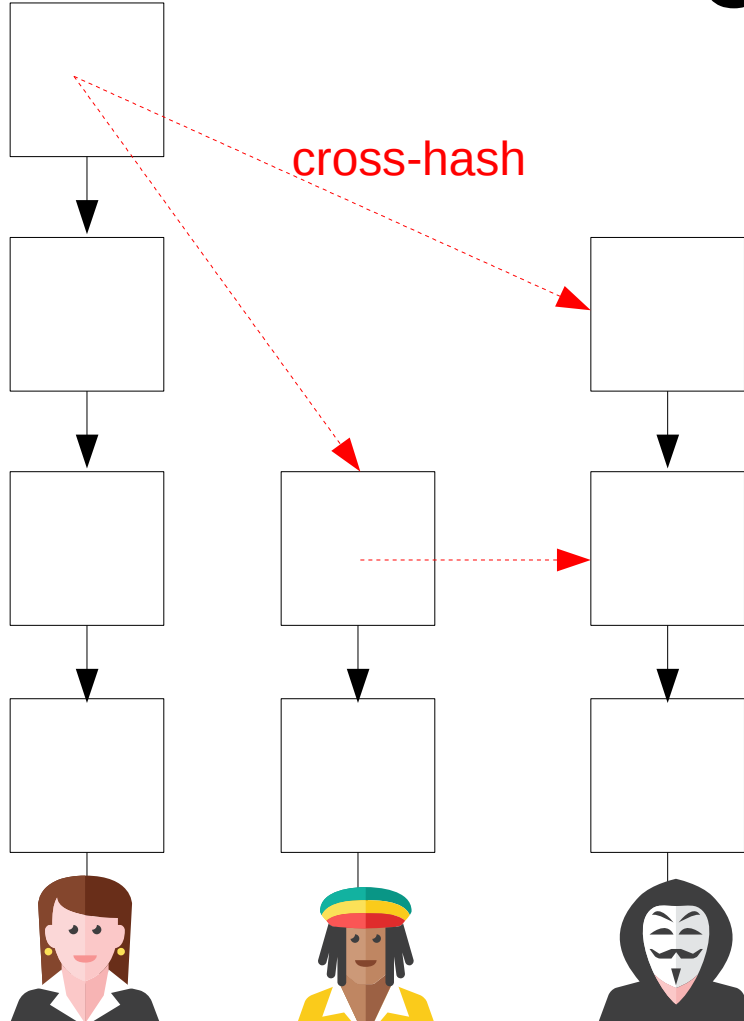
ClaimChains

claimchain.github.io



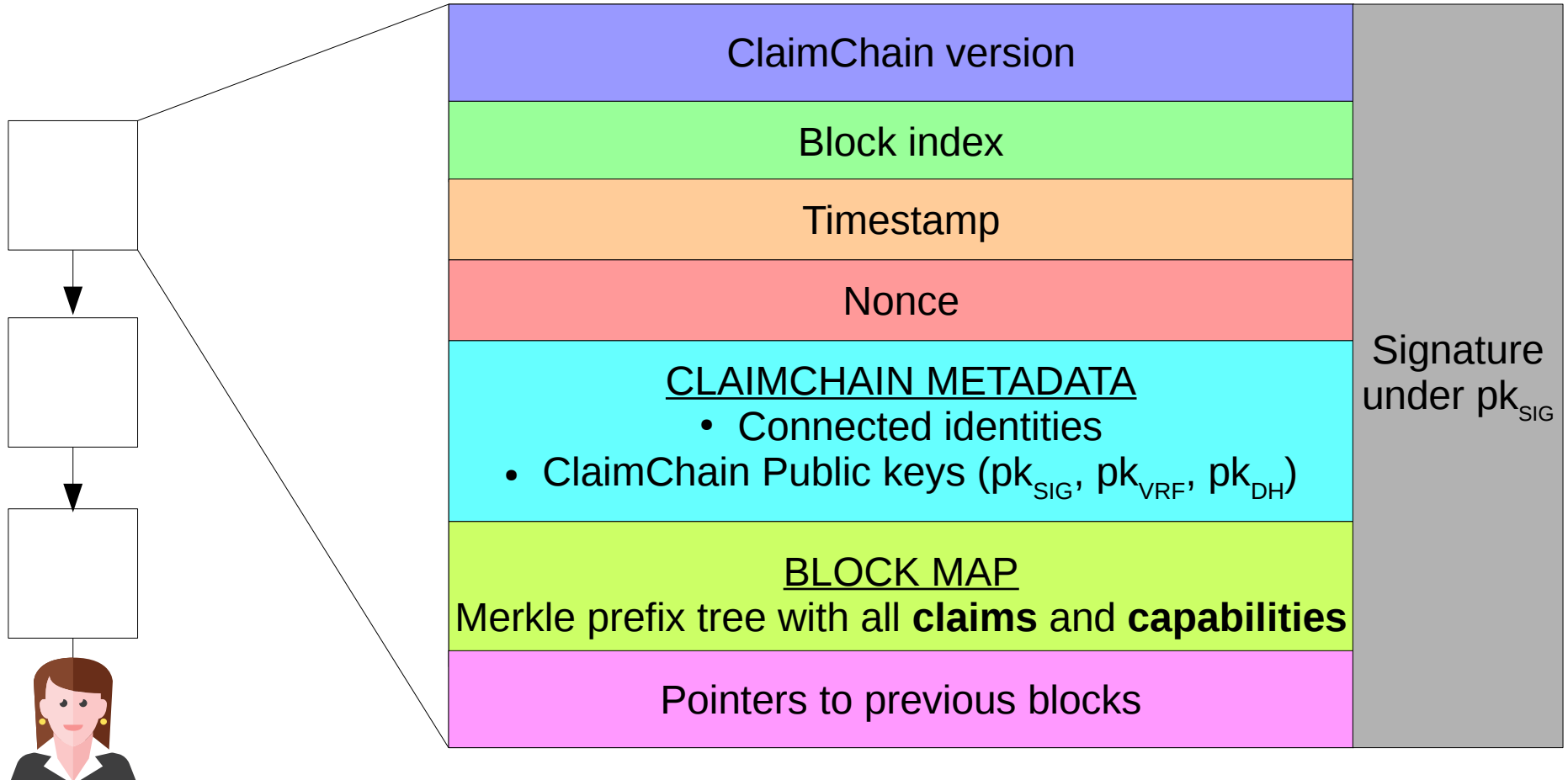
photo by Wendi Halet

ClaimChains



- A ClaimChain for each user/device/identity
- Blocks appended as needed
- Compromises appear as ClaimChain forks
- Private Claims
- Chain owner selects who can read a specific claim - all readers get the same content
- Propagation of key updates in “cliques” of users
- Vouch for the latest state of a friend’s ClaimChain
- Privacy-friendly social validation - Web of Trust

ClaimChains block structure



Resilience

- Field research to understand user needs
 - Collaboration with related communities
 - Formal methods from security research:
 - Cryptographic games to define security and privacy properties
 - Formally verified implementation
 - Simulations using real world data
 - Interoperability and plans for gradual deployment
-
- User-centric design
 - Multidisciplinarity
 - Open Innovation (open access and extendability)

A green metal ring is attached to a chain. The ring is on the left, and the chain extends to the right. The background is blurred, showing a building and two orange lights.

Thank you

@misaakidis
claimchain.github.io