

Decentralised location verification system

Conor Taylor

B.A.(Mod.) Computer Science
Final Year Project, April 2016
Supervisor: Stephen Barrett

Problem

A system that allows participants to verify a users claimed location.

Problem

A system that allows participants to verify a users claimed location.

Goals:

Problem

A system that allows participants to verify a users claimed location.

Goals:

- ▶ False location claims must be detectable.

Problem

A system that allows participants to verify a users claimed location.

Goals:

- ▶ False location claims must be detectable.
- ▶ Privacy protecting.

Problem

A system that allows participants to verify a users claimed location.

Goals:

- ▶ False location claims must be detectable.
- ▶ Privacy protecting.
- ▶ Cannot rely on any centralised resources.

Problem

A system that allows participants to verify a users claimed location.

Goals:

- ▶ False location claims must be detectable.
- ▶ Privacy protecting.
- ▶ Cannot rely on any centralised resources.
- ▶ Capable of running in the background on mobile devices.


Background


There are **no** known existing decentralised location proof systems.


Existing centralised solutions: hardware and/or software

Design

3 distinct entities:

▶ Mobile node 

▶ Miner node 

▶ Verifier node 

Design

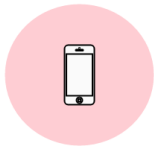
Overview



Mobile node

Design

Overview



Mobile node

Design

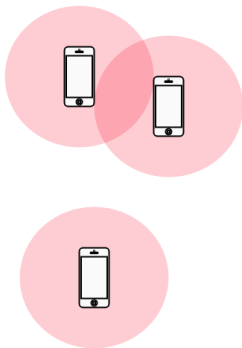
Overview



Mobile nodes

Design

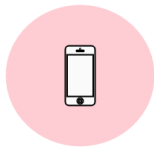
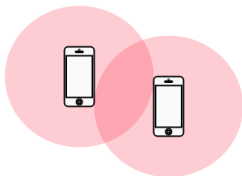
Overview



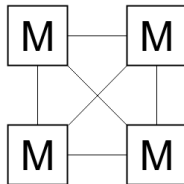
Mobile nodes

Design

Overview



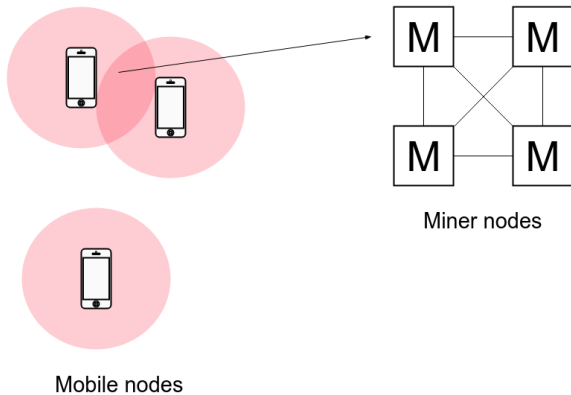
Mobile nodes



Miner nodes

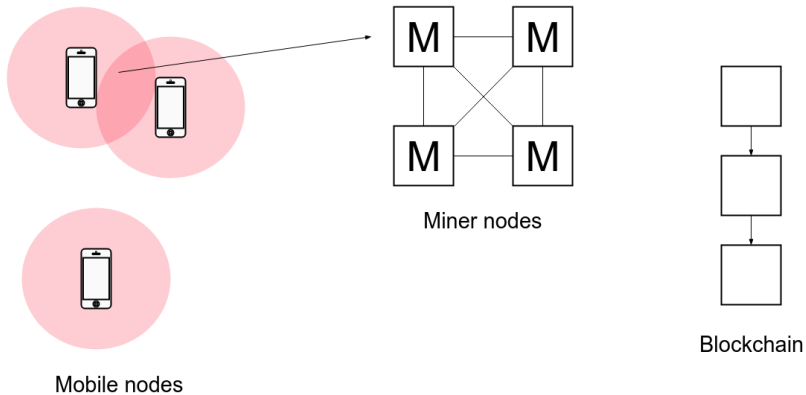
Design

Overview



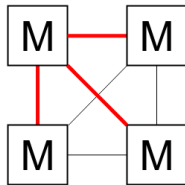
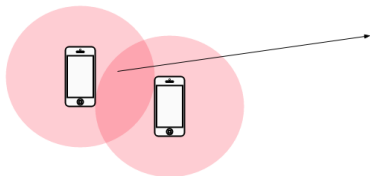
Design

Overview

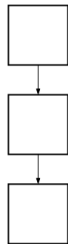


Design

Overview



Miner nodes

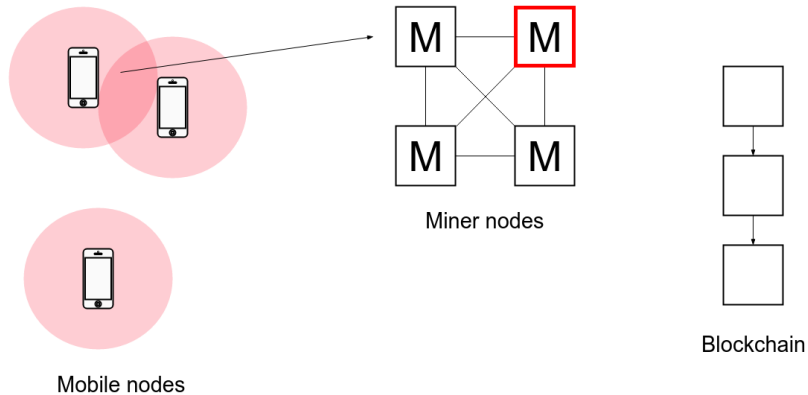


Blockchain

Mobile nodes

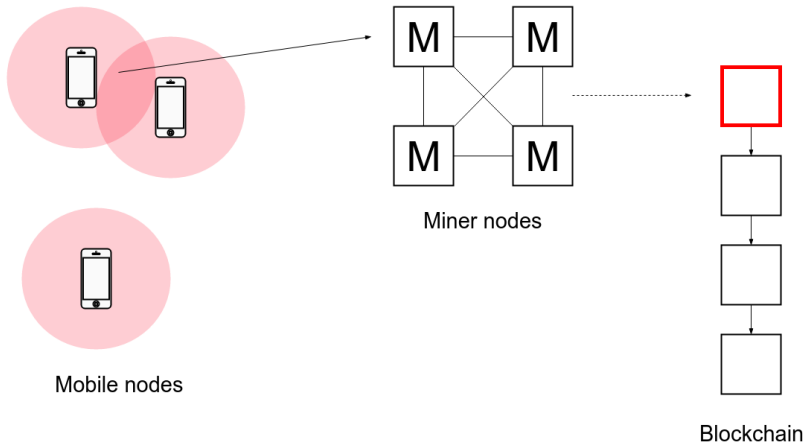
Design

Overview



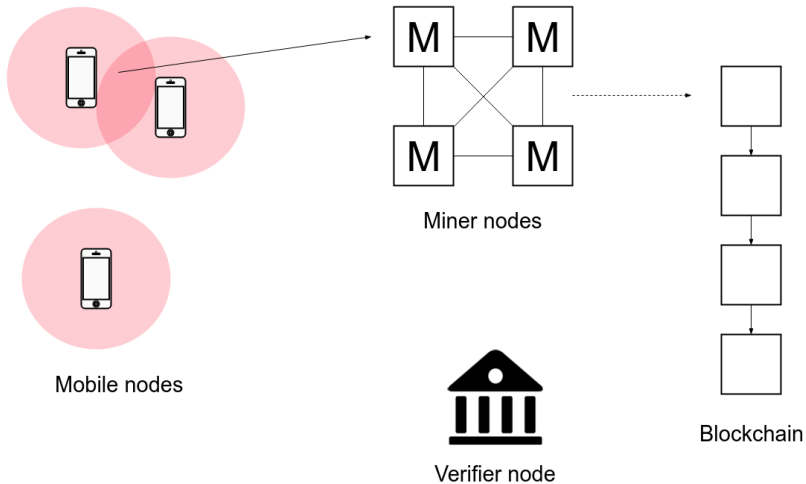
Design

Overview



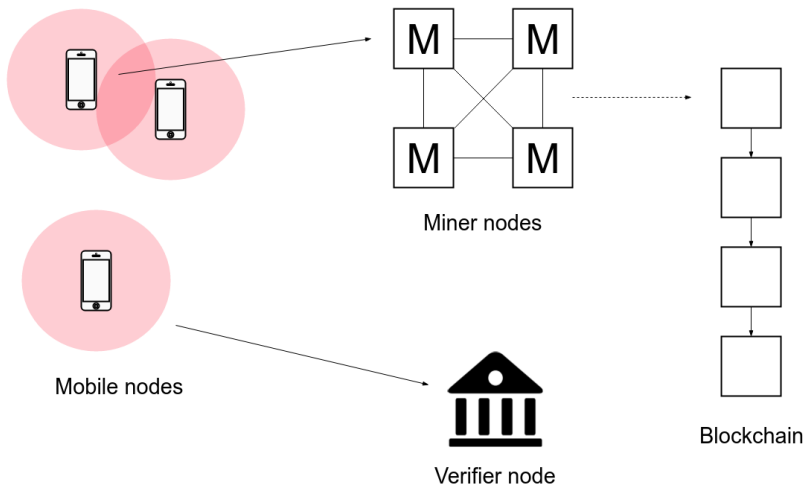
Design

Overview



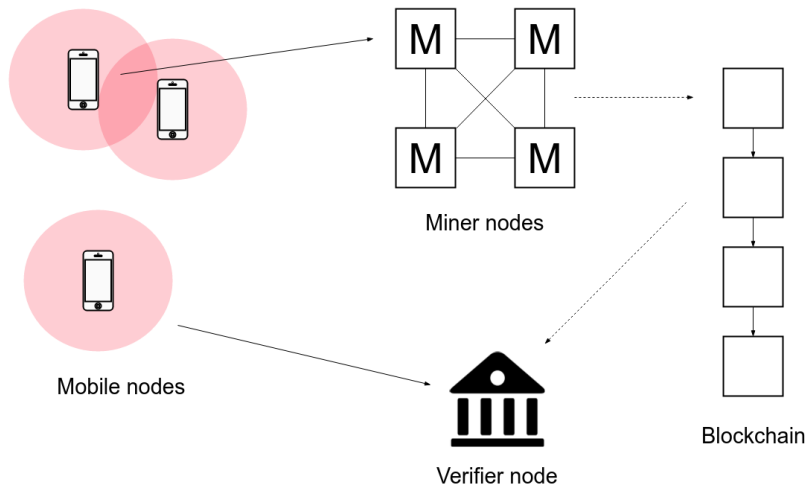
Design

Overview



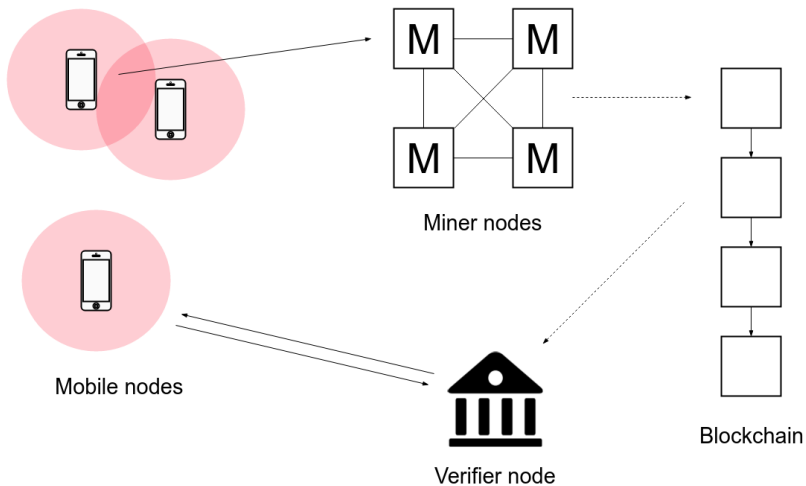
Design

Overview



Design

Overview



Design

Identities

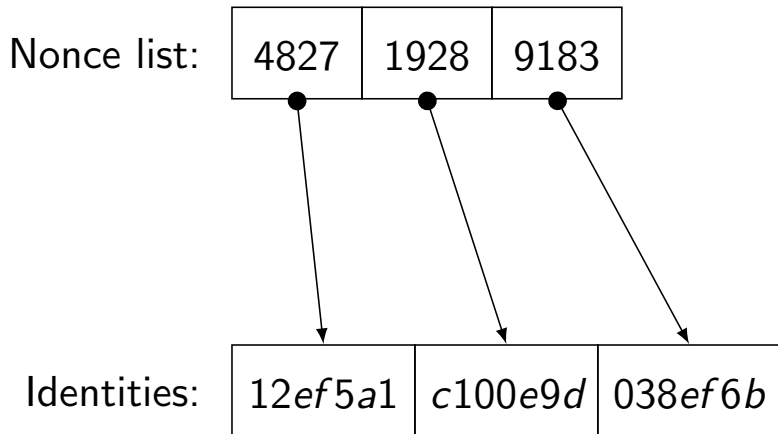
Used to anonymously identify a node in a transaction.

Balancing goals:

- ▶ False location claims must be detectable.
- ▶ Privacy protecting.

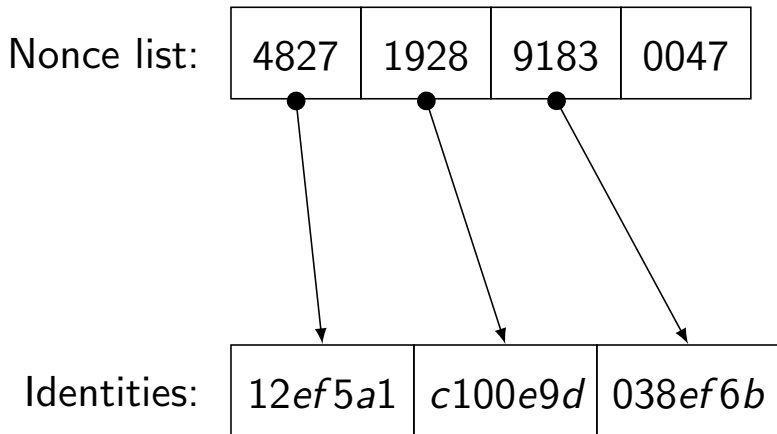
Design

Identities: Nonce Lists



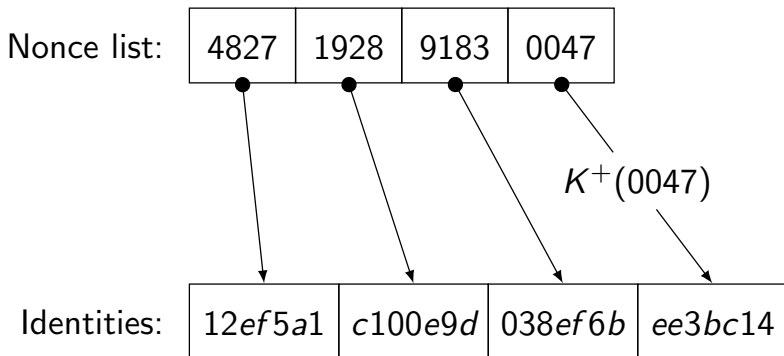
Design

Identities: Nonce Lists



Design

Identities: Nonce Lists



Design

Identities: Duplication

Identity duplication is unavoidable in a decentralised system.

ID	Contents
...	
ffa0	
ffa1	
ffa2	T_{A4}
ffa3	
ffa4	T_{B87}
...	

Design

Identities: Duplication

Identity duplication is unavoidable in a decentralised system.

ID	Contents
...	
ffa0	
ffa1	
ffa2	T_{A4} , T_{C102}
ffa3	
ffa4	T_{B87}
...	