Decentralised location verification system

Conor Taylor

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

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

- Is is possible?

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

- Is is possible?
- Is it resilient to attack?

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

- Is is possible?
- Is it resilient to attack?
- Does it satisfy my goals?

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

- Is is possible?
- Is it resilient to attack?
- Does it satisfy my goals?

Goals:

- Privacy protecting.

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

- Is is possible?
- Is it resilient to attack?
- Does it satisfy my goals?

Goals:

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

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

- Is is possible?
- Is it resilient to attack?
- Does it satisfy my goals?

Goals:

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

Problem

Design and evaluate a decentralised system that allows participants to prove their location.

- Is is possible?
- Is it resilient to attack?
- Does it satisfy my goals?

Goals:

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

Background

There are no known existing decentralised location proof systems.

Background

There are no known existing decentralised location proof systems.

There are existing *distributed* location proof systems, with different interesting approaches.

Background

HP Laboratories

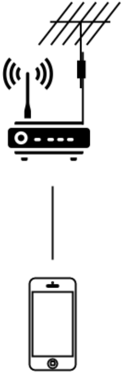
HP Laboratories.

Background

HP Laboratories

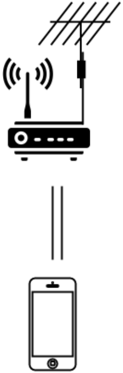
Background

HP Laboratories



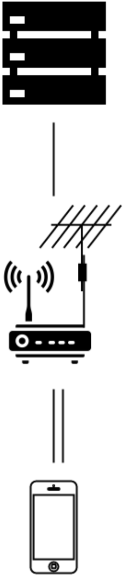
Background

HP Laboratories



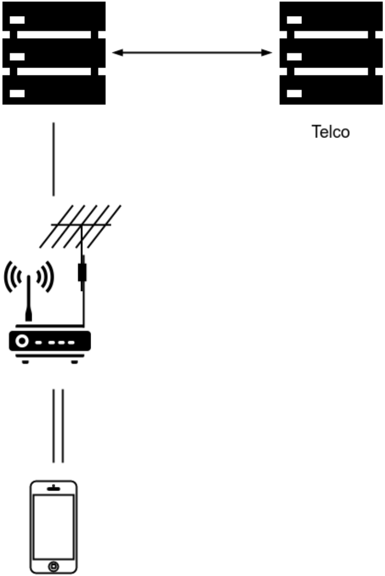
Background

HP Laboratories



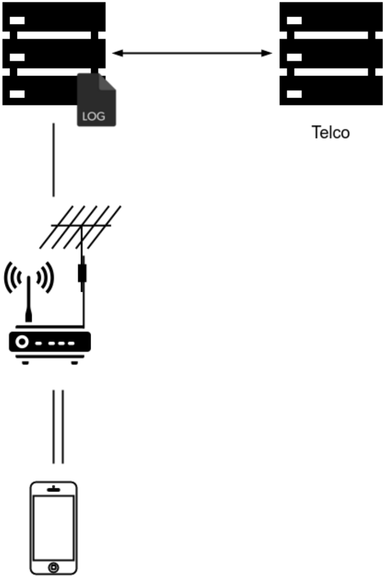
Background

HP Laboratories



Background

HP Laboratories



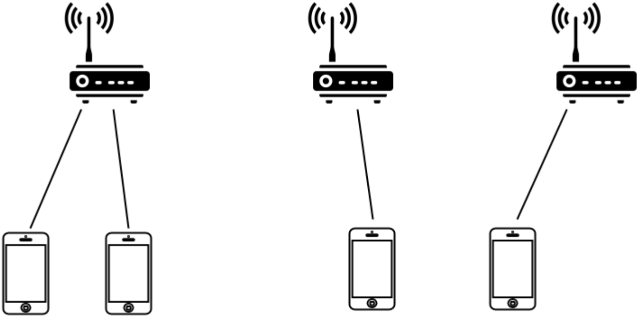
Background

University of Waterloo

University of Waterloo.

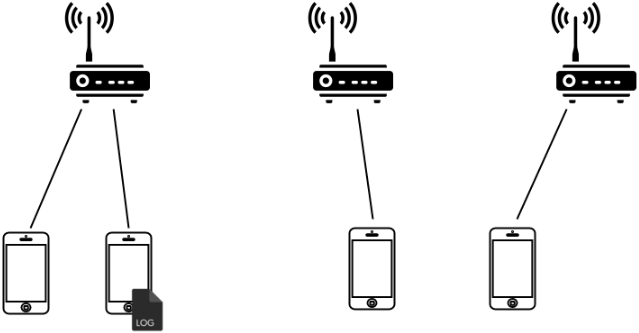
Background

University of Waterloo



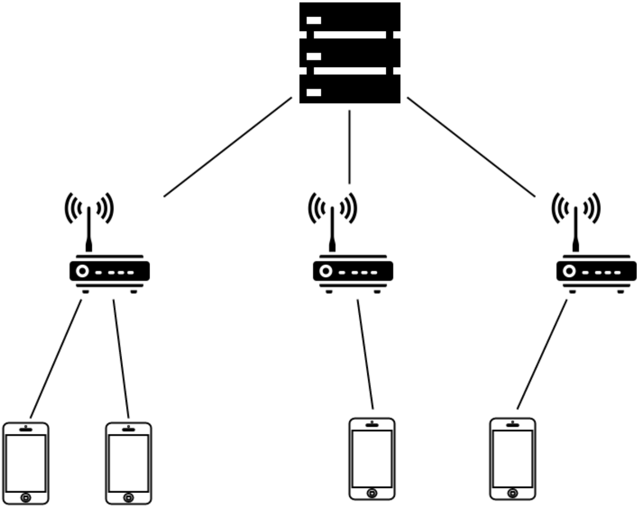
Background

University of Waterloo



Background

University of Waterloo



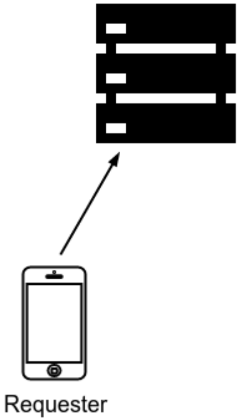
Background

Who, When. and Where?

Who, When, and Where?
University of Alabama.

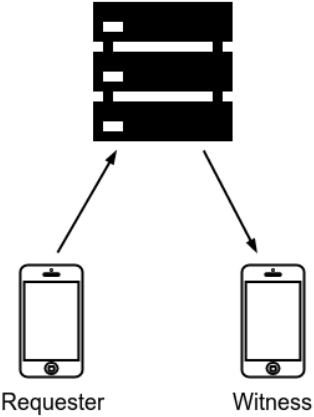
Background

Who, When. and Where?



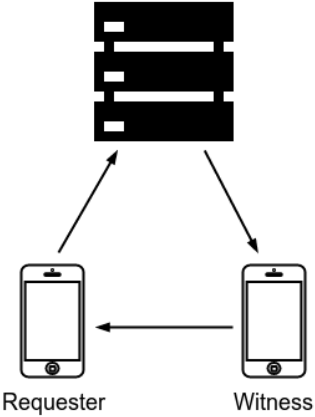
Background

Who, When. and Where?



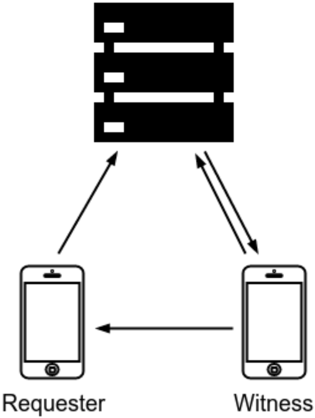
Background

Who, When. and Where?



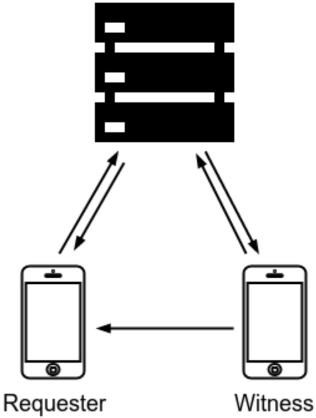
Background

Who, When. and Where?



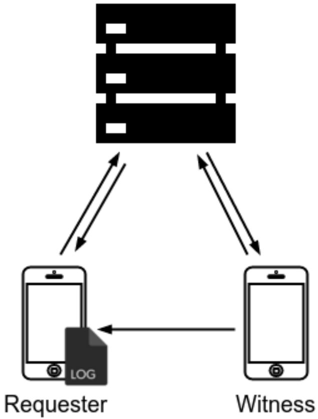
Background

Who, When. and Where?



Background

Who, When. and Where?



Problem

Issues

A decentralised location proof system needs a way of:

- Creating, storing, and providing access to location proofs.
- Detecting fake location proofs.
- Allowing users full control over their own privacy.

Problem

Issues

A decentralised location proof system needs a way of:

- Creating, storing, and providing access to location proofs.
- Detecting fake location proofs.
- Allowing users full control over their own privacy.

Without any central resource to store data or manage the system.

Background

Blockchain

A blockchain is a decentralised, tamper-proof, append-only ledger.

Background

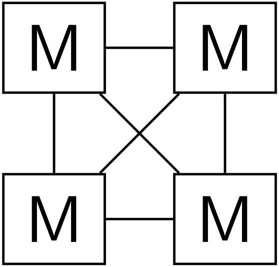
Blockchain

A blockchain is a decentralised, tamper-proof, append-only ledger.

Allows transaction records to be stored publicly and permenantly, without use of a central authority.

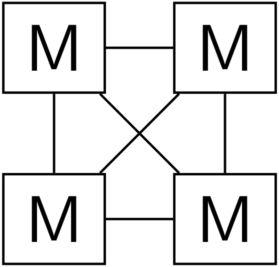
Background

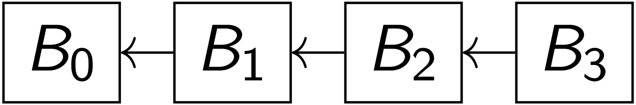
Blockchain



Background

Blockchain





Background

Blockchain

Decentralised, tamper-proof method of storing location proofs.

Design

3 distinct entities:

- Mobile node 📱
- Miner node M
- Verifier node 🏛

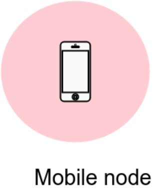
Design

Overview

Mobile node

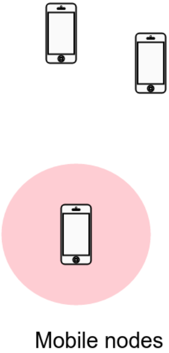
Design

Overview



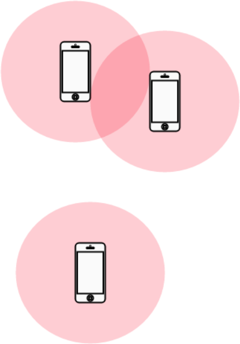
Design

Overview



Design

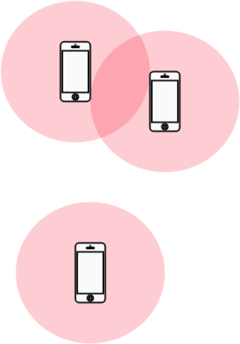
Overview



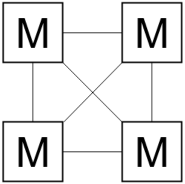
Mobile nodes

Design

Overview



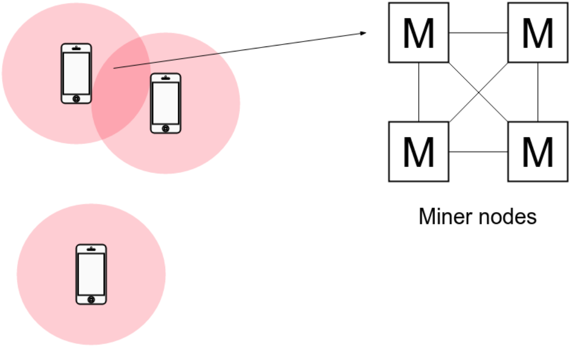
Mobile nodes



Miner nodes

Design

Overview

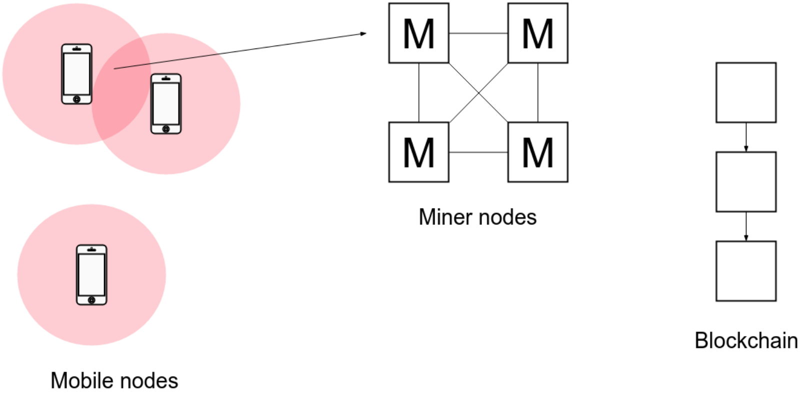


Miner nodes

Mobile nodes

Design

Overview



M M

M M

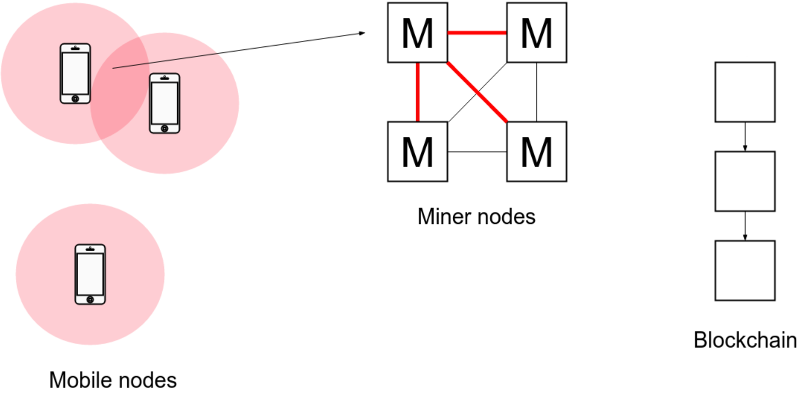
Miner nodes

Mobile nodes

Blockchain

Design

Overview



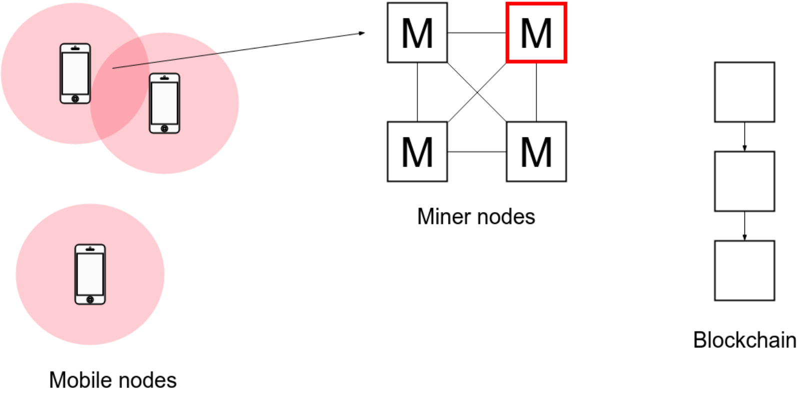
Mobile nodes

Miner nodes

Blockchain

Design

Overview



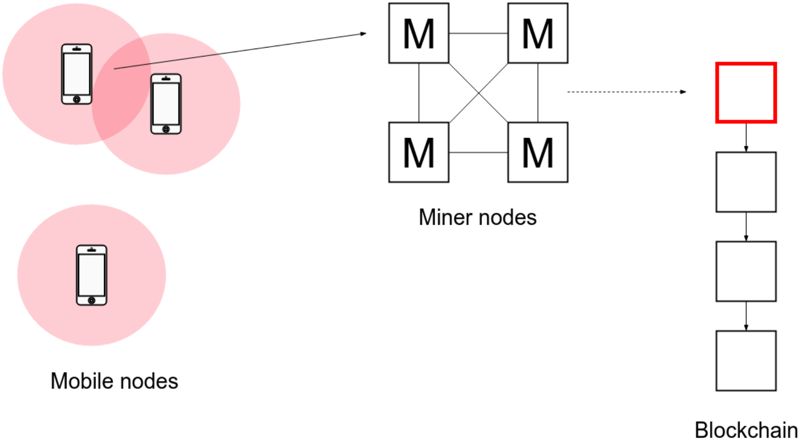
Mobile nodes

Miner nodes

Blockchain

Design

Overview



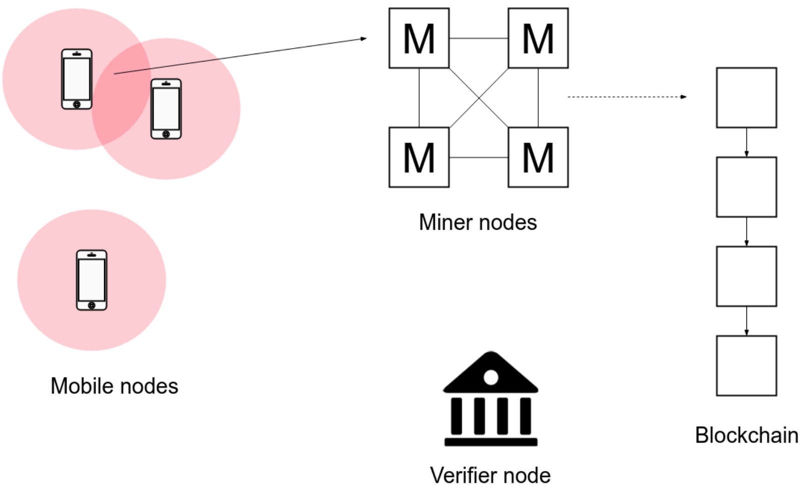
Mobile nodes

Miner nodes

Blockchain

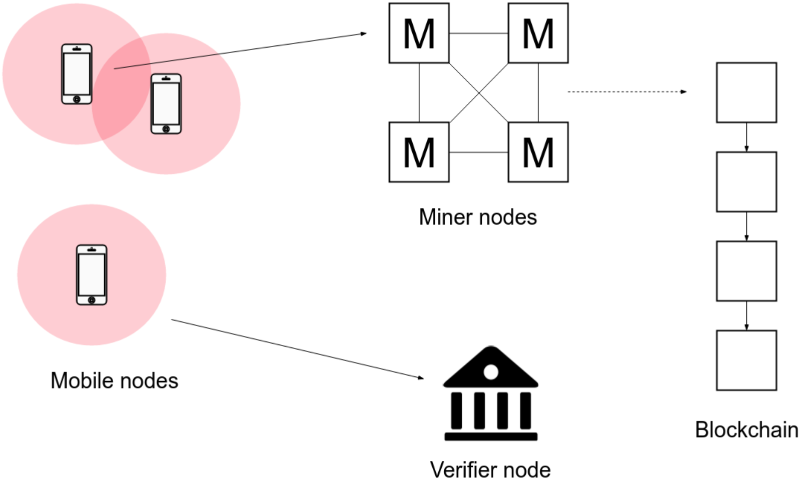
Design

Overview



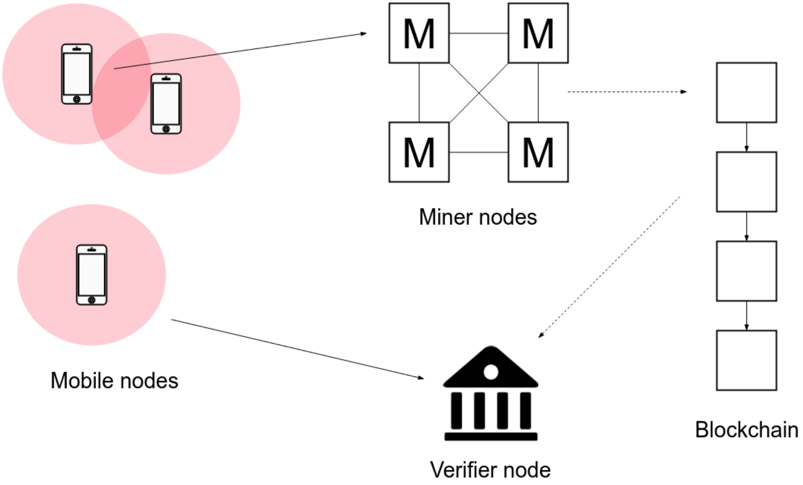
Design

Overview



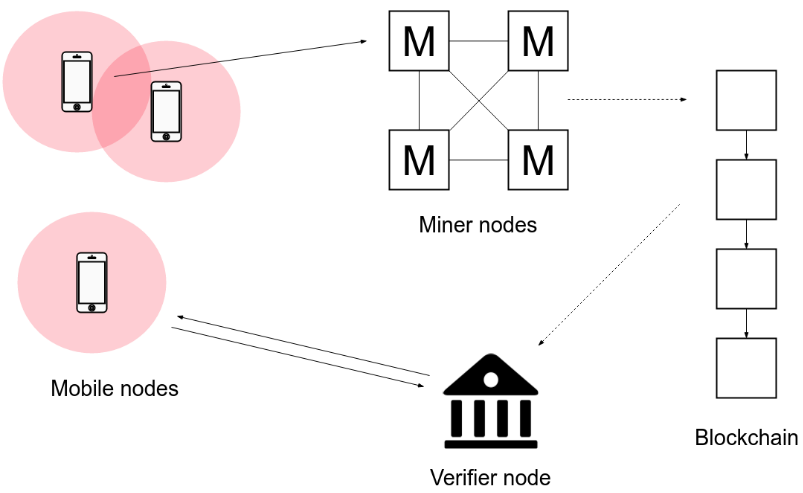
Design

Overview



Design

Overview



Problem

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

Goals:

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

Design

Identities

Used to **anonymously** identify a node in a transaction.

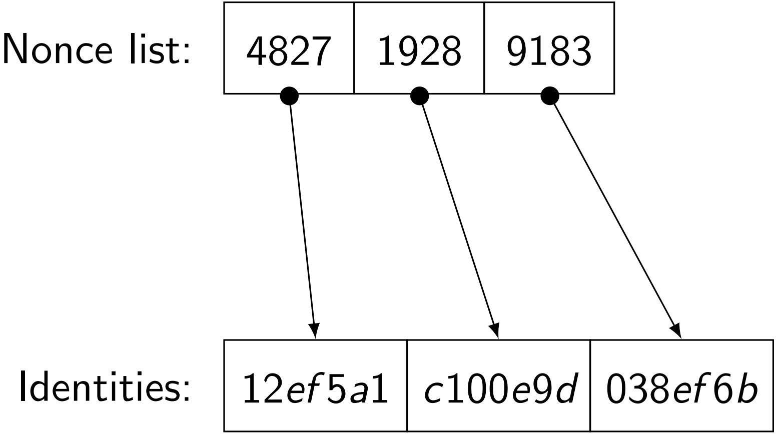
Every node generates a new identity for each transaction, making it untrackable.

Balancing goals:

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

Design

Identities: Nonce Lists

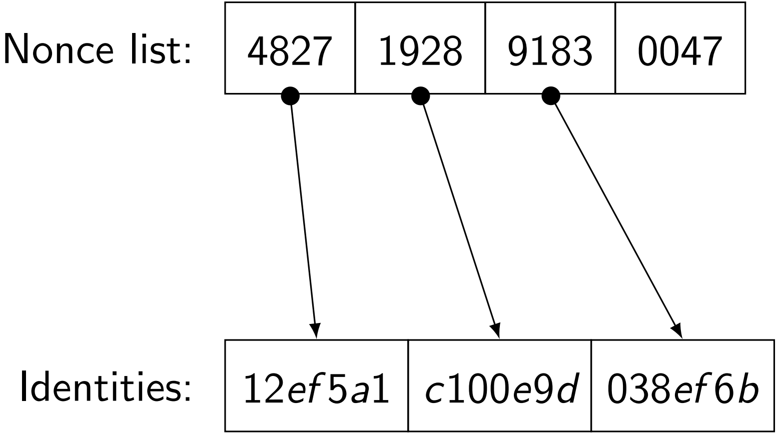


Nonce list: 4827 | 1928 | 9183

Identities: $12ef5a1$ | $c100e9d$ | $038ef6b$

Design

Identities: Nonce Lists

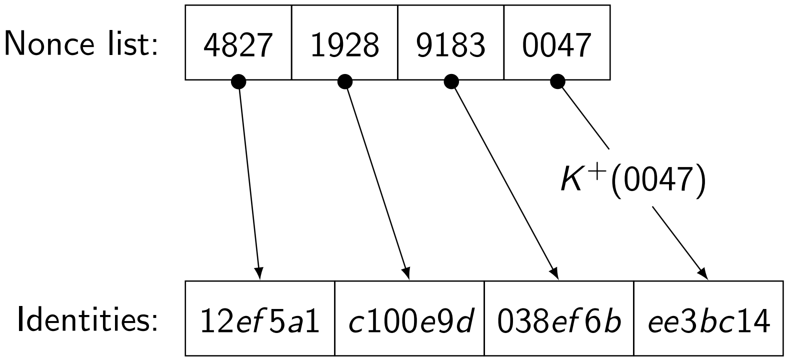


Nonce list: 4827 | 1928 | 9183 | 0047

Identities: $12ef5a1$ | $c100e9d$ | $038ef6b$

Design

Identities: Nonce Lists



Nonce list:	4827	1928	9183	0047
Identities:	$12ef5a1$	$c100e9d$	$038ef6b$	$ee3bc14$

$K^+(0047)$

Design

Identities: Duplication

Identity duplication unavoidable in a scalable decentralised system.

Design

Identities: Duplication

Identity duplication unavoidable in a scalable decentralised system.

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

Design

Identities: Duplication

Identity duplication unavoidable in a scalable decentralised system.

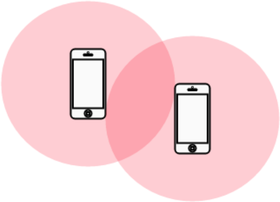
ID	Contents
...	
ffa0	
ffa1	
ffa2	T_{A4} , T_{C102}
ffa3	
ffa4	T_{B87}
...	

Design

Transactions

Transactions are created when two mobile nodes physically meet.

- Ad-hoc bluetooth connection between the nodes.



Design

Transactions

Node A will create the following transaction after meeting node B:

$$T_{An} = K_A(ts_A | loc_A | ID_{An} | KP_{Bm})$$

Design

Transactions

Node A will create the following transaction after meeting node B:

$$T_{An} = K_A(ts_A|loc_A|ID_{An}|KP_{Bm})$$

Design

Transactions: Key Packets

Key Packets provide a Verifier with a means of examining a mobile node's transactions.

Design

Transactions: Key Packets

Key Packets provide a Verifier with a means of examining a mobile node's transactions.

Two main properties:

- Allow a Verifier to build a tree of a mobile node's activity.
- Allow a mobile node to preserve control its own privacy.

Design

Transactions: Key Packets

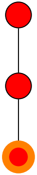
Key Packets provide a Verifier with a means of examining a mobile node's transactions.

Two main properties:

- Allow a Verifier to build a tree of a mobile node's activity.
- Allow a mobile node to preserve control its own privacy.

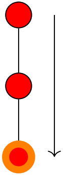
Design

Transactions: Key Packets - Verification



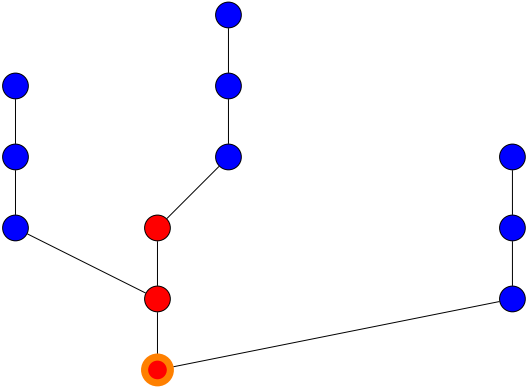
Design

Transactions: Key Packets - Verification



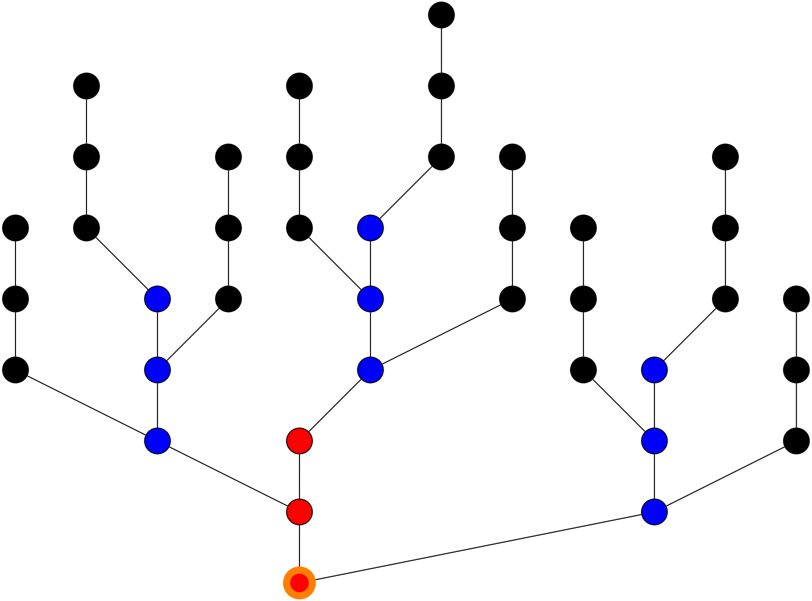
Design

Transactions: Key Packets - Verification



Design

Transactions: Key Packets - Verification



Problem

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

Goals:

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

Design

Transactions: Key Packets

Key Packets provide a Verifier with a means of examining a mobile node's transactions.

Two main properties:

- Allow a Verifier to build a graph of a mobile node's activity.
- Allow a mobile node to preserve control its own privacy.

Design

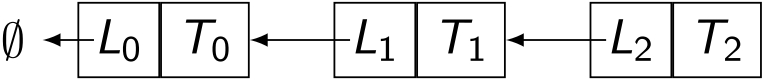
Transactions: Key Packets - Privacy

Published transactions split into two parts: Link and Transaction

Design

Transactions: Key Packets - Privacy

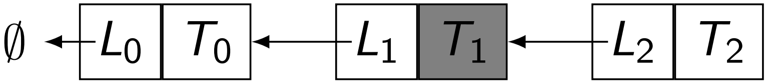
Published transactions split into two parts: Link and Transaction



Design

Transactions: Key Packets - Privacy

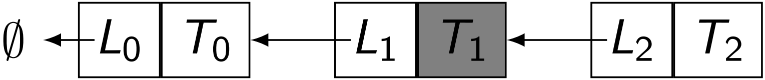
Published transactions split into two parts: Link and Transaction



Design

Transactions: Key Packets - Privacy

Published transactions split into two parts: Link and Transaction

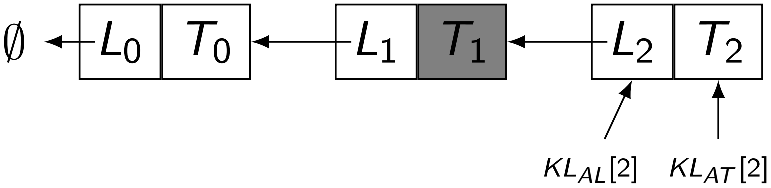


Two *Key Lists*: KL_{AT} and KL_{AL}.

Design

Transactions: Key Packets - Privacy

Published transactions split into two parts: Link and Transaction

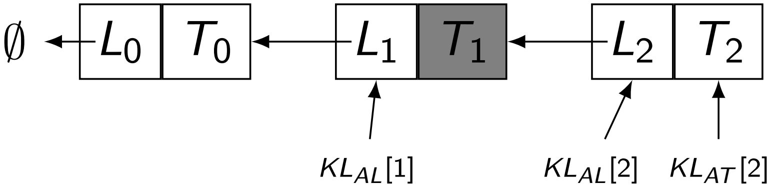


Two *Key Lists*: KL_{AT} and KL_{AL}.

Design

Transactions: Key Packets - Privacy

Published transactions split into two parts: Link and Transaction



Two *Key Lists*: KL_{AT} and KL_{AL}.

Design

Transactions

Node A will create the following transaction after meeting node B:

$$T_{An} = {\color{red}K_A}(ts_A|loc_A|ID_{An}|KP_{Bm})$$

Design

Transactions

Node A will create the following transaction after meeting node B:

$$T_{An} = KL_{AT}[n](ts_A | loc_A | ID_{An} | KP_{Bm})$$

Design

Transactions

Node A will create the following transaction after meeting node B:

$$T_{An} = KL_{AT}[n](ts_A|loc_A|ID_{An}|KP_{Bm})$$

Node A will then publish the following to the blockchain:

$$P_{An} = ID_{An}|KL_{AL}[n](ID_{An-1}|ts_A)|T_{An}$$

Design

Verification

Mobile node needs to provide Verifier node with:

- ID of most recent transaction.
- Key Packet for *n* most recent transactions.
- Nonce list for *n* most recent IDs.
- Public key.

Problem

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

Goals:

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

Evaluation

Case-based evaluation.

Evaluation

Case-based evaluation.

Two kinds of case-based evaluation:

- Desirable properties.
- Threats.

Evaluation

Desirable properties

OTIT defines 8 desirable properties of a location proof system:

- Chronological.
- Order-preserving.
- Verifiable.
- Tamper evident.
- Privacy preserved.
- Selective in-sequence privacy.
- Privacy protected chronology.
- Convenience and derivablilty.

Evaluation

Threats

A number of papers have gathered threats to evaluate their models against:

- Dishonest users.
- Malicious intruders.
- Curious users.
- Malicious applications.
- False timestamping.
- Implication.
- Proof switching.
- Relay attack.
- Eavesdroppers.
- Wormhole attacks.
- False presence.
- False assertion.
- Denial of presence.
- Denial of witness's presence.
- Privacy violation.
- ~~Weak identities.~~
- ~~Sybil attack.~~

Evaluation

Threats - Weak identities

I assume that private keys and nonce lists are never shared.

Evaluation

Threats - Sybil attack

No way of determining if two distinct location proof chains were created by two distinct mobile nodes.

Evaluation

Threats - Sybil attack

No way of determining if two distinct location proof chains were created by two distinct mobile nodes.

No provable decentralised solution to the Sybil attack (yet).

Evaluation

Threats - Sybil attack

No way of determining if two distinct location proof chains were created by two distinct mobile nodes.

No provable decentralised solution to the Sybil attack (yet).

Mitigations:

- Introduce identity creation penalty.
- Web of trust.
- Secret verification techniques.

Conclusion

Developed a privacy-protecting, decentralised location proof system.

Conclusion

Developed a privacy-protecting, decentralised location proof system.

Completed a case-based evaluation.

Conclusion

Developed a privacy-protecting, decentralised location proof system.

Completed a case-based evaluation.

Currently vulnerable to extremely targeted Sybil attacks.

Conclusion

Developed a privacy-protecting, decentralised location proof system.

Completed a case-based evaluation.

Currently vulnerable to extremely targeted Sybil attacks.

Resilient against every other known attack.

Conclusion

Developed a privacy-protecting, decentralised location proof system.

Completed a case-based evaluation.

Currently vulnerable to extremely targeted Sybil attacks.

Resilient against every other known attack.

- Sybil attack can be heavily mitigated against.

Conclusion

Developed a privacy-protecting, decentralised location proof system.

Completed a case-based evaluation.

Currently vulnerable to extremely targeted Sybil attacks.

Resilient against every other known attack.

- Sybil attack can be heavily mitigated against.
- Decentralised solution to Sybil attack may be found in future.

Future work

Further study into advanced Verification techniques.

Future work

Further study into advanced Verification techniques.

Investigate the impact that witholding certain private transactions has on verifiability.

Future work

Further study into advanced Verification techniques.

Investigate the impact that witholding certain private transactions has on verifiability.

Build it!