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 M
- Verifier node 🏛

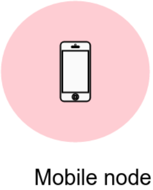
Design

Overview

Mobile node

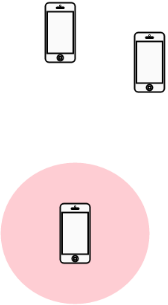
Design

Overview



Design

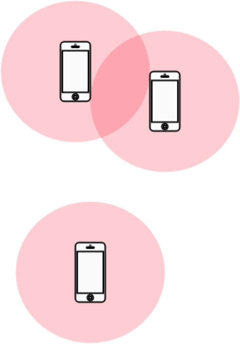
Overview



Mobile nodes

Design

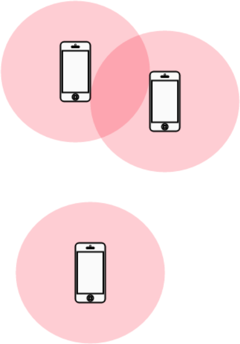
Overview



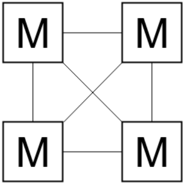
Mobile nodes

Design

Overview



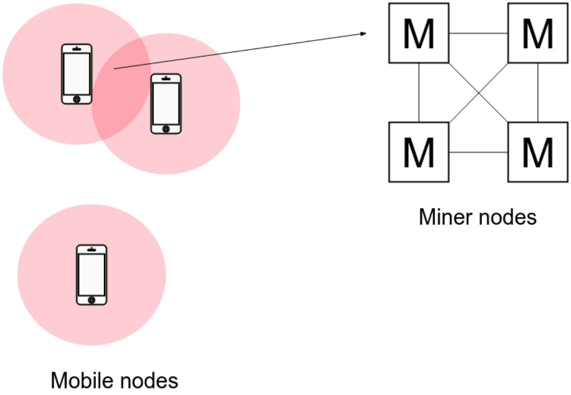
Mobile nodes



Miner nodes

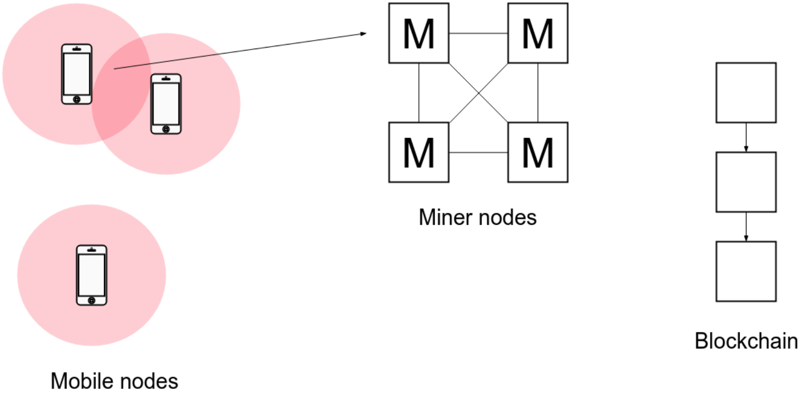
Design

Overview



Design

Overview



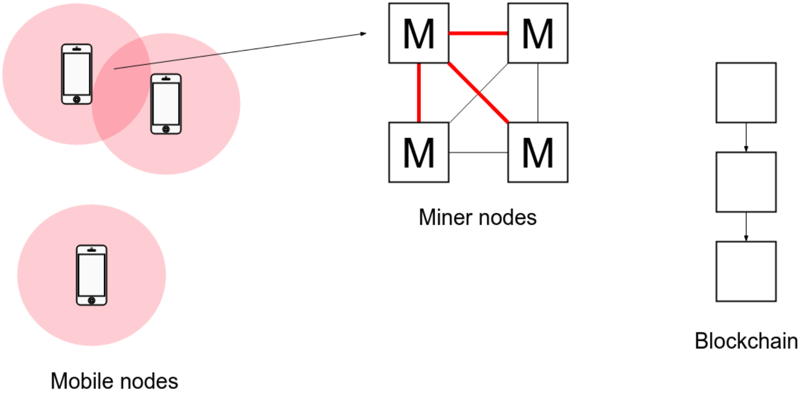
Miner nodes

Blockchain

Mobile nodes

Design

Overview



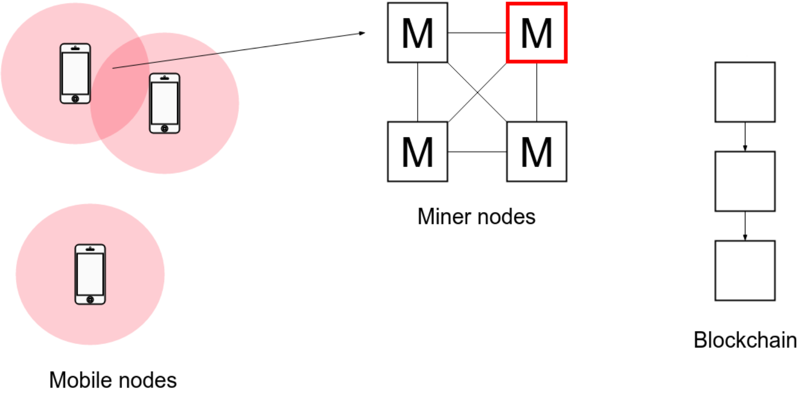
Mobile nodes

Miner nodes

Blockchain

Design

Overview



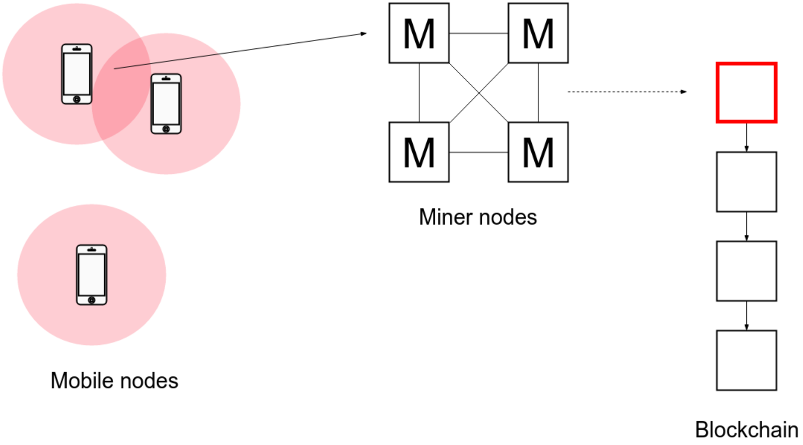
Miner nodes

Blockchain

Mobile nodes

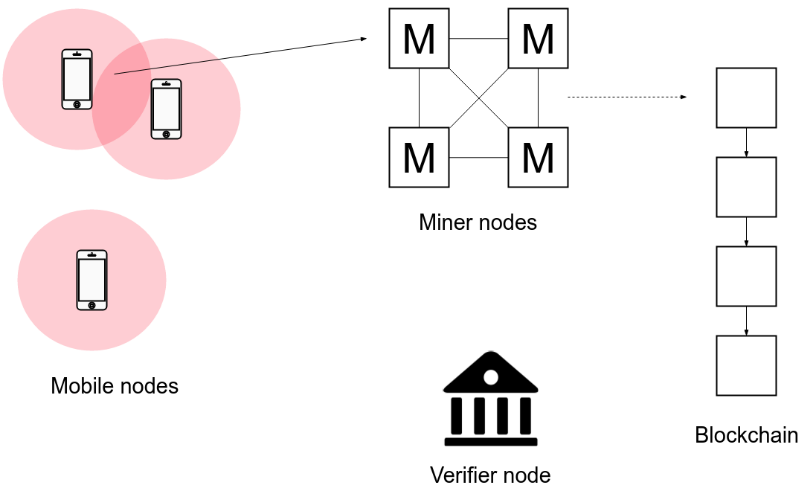
Design

Overview



Design

Overview



Miner nodes

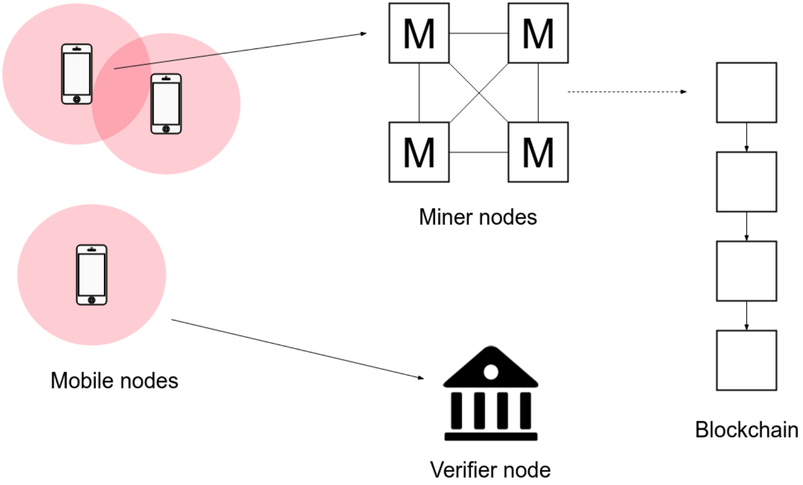
Mobile nodes

Blockchain

Verifier node

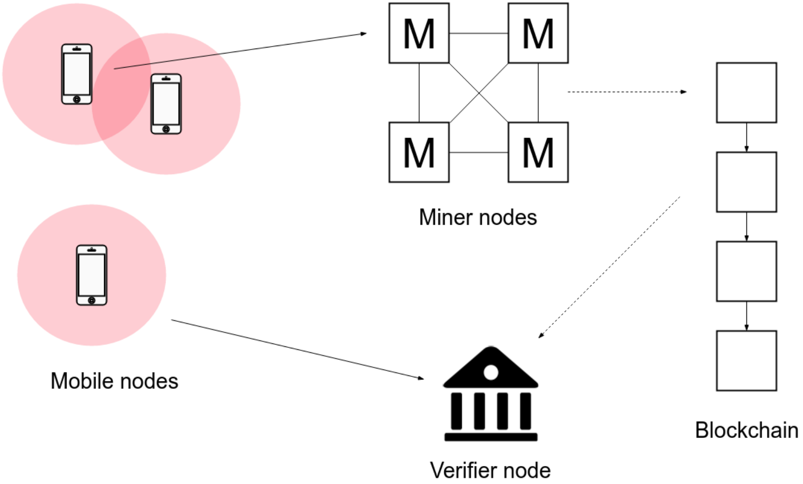
Design

Overview



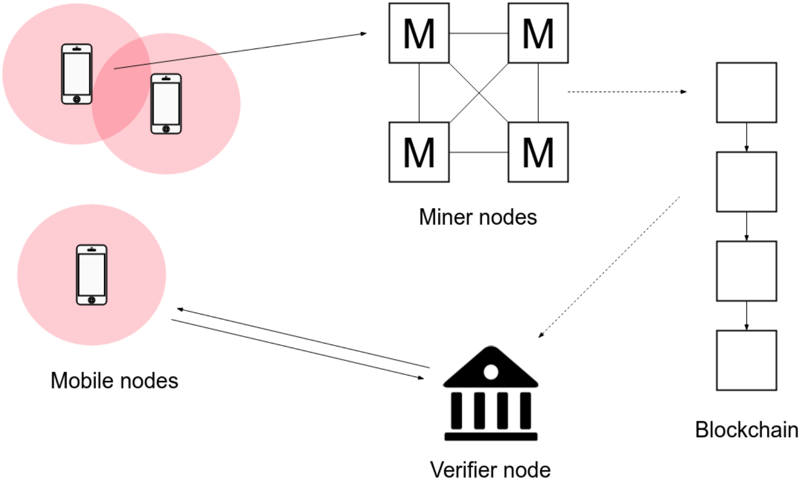
Design

Overview



Design

Overview



Design

Identities

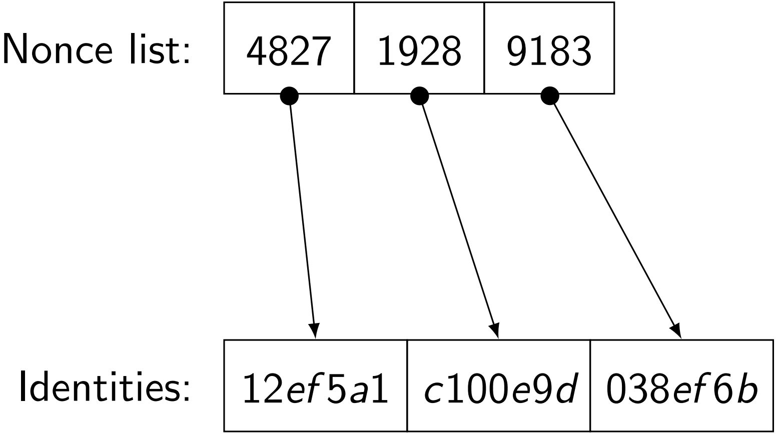
Used to anonymously identify a node in a transaction.

Balancing goals:

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

Design

Identities: Nonce Lists

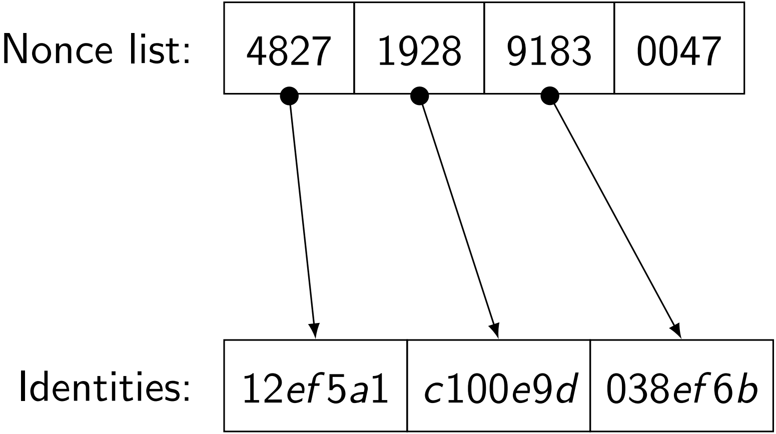


Nonce list: 4827 1928 9183

Identities: 12ef5a1 c100e9d 038ef6b

Design

Identities: Nonce Lists

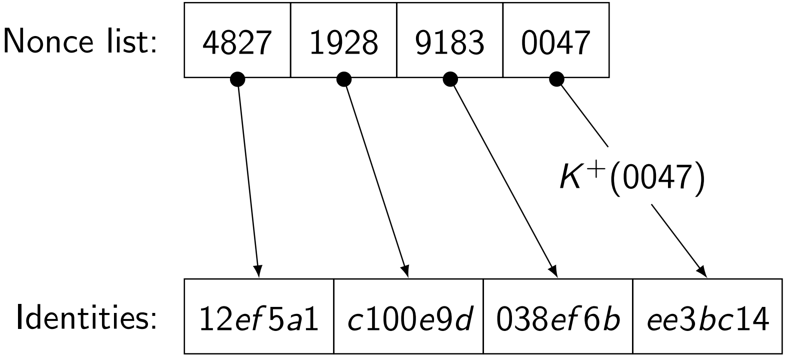


Nonce list: 4827 | 1928 | 9183 | 0047

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

Design

Identities: Nonce Lists



Nonce list: 4827 | 1928 | 9183 | 0047

$K^+(0047)$

Identities: $12ef5a1$ | $c100e9d$ | $038ef6b$ | $ee3bc14$

Design

Identities: Duplication

Identity duplication is unavoidable in a decentralised system.

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.

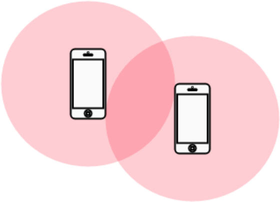
ID	**Contents**
...	
ffa0	
ffa1	
ffa2	T_{A4} , T_{C102}
ffa3	
ffa4	T_{B87}
...	

Design

Transactions

Transactions are created when two mobile nodes physically meet.

- Ad-hoc bluetooth connection between the nodes.



Design

Transactions II

Node A

Node B

Design

Transactions II

n

Node A

m

Node B

Design

Transactions II

n

Node A

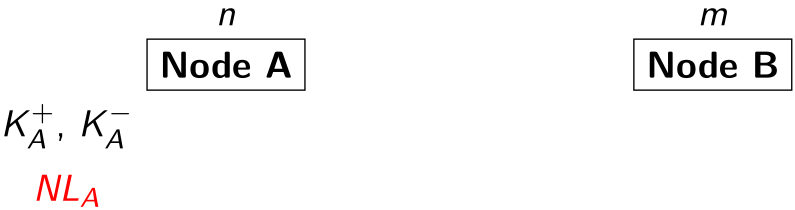
m

Node B

K_A^+, K_A^-

Design

Transactions II



n

Node A

m

Node B

K_A^+, K_A^-

NL_A

Design

Transactions II

n

Node A

m

Node B

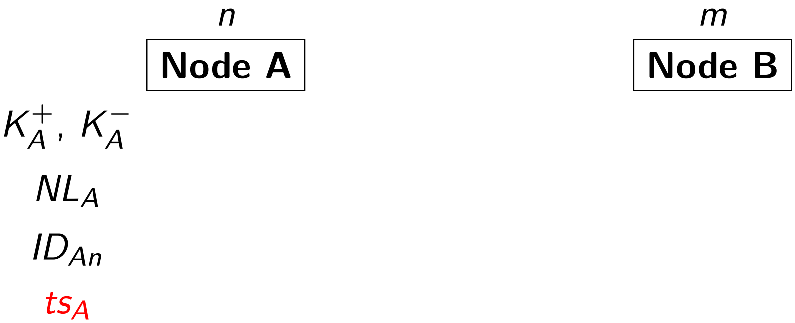
$K_A^+,\ K_A^-$

NL_A

$ID_{An} = K_A^+(NL_A[n])$

Design

Transactions II



n

Node A

m

Node B

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

Design

Transactions II

n

Node A

m

Node B

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

loc_A

Design

Transactions II

n

Node A

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

loc_A

m

Node B

K_B^+, K_B^-

NL_B

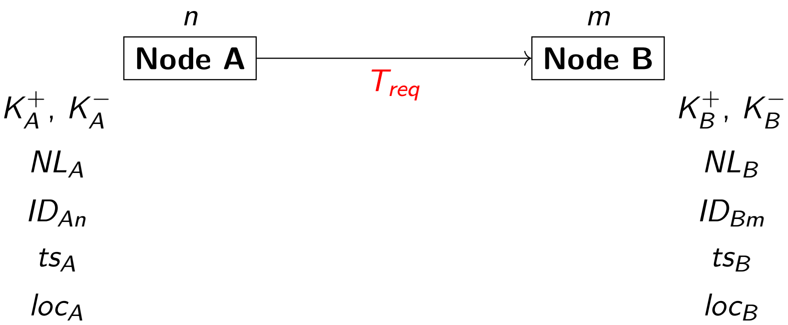
ID_{Bm}

ts_B

loc_B

Design

Transactions II



n

Node A

m

Node B

T_{req}

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

loc_A

K_B^+, K_B^-

NL_B

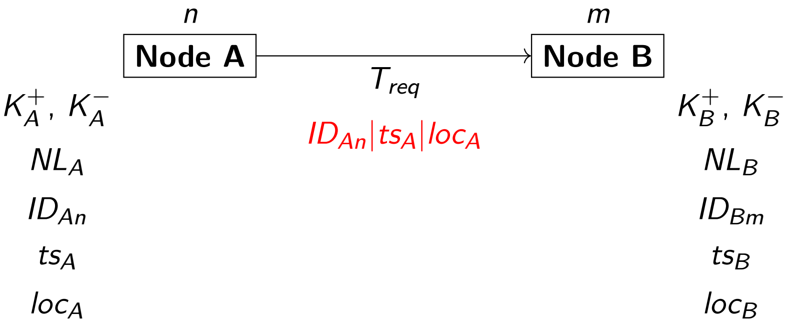
ID_{Bm}

ts_B

loc_B

Design

Transactions II



n

Node A

m

Node B

T_{req}

$ID_{An}|ts_A|loc_A$

$K_A^+,\ K_A^-$

NL_A

ID_{An}

ts_A

loc_A

$K_B^+,\ K_B^-$

NL_B

ID_{Bm}

ts_B

loc_B

Design

Transactions II

n

Node A

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

loc_A

m

Node B

K_B^+, K_B^-

NL_B

ID_{Bm}

ts_B

loc_B

ID_{An}

ts_A

loc_A

Design

Transactions II

n

Node A

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

loc_A

m

Node B

K_B^+, K_B^-

NL_B

ID_{Bm}

ts_B

loc_B

ID_{An}

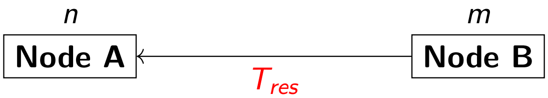
ts_A

loc_A

$verify\ |ts_A - ts_B| < \epsilon_{ts}$
$\&\&|loc_A - loc_B| < \epsilon_{loc}$

Design

Transactions II



n

Node A

m

Node B

T_{res}

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

loc_A

K_B^+, K_B^-

NL_B

ID_{Bm}

ts_B

loc_B

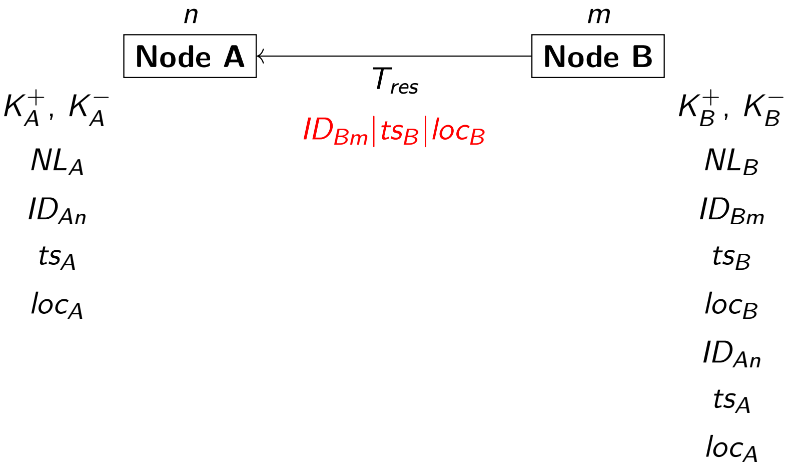
ID_{An}

ts_A

loc_A

Design

Transactions II



n

Node A

m

Node B

T_{res}

$ID_{Bm}|ts_B|loc_B$

K_A^+, K_A^-

NL_A

ID_{An}

ts_A

loc_A

K_B^+, K_B^-

NL_B

ID_{Bm}

ts_B

loc_B

ID_{An}

ts_A

loc_A

Design

Transactions II

n	m
Node A	**Node B**
K_A^+, K_A^-	K_B^+, K_B^-
NL_A	NL_B
ID_{An}	ID_{Bm}
ts_A	ts_B
loc_A	loc_B
ID_{Bm}	ID_{An}
ts_B	ts_A
loc_B	loc_A

Design

Transactions II

n		m
Node A		**Node B**
K_A^+, K_A^-		K_B^+, K_B^-
NL_A		NL_B
ID_{An}		ID_{Bm}
ts_A		ts_B
loc_A	$verify\ \lvert ts_A - ts_B \rvert < \epsilon_{ts}$	loc_B
ID_{Bm}	$\&\&\lvert loc_A - loc_B \rvert < \epsilon_{loc}$	ID_{An}
ts_B		ts_A
loc_B		loc_A