Course#236349 - Project in Computer Security

Mentor : Lionel Wolberger lionel@platin.io

Proof of Location for Blockchain

General Description

Location information, particularly about people, is extremely useful to modern industry. Businesses use it to analyze trends and make strategy. Individuals use it to navigate using Waze, find stores via local search, or have packages tracked automatically. Our smartphones and other personal devices (such as iOT, fitness sensors, smart watches) report our location better than any government spy agency in history.

Yet individuals need the right to conceal information about their position - sometimes called “spatial” or “locational privacy” – since location information is easily abused for example to rob your home when you are away, limit employee freedom, charge higher prices via targeted ads, and so on. Services that use location data have a similar right to privacy protection: a company should be able to either track its activities in an area, or subscribe to information about locations, without competitors knowing.

Protecting privacy is even more challenging in blockchain technologies than in web services, since transaction details are stored forever in a permanent, indelible, distributed ledger. **Bitcoin and Ethereum** have caused a revolution in cryptocurrency and distributed processing of contracts. However, location information has been difficult to transact on public blockchain ledgers, due to privacy issues. This project seeks to propose solutions to those issues.

Project Details

We explore a cryptocurrency “Platin” that pays a reward if a user can claim to be in a location. In the basic use case a “sender” offers to pay an individual price “P” of the cryptocurrency Platin (PTN) to a “receiver” when that receiver proves they are at a specified location. This basic scenario can be abstracted to cover many other use cases in future, from supply chain to iOT.

We start with a completely transparent scenario. Each side sends the information so that it can be inspected by anyone. Sending data in this way, while simple, has no privacy at all. We then improve this by implementing privacy using cryptographic protocols.

Goals

- Learn about sending and receiving cryptocurreny e.g. bitcoin
- Learn about location data and privacy
- Learn and compare various zero knowledge cryptographic protocols

Project Steps

The following steps are proposed. The scenario is described in more detail below.

MAP SERVICE

- Select or create a map service.
- Can store and display locations L. Look at Google Places API, Apple Core location, Mozilla Geolocation. Make sure that the location is expressed in a standardized way: see schema.org, ISO 6709.
- Can communicate with other parties to facilitate map/location activities

SENDER & RECEIVER APPLICATIONS

- Create applications to send and receive cryptocurrency, based on location requirements. This app may be part of an existing cryptocurrency wallet.
- SENDER stores a location L and a general margin of error M(L) that contains L. Can communicate with the other parties to list the location on the MAP SERVICE, and if a RECEIVER claims to be in M(L), make a payment
- RECEIVER stores a location L'. Can do the proper communications so that, if L' is in a location where a sender is sending money, the RECEIVER can make a claim and collect the money
- Both apps implement cryptography to avoid revealing private information

EVALUATOR SERVICE

- Create a software application to act as an intermediary in order to protect privacy.
- The EVALUATOR can be considered like a smart contract processor, or a trusted third party. It stores cryptocurrency offers and can evaluate claims to take currency (based on location data). It also can perform zero knowledge protocols to evaluate contracts without being aware of private details.

Scenario Flow Details

Transparent Scenario

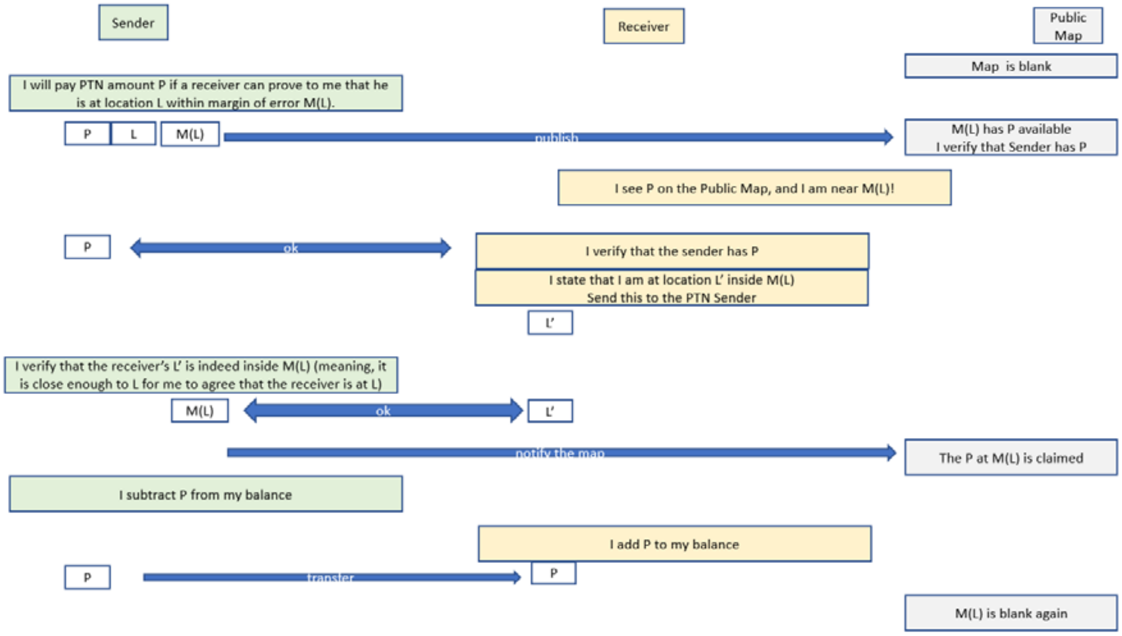
In this beginning scenario, sender and receiver each have full knowledge of what the other is doing.

There is no locational privacy.

The following describes flow shown in Diagram A:

1. A sender signs a simple contract: “I will pay PTN amount P if a receiver can prove to me that he is at location L within margin of error M(L).” M(L) could for example be a circle of radius R around location L, so any point within one meter of L is contained in M(L).
2. The sender contacts a public map service.
3. The map service verifies that the sender does in fact own PTN amount P.
4. The map agrees to accept the notification and display the PTN on the location. It also offers the node address of the publisher (the sender) for anyone to contact the sender.
5. The public map displays that area M(L) has PTN P available, from the sender.
6. Receiver accesses the map service. Receiver sees PTN amount P on the public map.
7. The receiver sees that he is in or near M(L) and is a candidate to claim the PTN amount.
8. The receiver states to the sender that he is at location L’ (L’ being inside M(L)).
9. The sender validates that the receiver is in fact inside M(L). (L’ is inside M(L)).
10. Sender agrees as originally committed, to pay / release the PTN to the receiver, since the receiver has satisfied the contract.
11. Sender transfers PTN P from to the receiver’s address —> this transfer is committed to the public ledger (blockchain).
12. The public map is made aware of this transaction and clears PTN amount from L.

Diagram A
Transparent Scenario DRAFT


Sender
Receiver
Public Map
Map is blank
I will pay PTN amount P if a receiver can prove to me that he is at location L within margin of error M(L).
P
L
M(L)
publish
M(L) has P available
I verify that Sender has P
I see P on the Public Map, and I am near M(L)!
P
ok
I verify that the sender has P
I state that I am at location L’ inside M(L)
Send this to the PTN Sender
L’
I verify that the receiver’s L’ is indeed inside M(L) (meaning, it is close enough to L for me to agree that the receiver is at L)
M(L)
ok
L’
notify the map
The P at M(L) is claimed
I subtract P from my balance
I add P to my balance
P
transfer
P
M(L) is blank again

Homeomorphic Hiding Scenario

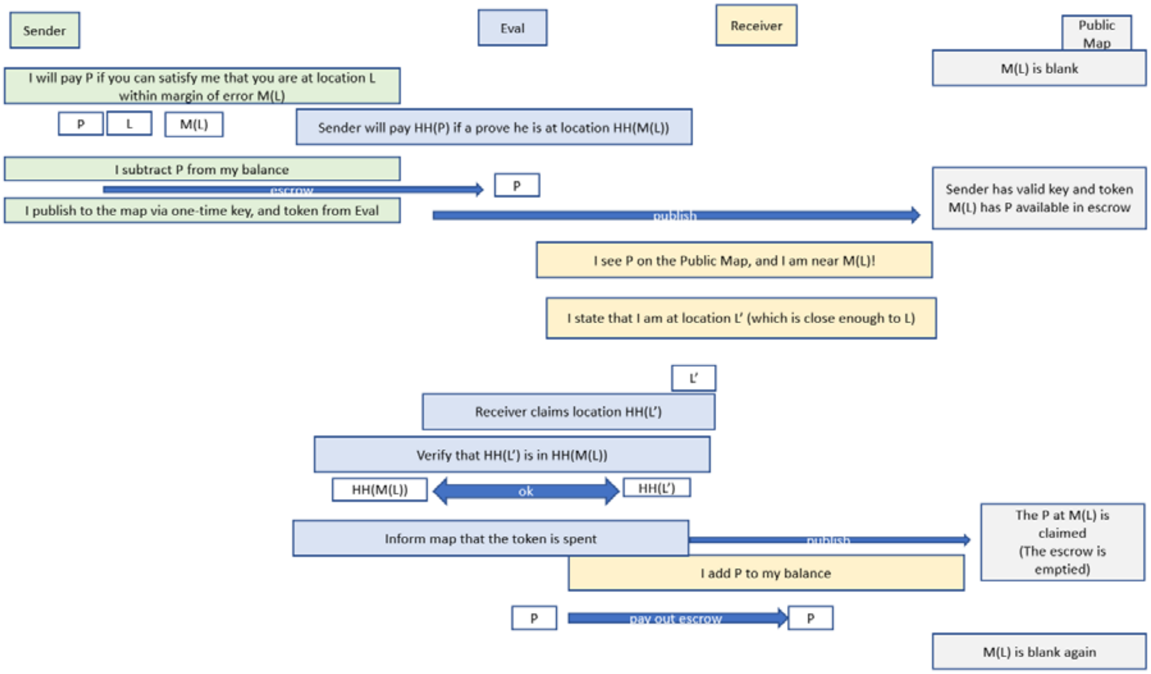
The above transparent scenario violates the location privacy of both parties. To begin to protect the privacy of both sender and receiver, a new service is added, called an evaluator. The evaluator protects each user—sender and receiver—from having any direct knowledge of the other, by harnessing cryptographic zero knowledge protocols.

The method of this hiding is called “homeomorphic hiding (HH), a general umbrella term that does not refer to any specific algorithm.

The following describes flow shown in Diagram B:

1. A sender signs a simple contract: “I will pay PTN amount P if a receiver can prove to me that he is at location L within margin of error M(L).” M(L) could for example be a circle of radius R around location L, so any point within one meter of L is contained in M(L).
2. The sender publishes this contract to the evaluator. Any details considered private are hidden using homeomorphic hiding (HH).
3. The sender pays the evaluator amount PTN P. This functions as an escrow deposit; the evaluator will pay this P to a valid receiver when such receiver offers a valid claim. In other words, The evaluator knows that the sender’s node S will pay HH(P) if a receiver node R can prove that they’re at location HH(M(L)).
4. The evaluator returns to the sender a token expressing that the claim is registered and valid.
5. The sender publishes to the map his announcement that he will pay PTN P to anyone in area M(L) and supplies the token from the evaluator.
6. The map validates the token, and publishes the information on its public map.
7. Receiver sees PTN amount P on the public map.
8. The receiver also sees that he is in or near M(L).
9. The receiver sends to the evaluator a claim that he is at HH(L’).
10. The evaluator now applies relevant methods (aka, zero knowledge) to compare the HH(M(L)) to HH(L’).
11. The evaluator finds that they match.
12. The evaluator transfers PTN P to the receiver’s address R.
13. The evaluator sends an updated token to the public map. By matching the token to the previous token, the public map can update its information and show that P at M(L) is no longer available.

Diagram B
Homeomorphic Hiding Scenario DRAFT


Sender
Eval
Receiver
Public Map
M(L) is blank
I will pay P if you can satisfy me that you are at location L within margin of error M(L)
P
L
M(L)
Sender will pay HH(P) if a prove he is at location HH(M(L))
I subtract P from my balance
escrow
P
I publish to the map via one-time key, and token from Eval
publish
Sender has valid key and token M(L) has P available in escrow
I see P on the Public Map, and I am near M(L)!
I state that I am at location L’ (which is close enough to L)
L’
Receiver claims location HH(L’)
Verify that HH(L’) is in HH(M(L))
HH(M(L))
ok
HH(L’)
Inform map that the token is spent
publish
The P at M(L) is claimed (The escrow is emptied)
I add P to my balance
P
pay out escrow
P
M(L) is blank again

Mentors

Lionel Wolberger, Ph.D. With over 15 years of extensive experience in the creation and deployment of new ideas and true "full stack" experience on mobile, PC, web, and cloud in everything from games to e-commerce, Lionel is also a world-class expert in privacy, video technology and security with experience in multiple companies as well as serving to create standards in W3C and Oasis.

As a leader of new technologies deployment charged with transforming and deploying cutting edge services, Lionel conceived, implemented and led engineering teams to create, modify and deliver demos, prototypes and products such as Cisco DRM, eBooks, Interactive Television and VideoGuard Everywhere. Services enabled by Lionel and his teams are used by tens of millions of people on almost every continent (Cox Cable, News America Marketing, European Broadcasters, DirecTV). The DevOps and CI/CD Agile transformation that he helped lead changed how Cisco delivered its flagship $500M revenue product to enterprises such as AT&T and Vodafone.