Infineon Hackathon 2019

notarization and proof for geo based games

Christian Baumann – baumann.at

The idea

- Infineon: Blockchain Security 2Go starter kit
  - „Bringing more security to blockchain applications“

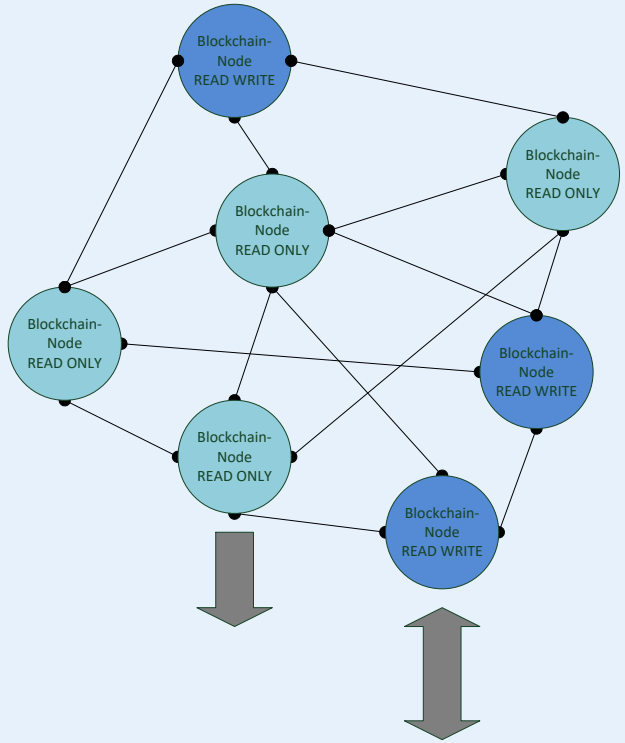
- Me: Use it to …
  - proof situations in geo based games (e.g. geocaching)
  - and notarize all information in a blockchain application

  - => physical logbook PLUS Chipcard


Official Logbook
GEOCACHING.COM
NAME:
PHONE:
EMAIL:
WAYPOINT:
infineon

Why blockchain?

- Key facts
  - decentralization
    - no trusted third party necessary
    - resilience: network and databases cannot be desctructed
  - transparency
    - “single truth” for all participants
  - immutability
    - data can only be appended …
    - … never changed or deleted

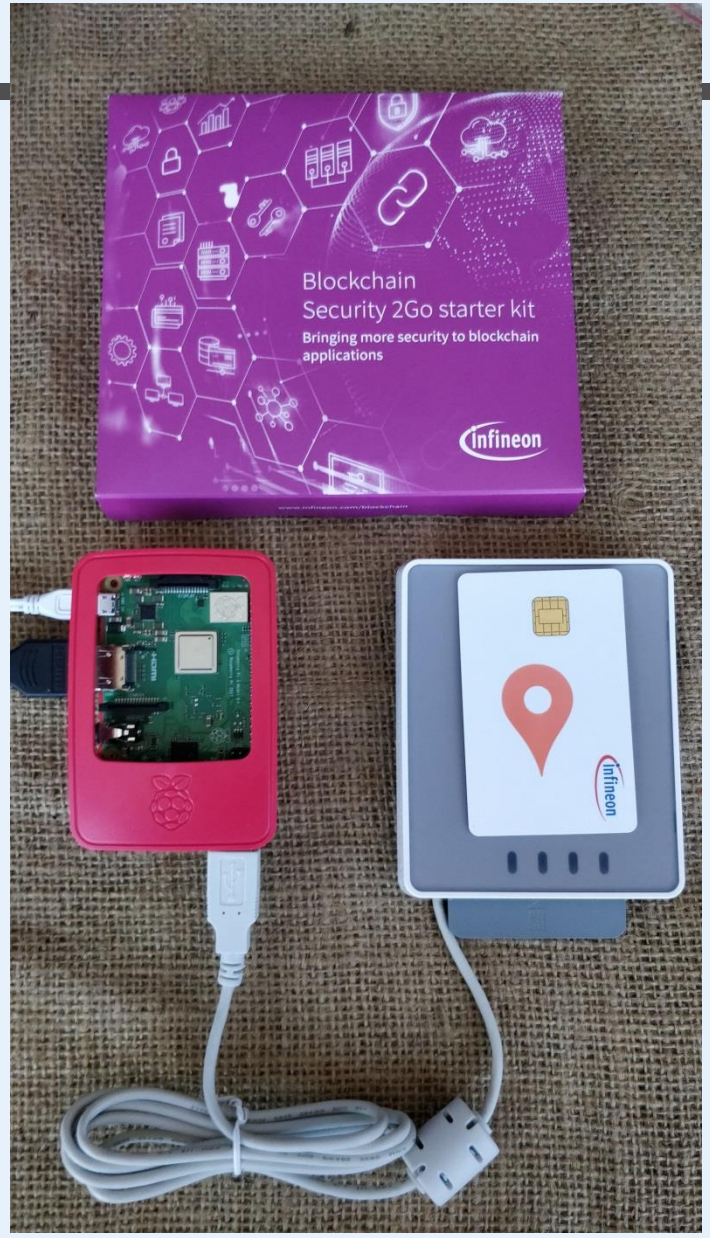


The process (overview)

- Step 0: prepare card
- Step 1: „check in“ into blockchain
  - … riddle is solved …
  - … location is visited …
  - … container (with card) is found!
- Step 2: register proof for „found it“ on the blockchain

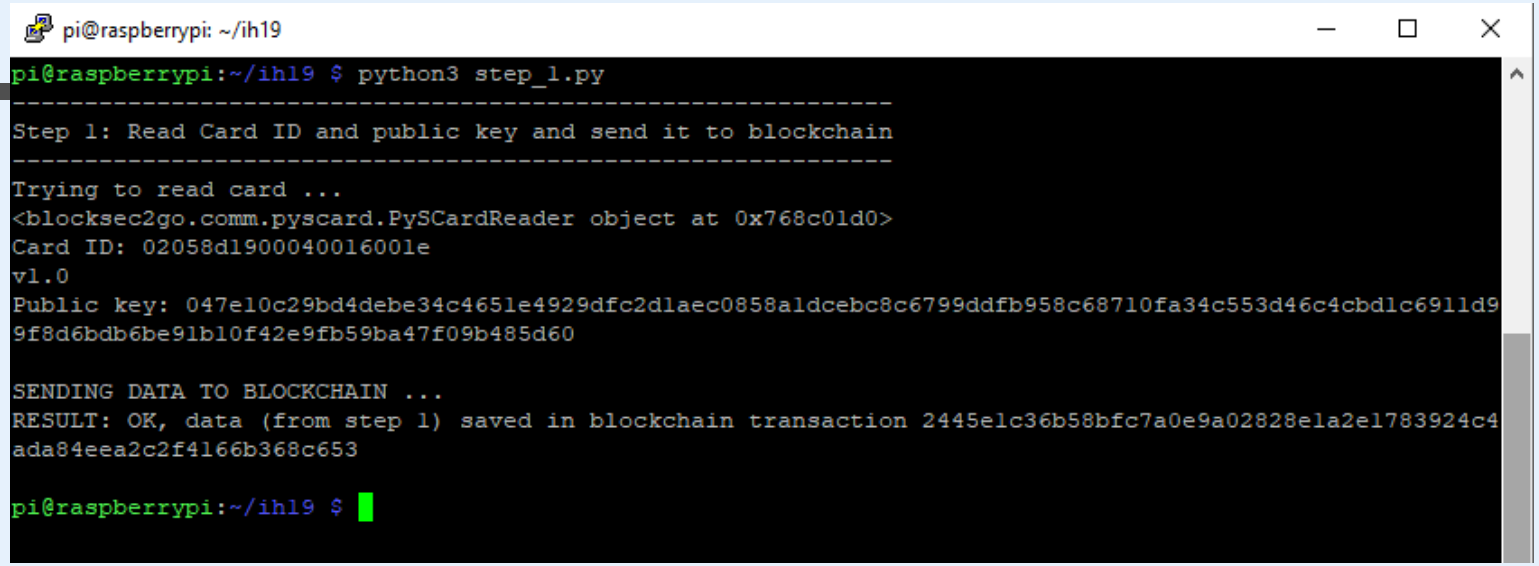
The setup

- Security 2Go starter kit
- Raspberry-Pi (2 apps)
  - Chipcard reader
  - => Mobile App (Android, iOS)
- Blockchain
  - E.g. Multichain
  - Rest-API
  - Explorer
- WebGUI



Step 0: prepare card

- generate keypair
- read public key & card id
- transmit this data to the blockchain application
- => the card is „known“

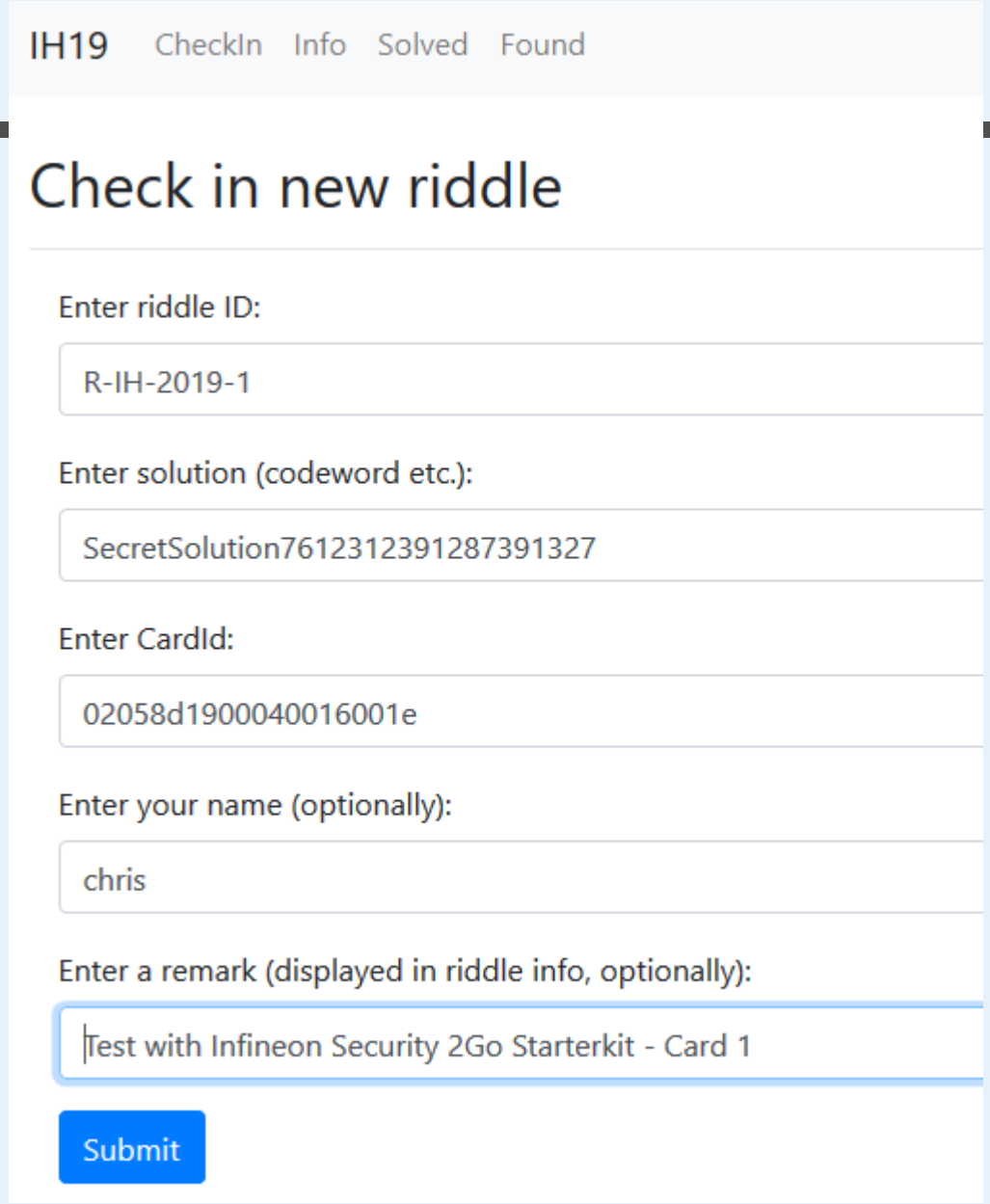


Stream: bs2go – 36 of 36 items

Publishers	1JQhLuexFQjDAwxtnRAnV1m3jkNbakNsjNLJnz
Key 0	02058d1900040016001e
JSON data	{ "Card": "02058d1900040016001e", "PubKey": "047e10c29bd4debe34c4651e4929dfc2d1aec0858a1dce" }
Added	2019-03-26 09:36:06 GMT (confirmed)
Data location	on-chain, available

Step 1: „Check In“

- Collect Data
  - ID
  - Solution
  - Name
  - Remark
  - …
  - CardID
- Save to blockchain



Step 1: „Check In“ - Information

Datasheet for riddle R-IH-2019-1

26.03.2019 10:43:43

Lorem ipsum ...

Riddle ID	R-IH-2019-1
Owner	chris
Remark	Test with Infineon Security 2Go Starterkit - Card 1
Checked in	2019-03-26T10:43:35+01:00
Solution	SecretSolution7612312391287391327
Find-Code	f775e5080c534c297f856eb0434b56e8
Card-Id	02058d1900040016001e

Open the following QR-Code or link to get current info about the riddle.

Check server address when opening with a QR-code reader!
https://test.baumann.at/dev9/ih19/?page=info&rid=R-IH-2019-1

IH19 CheckIn Info Solved Found

Info about riddle

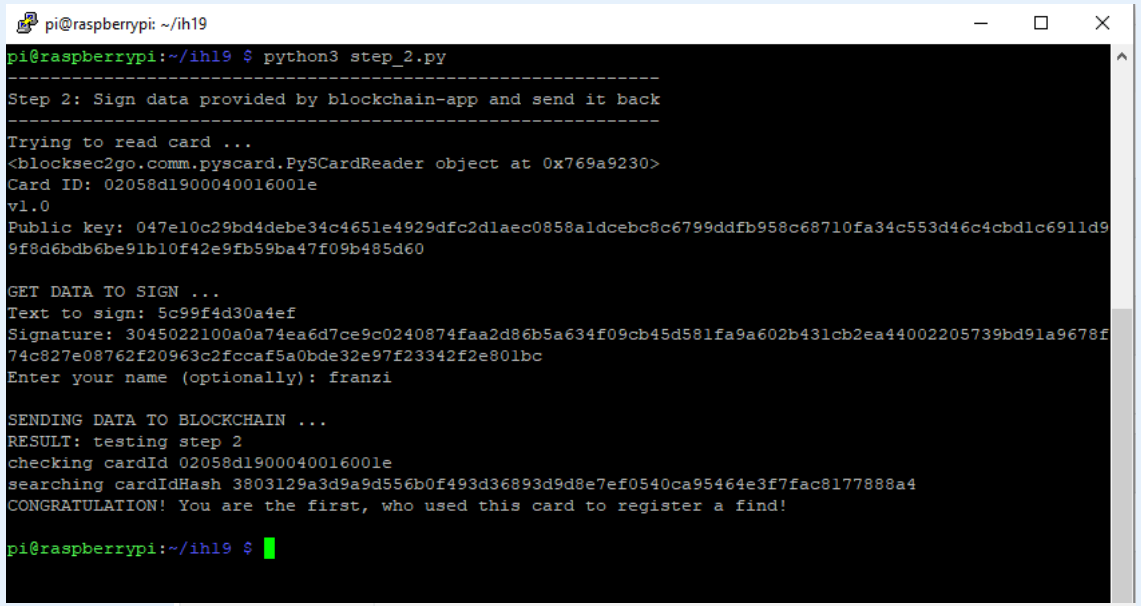
Riddle	R-IH-2019-1
Owner	chris
Remark	Test with Infineon Security 2Go Starterkit - Card 1
CardId Hash	3803129a3d9a9d556b0f493d36893d9d8e7ef0540ca95464e3f7fac8177888a4

Event	checkedin
By	chris
TimeStamp	2019-03-26T10:43:35+01:00
Transaction	b40af056d547ff33a58f44edb417fefb6f7861b80f855a235a4f62d6631f30d8
BlockHash	008a6bd76e66c1676c4d5876abcef5ec60c5bc4d3d5cfc44e69cd3fab1e19a77
BlockTime	2019-03-26T10:43:38+01:00

Generate a datasheet for your records and generate a codesheet to put into the geocache for the first finder.
When you are done, you can clear the session data from your browser.

Step 2: Register „found it“ on the blockchain

- Read card (with mobile App)
- Server sends token to sign („challenge“)
- Digital signature is created …
- … sent back to the server
- Everything is stored in the blockchain



BlockTime	2019-03-26T10:43:38+01:00

Event	card
By	franzi
TimeStamp	2019-03-26T10:46:07+01:00
Transaction	e2db0c04220df66bf54da5fc48cb9384249463c48c344944fbfed06390da1492
BlockHash	000a7fa14ac6f81b8d52e486e0bce384ed1f5829fdeefb5f11ac0410084e7d91
BlockTime	2019-03-26T10:46:25+01:00

Step 2: Register „found it“ on the blockchain

- „FTF-certificate“ can be issued
- Further readings of the card show warnings

Congratulations! You seem to be the first to have found this codesheet, belonging to the following riddle:

Riddle ID	R-IH-2019-1
Owner	chris
Remark	Test with Infineon Security 2Go Starterkit - Card 1
Checked in	2019-03-26T10:43:35+01:00
Find-Code	f775e5080c534c297f856eb0434b56e8

Check server address wh
https://test.baumann.at/de

```
pi@raspberrypi: ~/ih19
pi@raspberrypi:~/ih19 $ python3 step_2.py
------------------------------------------------------------
Step 2: Sign data provided by blockchain-app and send it back
------------------------------------------------------------
Trying to read card ...
<blocksec2go.comm.pyscard.PySCardReader object at 0x768d7230>
Card ID: 02058d1900040016001e
v1.0
Public key: 047e10c29bd4debe34c4651e4929dfc2d1aec0858a1dcebc8c6799ddfb958c68710fa34c553d46c4cbd1c6911d9
9f8d6bdb6be91b10f42e9fb59ba47f09b485d60

GET DATA TO SIGN ...
Text to sign: 5c99f53a6ae9f
Signature: 304402207306ac913598ff6e28595fac68e53669ec6e19cb36fc0e2a9ee6a4271459df050220410eccd934599ad6
b23641b031e0fdddb77d748bbc49e2c6b4d88fe0beadbcf9
Enter your name (optionally):

SENDING DATA TO BLOCKCHAIN ...
RESULT: testing step 2
checking cardId 02058d1900040016001e
searching cardIdHash 3803129a3d9a9d556b0f493d36893d9d8e7ef0540ca95464e3f7fac8177888a4
Sorry, this card was ALREADY USED to register the found.

pi@raspberrypi:~/ih19 $
```

Further ideas

- Additional „monetary motivation“
  - Bitcoin or Ethereum on card
  - PIN to unlock the card = solution of the riddle
- Adoption of the concept for different other games or similar usecases
- …

Contact

DI Dr. Christian Baumann

+43 664 4324243

c.baumann@baumann.at

https://www4.baumann.at