
Infineon Hackathon Villach 2019



blockchain security for (geo based) games

Christian Baumann – baumann.at

Content

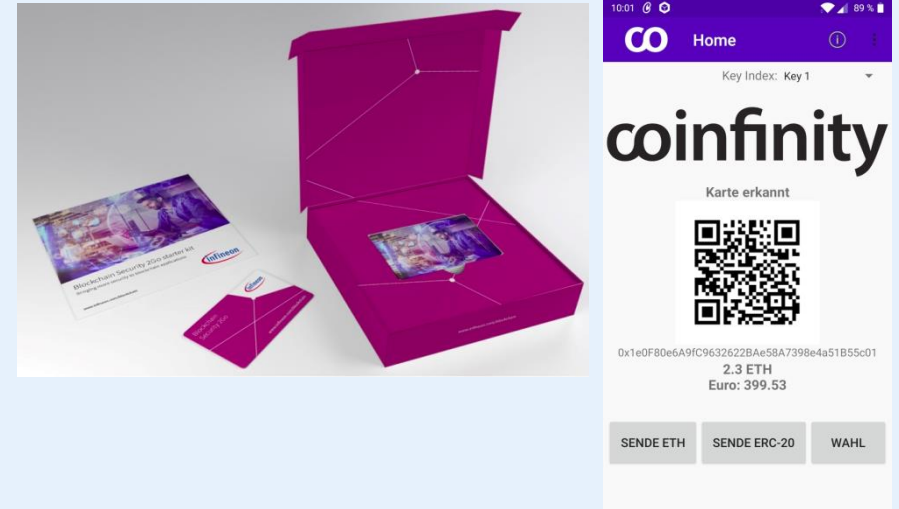
- Team
- Idea (problem / challenge)
- Used components
- Practical solution / demonstration
- Outlook

Idea

- Basis: Hackathon March 2019 in Graz
 - Topic „notarization and proof for geo based games“ (e.g. geocaching)
 - Concept & prototype blockchain solution
 - Check in riddles
 - Check & notarize („proof“) the first solver & physical finder
- Now: Some extensions
 - Usage of PIN to lock/unlock the card
 - Usage of Wallet functions (i.e. cryptocurrencies)
 - Creation of a Blockchain Token („Infineon Security 2GO Token“)

Used components

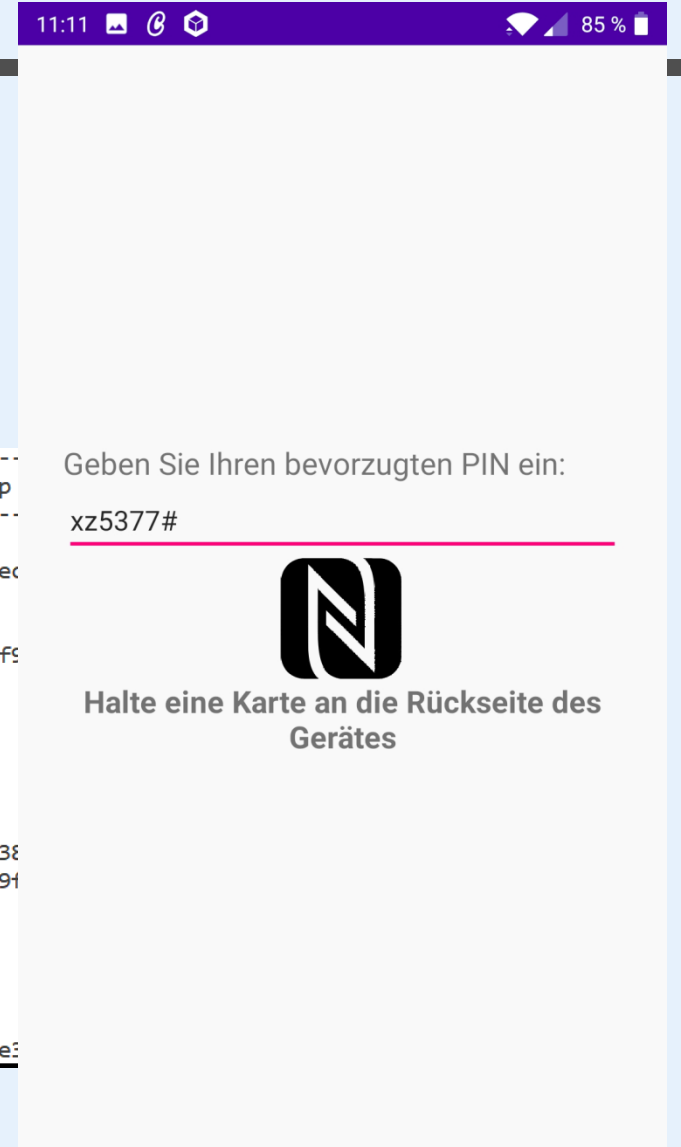
- Infineon Blockchain Security 2 Go
 - Chipcards & Reader
- Coinfinity Android Wallet
 - NFC card functionality
- Software
 - <https://github.com/Infineon/BlockchainSecurity2Go-Python-Library>
 - <https://github.com/DhruvKhemani/Praesidium> - Bitcoin Wallet in Python
 - Node.js, Truffle ...



PIN

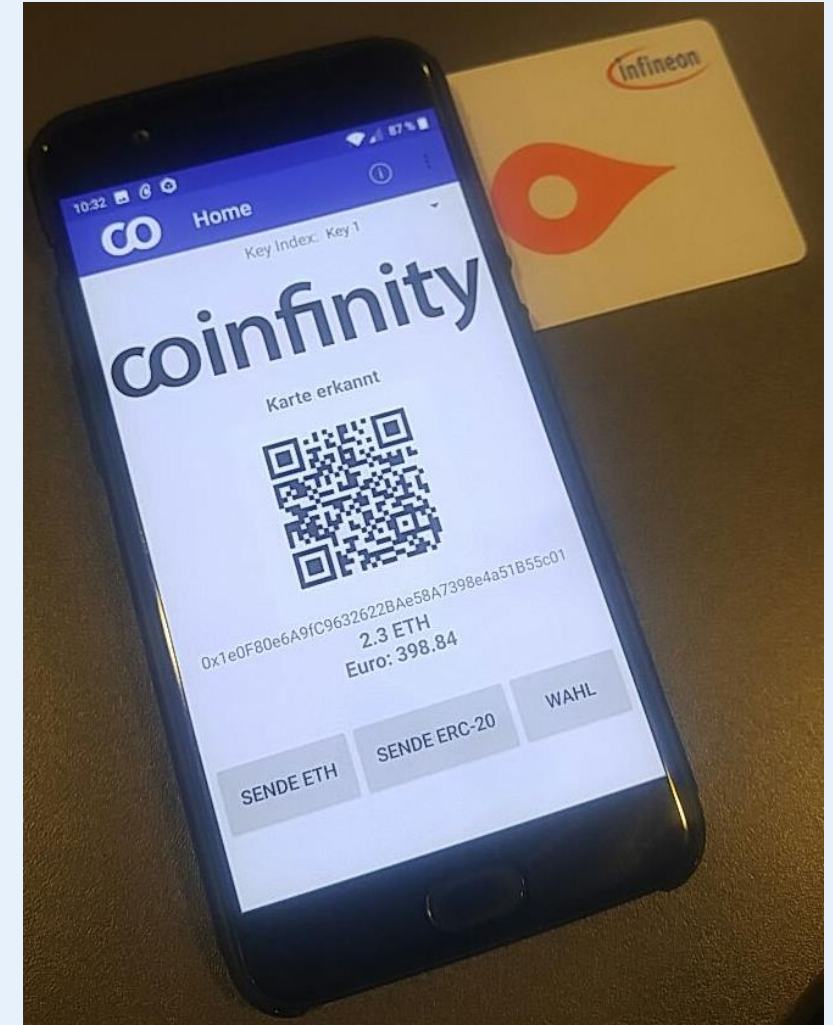
- Usage of PIN to lock/unlock the card
 - PIN as result of the riddle
- Benefit: Enhanced security
 - no „random found“

```
-----  
Step 2: Sign data provided by blockchain-app  
-----  
Trying to read card ...  
<blocksec2go.comm.pyscard.PySCardReader objec  
Card ID: 02058d1900040020001d  
v1.0  
Public key: 042e4688dbdbfc7c130b25b7bd54a72f5  
51d366fc8ee0aacd5fb9e229bdd1a5c3fc5c5412  
Enter PIN to unlock the card: xz5377#  
  
GET DATA TO SIGN ...  
Text to sign: 5dcbd3326b1be  
Signature: 3045022100fcf524e06e5c5e0ebe5ffb3f  
08092b233a595f5cceb940f446030c79e4ab4d56979f  
Enter your name (optionally): Chris  
  
SENDING DATA TO BLOCKCHAIN ...  
RESULT: testing step 2  
checking cardId 02058d1900040020001d  
searching cardIdHash 762ee75010fb5bc4648ba2e5
```



Wallet

- Usage of Wallet functions
 - Card holds keys for cryptotoins
 - Finder can claim the coins
- Mobile App
 - NFC communication with card & Ethereum Blockchain
 - Use tokens
 - Call smart contracts
- Benefit: additional „financial motivation“ for players
- (alternative: Bitcoin-Wallet)



Token

- Creation of a Blockchain Token
 - „Infineon Security 2GO Token“ (IS2T)
 - Represents some real value
 - Transferred to cards
 - Used to pay for e.g. Infineon products (Webshop ...)

```
/*  
Ethereum Smart contract for "Infineon Security 2Go"  
baumann.at - 12.11.2019  
*/  
pragma solidity ^0.5.0;  
  
import "openzeppelin-solidity/contracts/token/ERC20/ERC20.sol";  
  

```

Summary

- Infineon Blockchain Security 2Go
 - Hardware Security System
 - Different usecases
 - ...
- Usage in (geo based) gaming (e.g. geocaching)
 - Blockchain based proof of situations (solving of riddles, presence at geographical locations ...)
 - Additional aspects (financial motivation, marketing, security ...)

Outlook

- Further potential usecases for BC Sec 2Go
- Examples for similar applications
 - Crypto Stamp
 - Cryptokitties
 - Satoshi's Treasure

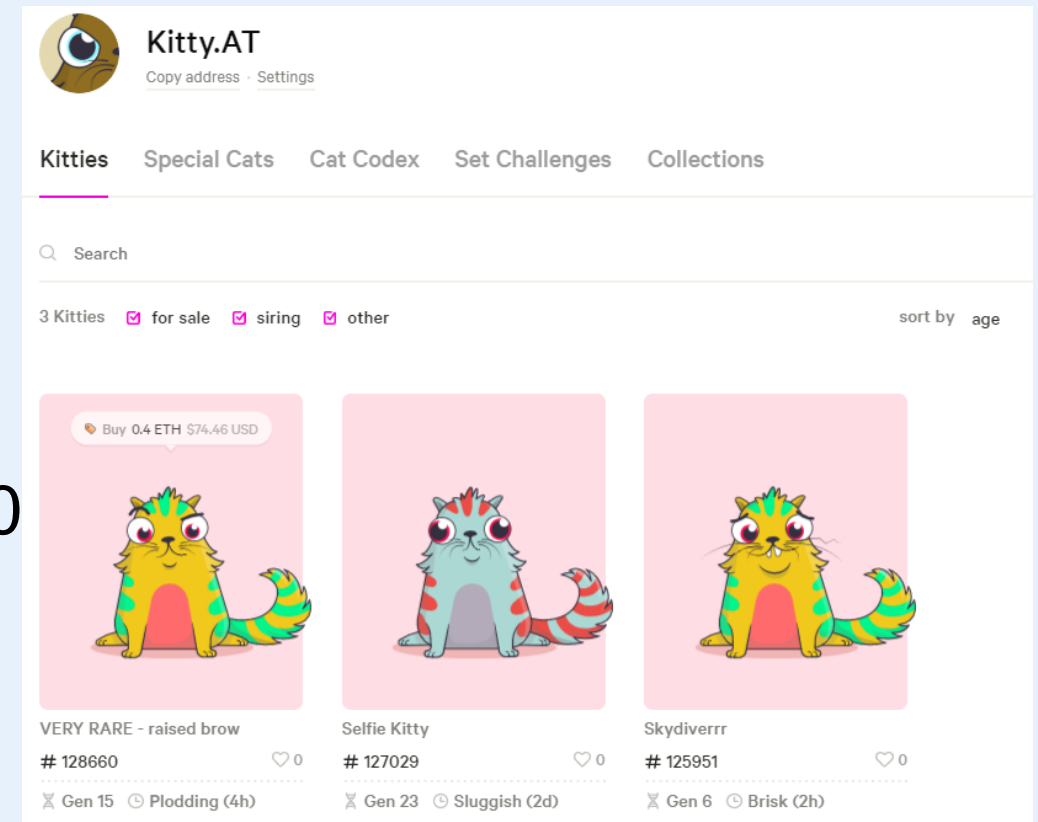
■ Crypto Stamp

- series of post-stamps (post.at)
 - with a digital twin
 - as ERC721 Token on Ethereum Blockchain
 - 150.000 pieces, sold out almost immediately
- ## ■ Why BC S2Go Hardware?
- Additional hardware security (replacing QR-codes, which hold the private key)



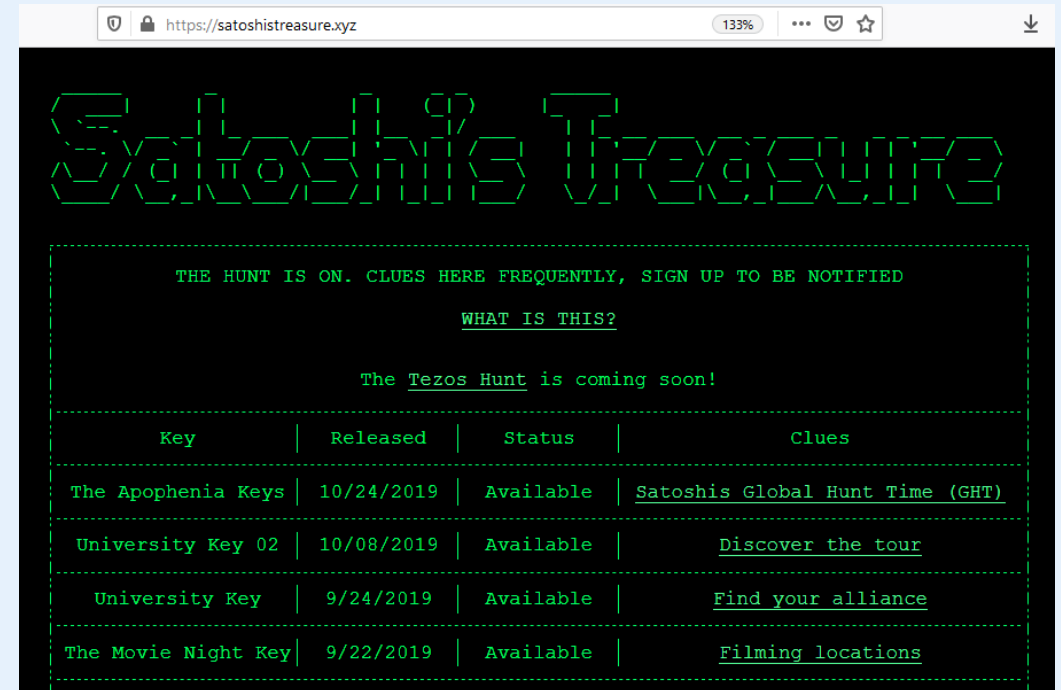
Cryptokitties

- Collection game
 - Virtual cats as tokens on a blockchain
 - can be bought, sold or transferred digitally
 - with strong guarantees of ownership
 - ca. 1,5 Million kitties, up to 150.000 US\$
- Why BC S2Go Hardware?
 - Combination of Blockchain and “real world”
 - card collectors => physical card



Satoshistreasure.xyz

- **Crypto-Challenge**
 - Worldwide hunt, solve riddles
 - visit locations worldwide
 - physical, QR-Code
 - find 400 out of 1000 keys & reconstruct a Bitcoin private key
 - 1 Mio. US\$ in Bitcoin
- **Why BC S2Go Hardware?**
 - Physical security for keys (on geo locations) replacing QR-Codes



Contact



DI Dr. Christian Baumann

+43 664 4324243

c.baumann@baumann.at

<https://www4.baumann.at>