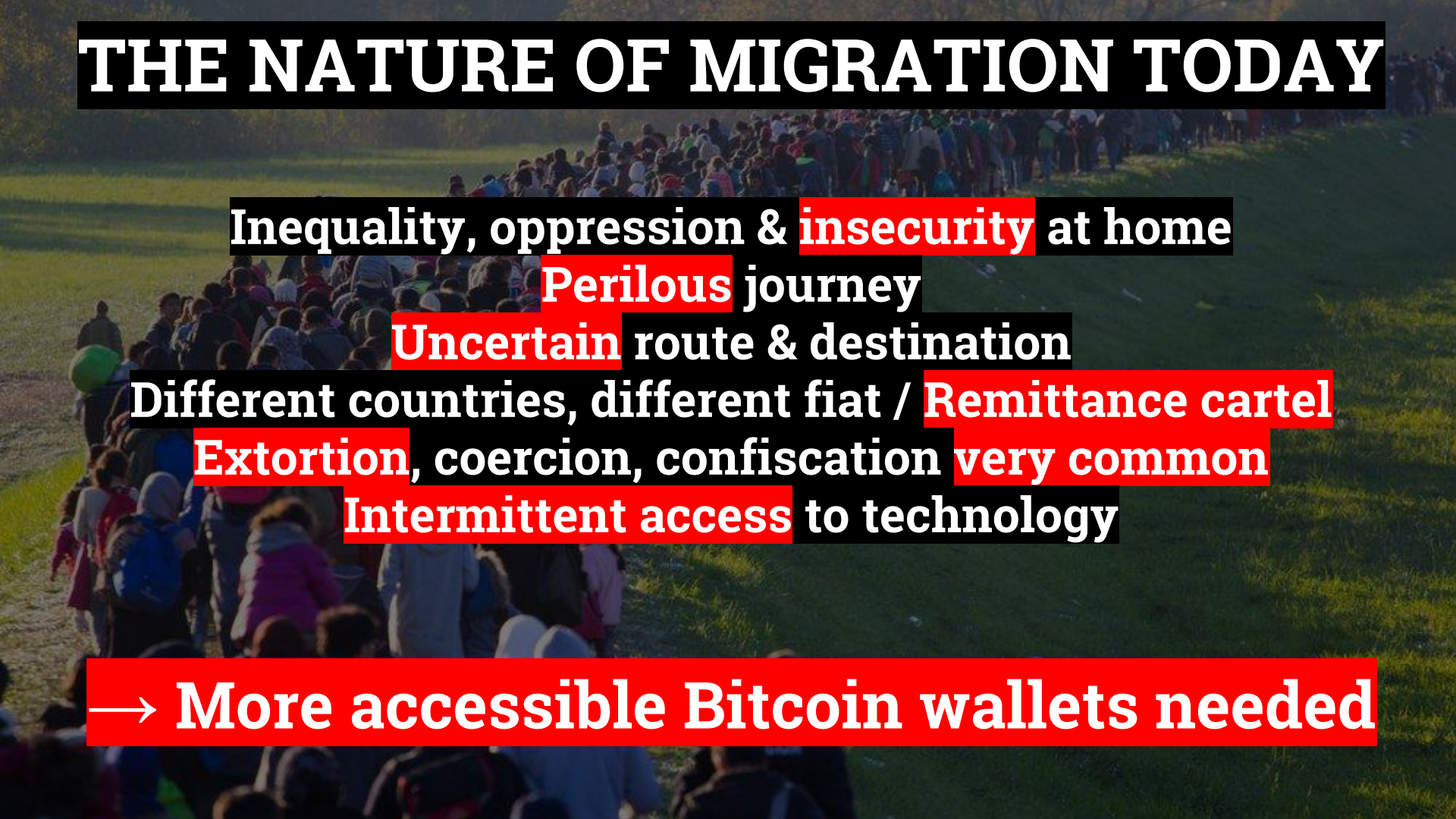

# Team 4: Reaching Everyone

#chainhack3 / Lisbon / 29 June - 1 July 2018

These Slides: www.reachingeveryone.net

info@reachingeveryone.net


TLDR:
A Bitcoin wallet for migrants & their families with limited access to infrastructure & technology
SHARED NODE
ACCESS POINT

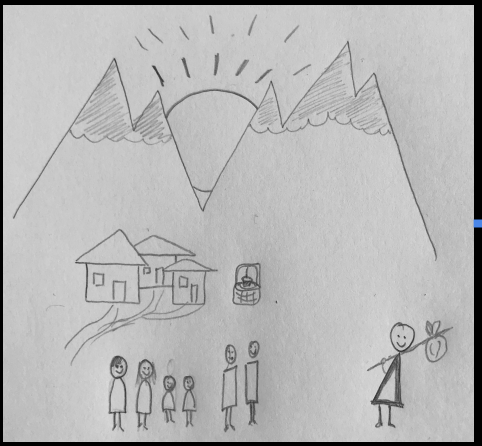


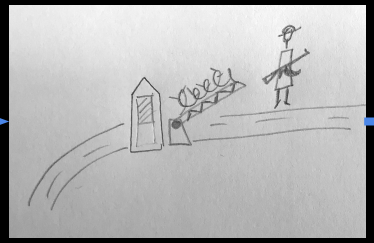
# THE NATURE OF MIGRATION TODAY

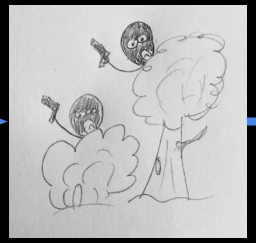
Inequality, oppression & insecurity at home
Perilous journey
Uncertain route & destination
Different countries, different fiat / Remittance cartel
Extortion, coercion, confiscation very common
Intermittent access to technology

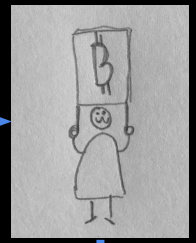
**→ More accessible Bitcoin wallets needed**

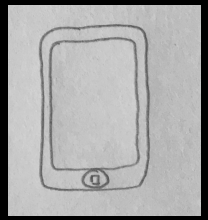
# MIGRANT JOURNEY

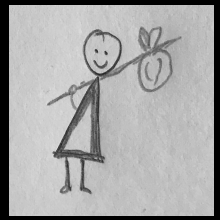


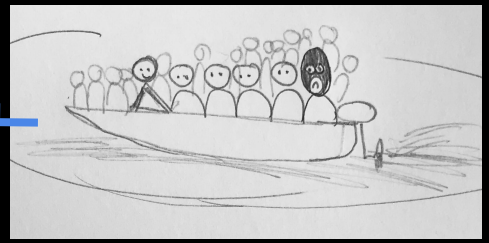


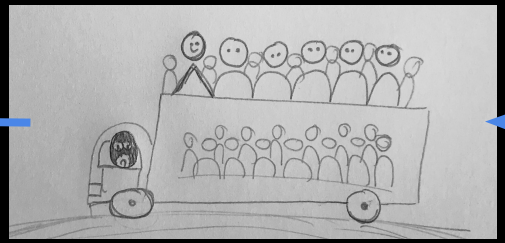


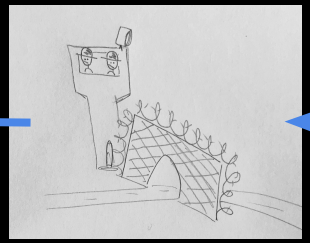



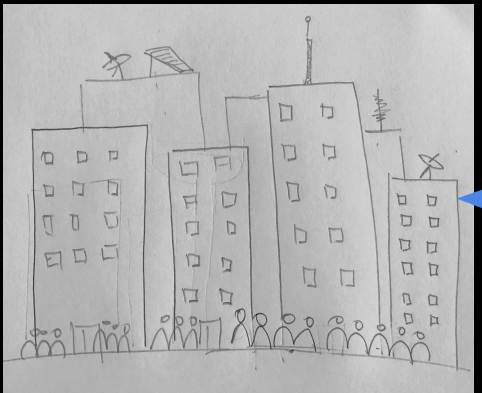








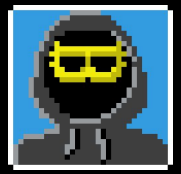




# WHY BITCOIN?
# DOES THIS NEED A BLOCKCHAIN?

## Political & Economic Oppression
## Censorship / Extortion / Confiscation

IT'S DANGEROUS TO GO ALONE! TAKE THIS.




BAYT

# “BAYT” بيت (HOME)

A simple web wallet

Minimal technology requirements

Personal Q&A generates privkey

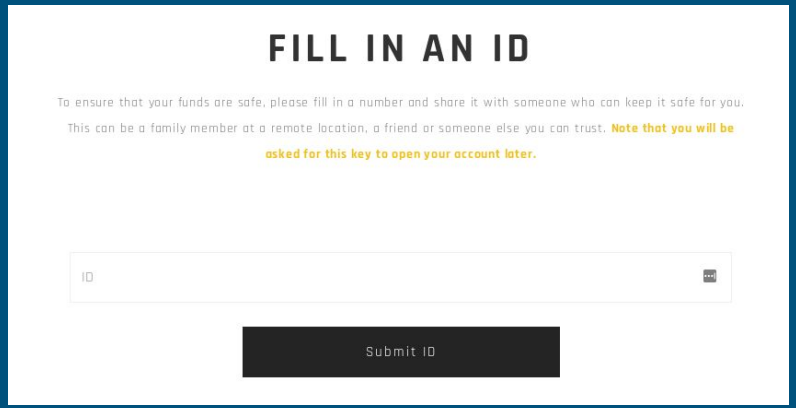
Drip-feed funds to migrant

→ Minimise extortion / confiscation

(play with our demo @ Table 4 at the back of the room)
http://web.tecnico.ulisboa.pt/~ist186428/chainhack/

# “BAYT” WEB APP SCREENSHOTS





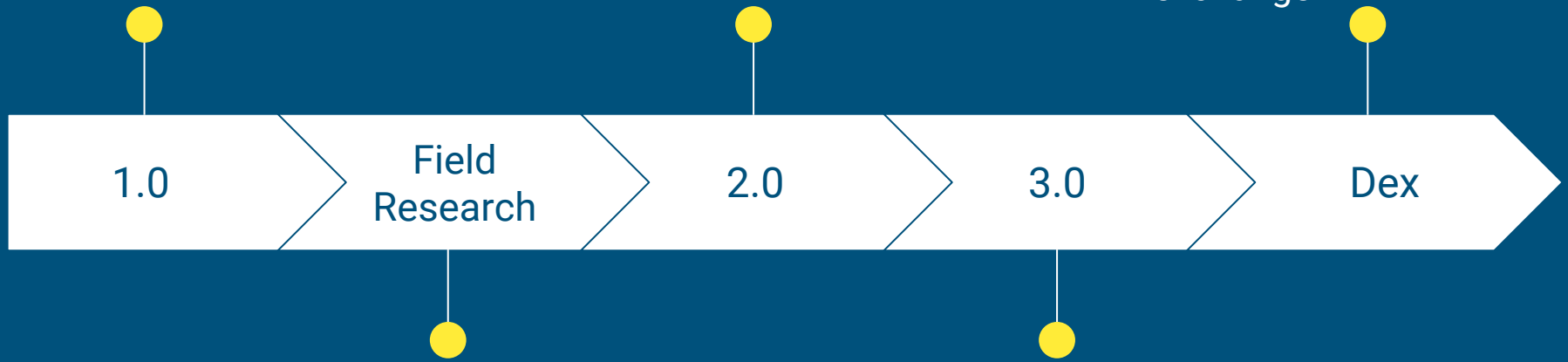

**(play with our demo @ Table 4 at the back of the room)**
**http://web.tecnico.ulisboa.pt/~ist186428/chainhack/**

# PROTOTYPE → REALITY

1. Finishing the MVP
2. Build interest

1. Expanded Q&A for privkey generation
2. IPFS/SIA resilient hosting

DEX for P2P/R2R exchange



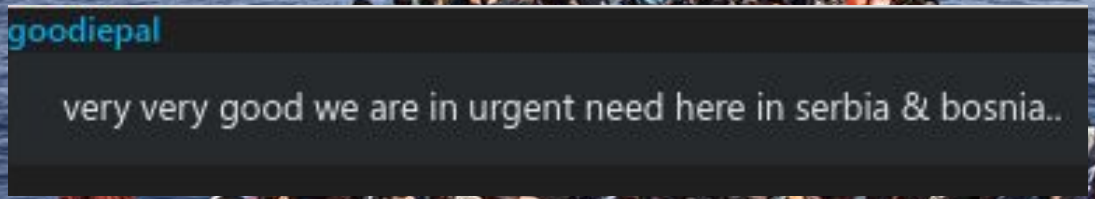

1. Testing in Serbia
2. Bitcoin Magazine articles
3. Multi-Language support

1. Duress mitigation / Plausible deniability
2. NFC/RFID/HW wallet R&D

# HOW TO SUSTAIN PROJECT?

## Hackathon prize money would help!

**100% goes directly to project**

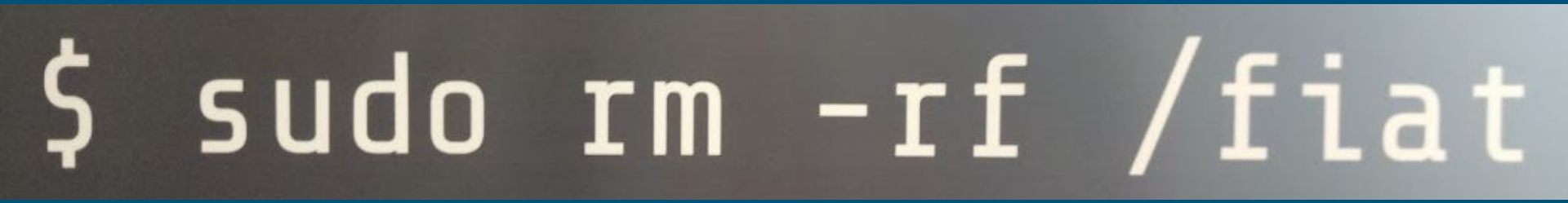



## We need YOU!

**info@reachingeveryone.net / @parallelind**

**Why help? BTC adoption = PERMA-MOON**

# THANKYOU #CHAINHACK3!




# QUESTIONS & COMMENTS?

# SECURITY / TRUST MODEL RELAXATIONS

Censorship Resistance > Security
Imperfect entropy in privkey gen
Hub & Spoke
Web wallet
Insecure devices

# GRAMTROPY: PASSWORDS FOR HUMANS (adapt for wider region support)

## Pieter Wuille FACTS

1. Pieter Wuille won the underhanded crypto contest but his entry was so underhanded nobody even knows he entered.
2. If you SHA256 the IPA pronunciation of Pieter Wuille, the result is 0. Fortunately, nobody but Pieter Wuille knows what that is.
3. The blockchain is getting bigger, yet every time Pieter Wuille uses his fingers it takes less to sync - if we extrapolate, singularity?
4. Only Pieter Wuille can name things harder to pronounce than Pieter Wuille.
5. Pieter Wuille is so much above the Ballmer Peak that if you add him to the graph you can't see the old curve anymore.
6. Blocks containing transactions by Pieter Wuille propagate faster than other blocks.
7. Pieter Wuille once calculated a 256-bit SHA on an abacus, and the resulting block gave 25 bitcoins to charity.
8. Pieter Wuille is the quantum state of bitcoin.
9. If a tree falls in a forest and no one is around to hear it, Pieter Wuille knows.
10. Consensus occurs when Pieter Wuille agrees with himself.

## Gramtropy: a grammar-based password generator

https://github.com/sipa/gramtropy

### What is Gramtropy

Gramtropy is a tool that can generate passwords or passphrases taken uniformly from a set specified by an unambiguous Context-free Grammar.

It aims to solve the problem of generated passwords that are pronouncable according to arbitrary rules, while simultaneously guaranteeing a given security level (in bits).

### Building

You need the C++11 compiler from GCC 4.7 or later. It likely works with other C++11 compilers, but I haven't tested it.

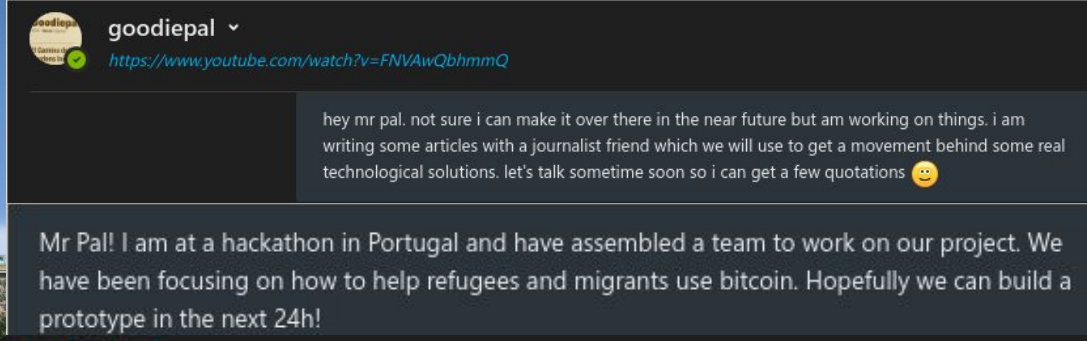
Run `make`. Two binaries should be produced, `gramc` and `gram`. The first is a compiler that takes a grammar file and a security level, and produces a translation file. The second interprets a translation file to generate passphrases and more.

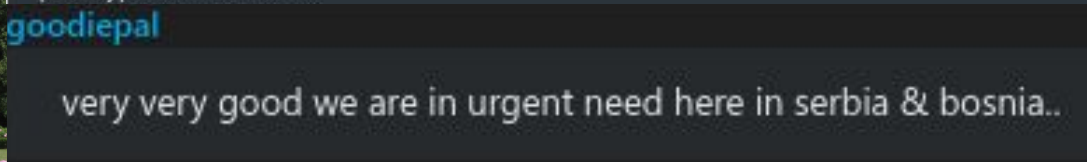
### Usage

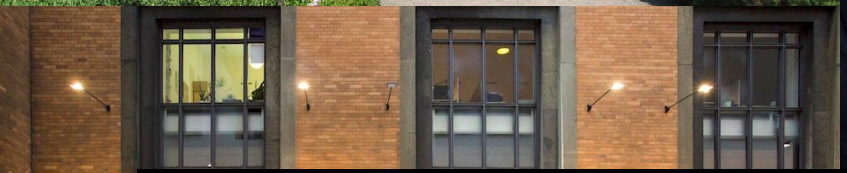
Create a file `simple.gram` with the following contents:

```
vowel = "a"|"e"|"i"|"o"|"u";
consonant = "b"|"d"|"f"|"g"|"h"|"k"|"l"|"m"|"n"|"p"|"r"|"s|"t"|"v"|"w"|"z";
convow = consonant vowel;
main = convow+;
```

# TORTURE, CONFISCATION, CENSORSHIP, UNCONCEALABILITY, FLIGHT TO SAFETY

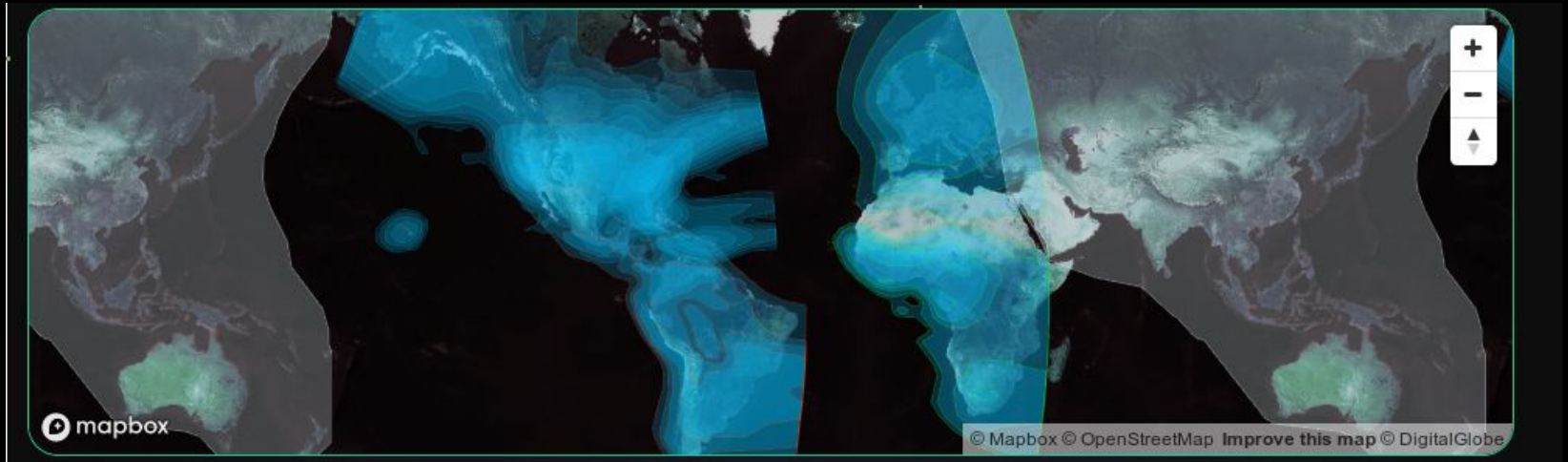



# GOODIEPAL - RADICAL MUSICIAN & HUMANITARIAN

# Blockstream Satellite Network:
# Mitigate censorship / sync without censorship / verify!




**GALAXY 18**
North America
Long: 123W
Freq: 12022.85 MHz
Pol: Horizontal

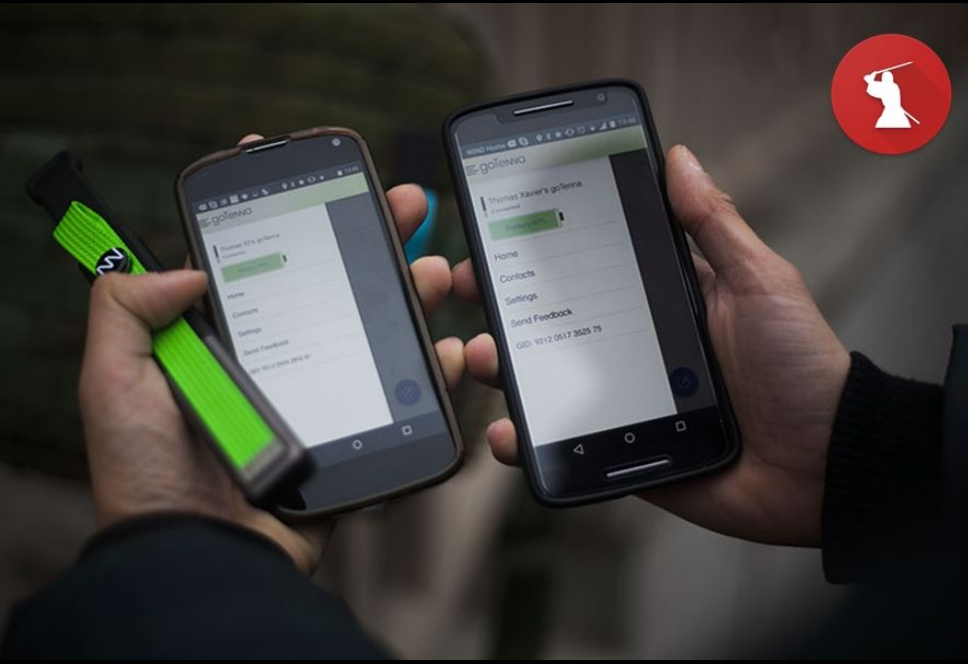
**EUTELSAT 113**
South America
Long: 113W
Freq: 12026.15 MHz
Pol: Vertical

**TELSTAR 11N**
Africa
Long: 37.5W
Freq: 11476.75 MHz
Pol: Horizontal

**TELSTAR 11N**
Europe
Long: 37.5W
Freq: 11504.02 MHz
Pol: Vertical

**PHASE 2**
Coming Soon
Long: TBD
Freq: TBD
Pol: TBD

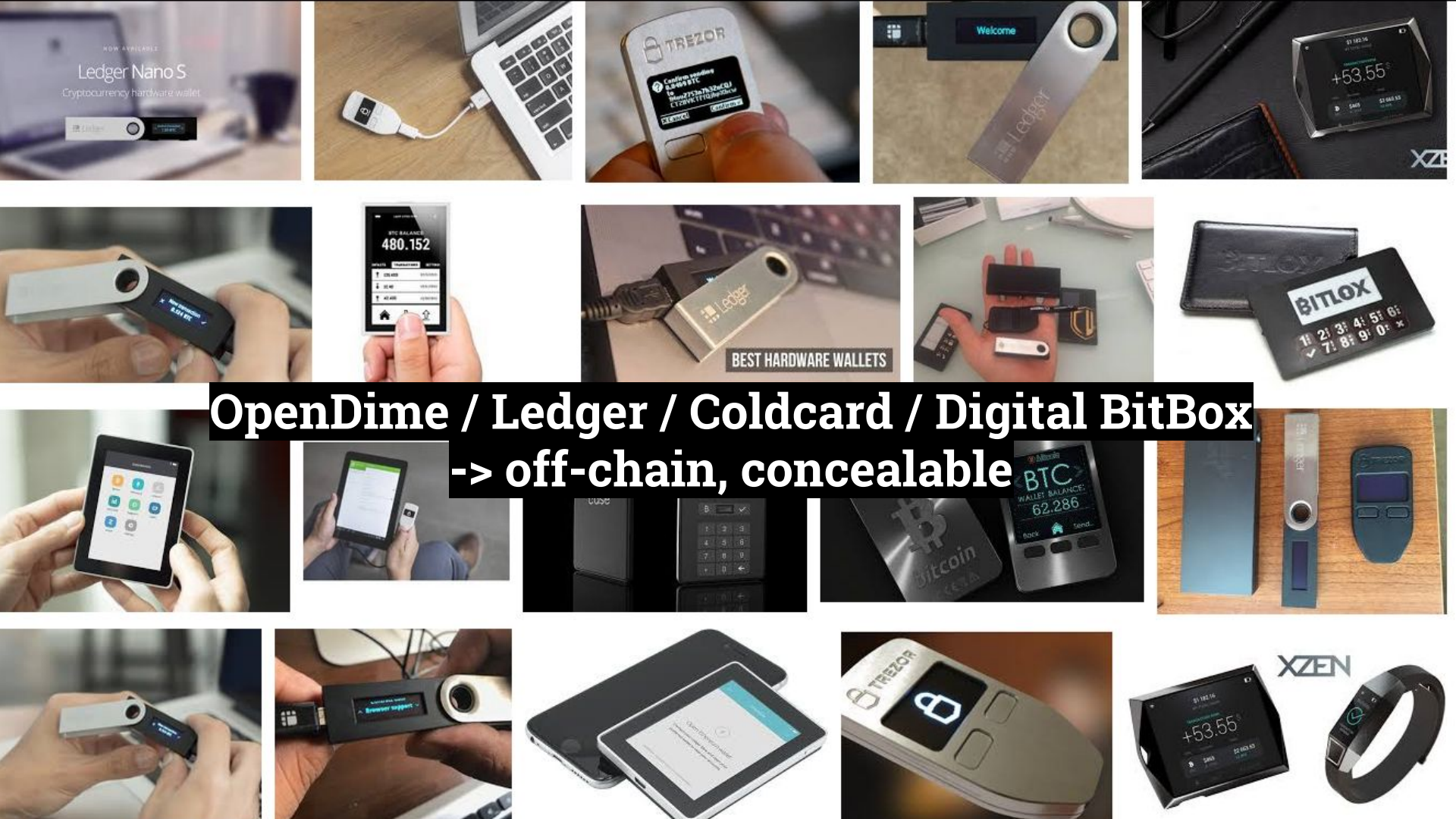
# goTenna MESH Networking + Samourai = txTenna



- SMS relay
- satellite hook-up
- fax or any form of hard copy to character recognition
- save to external support (USB)
- Portable Document Format (PDF)
- telex
- HF audio
- Morse code
- meshNets
- NFC
- BLE
- chat apps (especially encrypted)

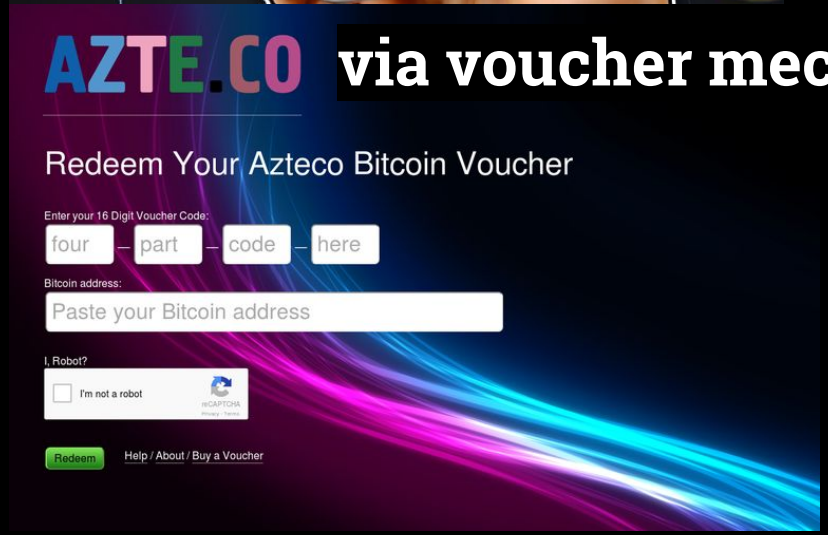
# (HK Umbrella Revn)

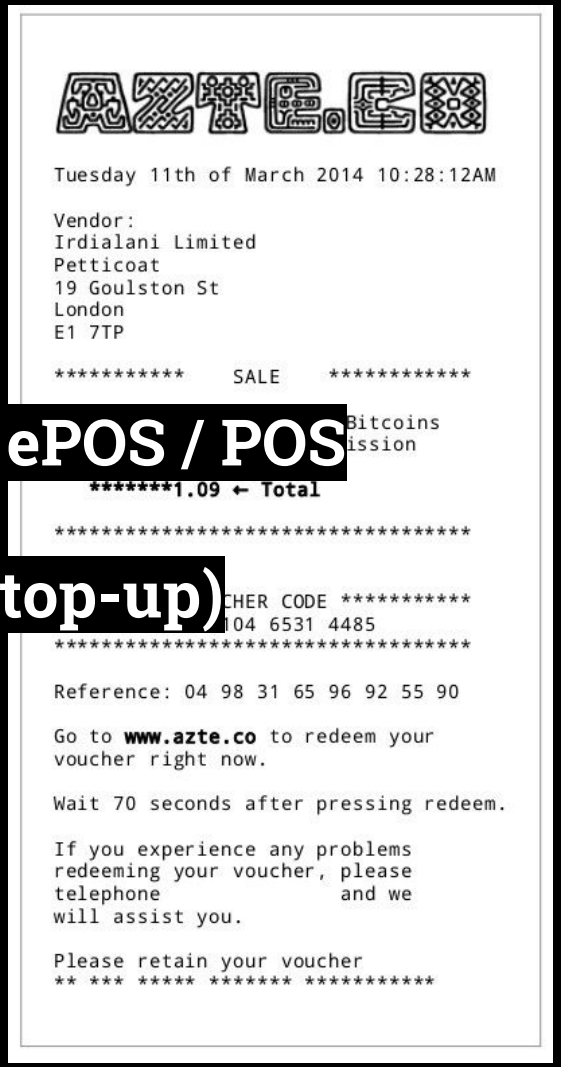

Polymerbit / Tangem / BitNotes
-> Printable, streaming top-up with Lightning
-> concealable, durable, offline




# OpenDime / Ledger / Coldcard / Digital BitBox
# -> off-chain, concealable


# Azteco / Bitrefill - purchase crypto at ePOS / POS via voucher mechanism / mobile top-up)



AZTE.CO

Tuesday 11th of March 2014 10:28:12AM

Vendor:
Irdialani Limited
Petticoat
19 Goulston St
London
E1 7TP

********** SALE **********

Bitcoins
ission

*******1.09 ← Total

**********

CHER CODE **********
104 6531 4485
**********

Reference: 04 98 31 65 96 92 55 90

Go to **www.azte.co** to redeem your voucher right now.

Wait 70 seconds after pressing redeem.

If you experience any problems redeeming your voucher, please telephone and we will assist you.

Please retain your voucher
** *** ***** ******* **********

# THE BUSINESS MODEL

*Operational inefficiency, lack of transparency, local corruption, outcomes unclear.*


## Donor

Altruistic, unconditional. Direct impact of benefit unclear. Donations can take a long time to reach those in need.

## Collection

Donations are collected by charity and enter an archaic and inefficient system. High operational costs in legacy systems.

## Distribution

Partner organisations in beneficiary countries are at risk of corruption and chronic bureaucracy.

## Beneficiary

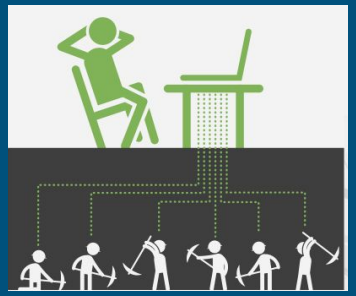
Complex supply chains and FX / logistical costs erode value of donations.

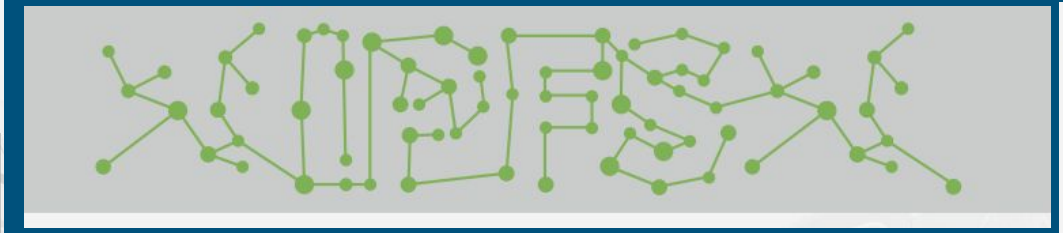
Mail Online News

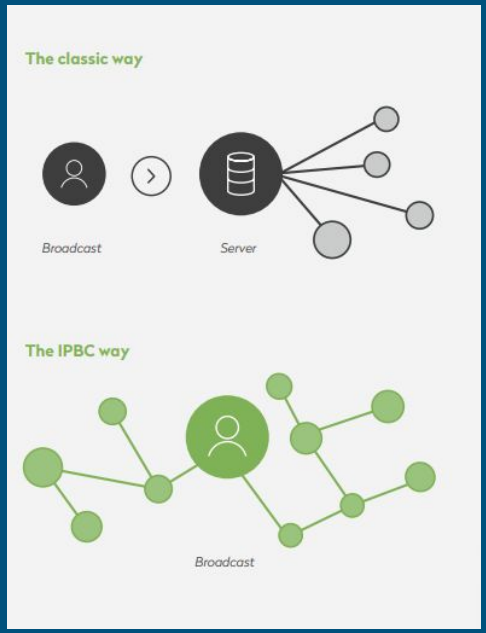
# One in five of the UK's biggest charities are 'spending less than half of their income on good causes' (and some spend as little as ONE PER CENT on charitable work)

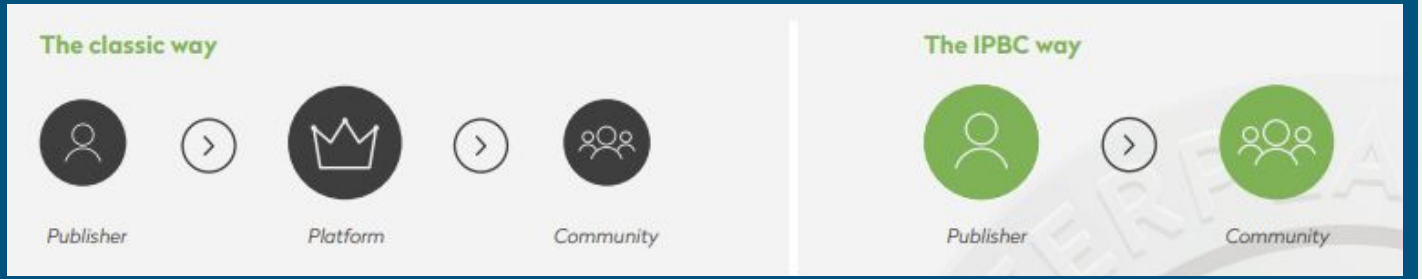
- Big UK charities 'are spending less than half their income on good work'
- Nearly 300 allegedly spent just 10% on charitable activities in three years
- And Lloyd's Register Foundation used only 1% of money on such causes
- Other accused charities include the British Heart Foundation and Age UK

***2015***

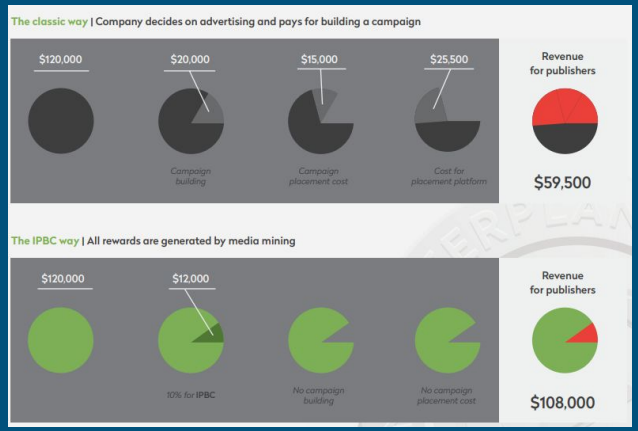




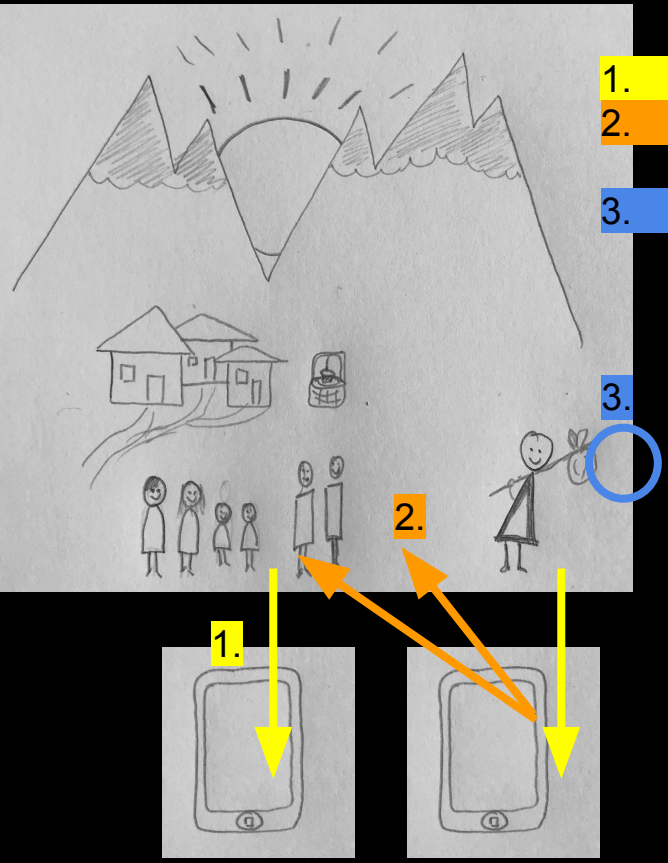

The classic way
Broadcast
Server
The IPBC way
Broadcast


The classic way
Publisher
Platform
Community


The IPBC way
Publisher
Community


The classic way | Company decides on advertising and pays for building a campaign
$120,000
$20,000
$15,000
$25,500
Campaign building
Campaign placement cost
Cost for placement platform
Revenue for publishers
$59,500
The IPBC way | All rewards are generated by media mining
$120,000
$12,000
10% for IPBC
No campaign building
No campaign placement cost
Revenue for publishers
$108,000

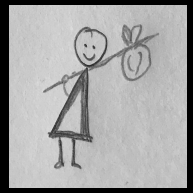
# Before the journey




1. M & family generates “Simple Seed”
2. M leaves questions-backup partitioned with family & friends
3. M practices seed-memorization

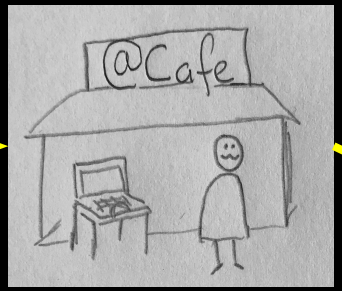
# On the journey

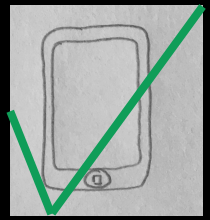
1. Threatened by borderpatrol
   → Restore wallet with mnemic seed
2. Robbed and injured by bandits
   → Restore wallet with family backup

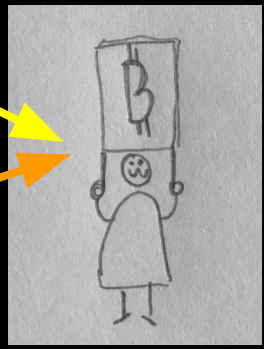


1.

2.

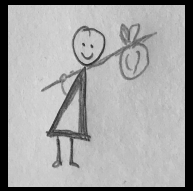


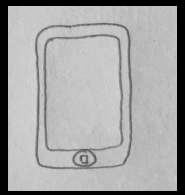



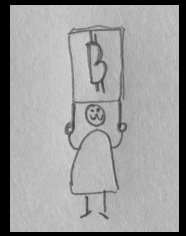


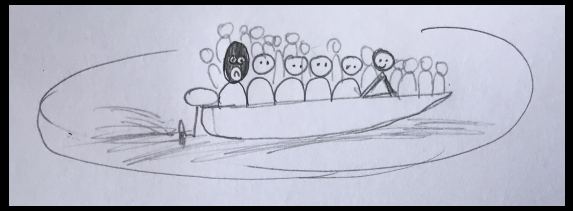
# On the journey (2)

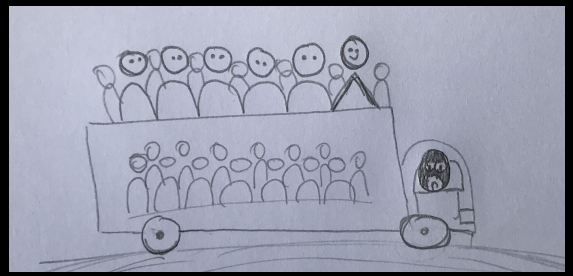
1. Save retrieval of  funds and payout for smugglers
2. Keeping funds save from

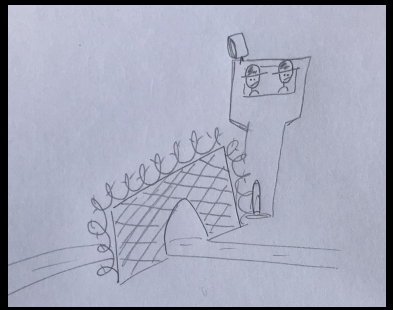












# FROM PROTOTYPE TO REALITY

- We need you! Help us bootstrap a community :)
- Field research & trials in Serbia & Bosnia
- Bitcoin Magazine articles soon™
- Single wallet -> Multi wallet & drip-feed functionality
- Multi-lanuage support
- Expanded Q&A for privkey generation
- IPFS / Sia for resilient hosting
- Duress / Plausible deniability mitigation
- Local hubs (NGOs, activists, bitcoiners) w/ crypto <-> fiat tx
- NFC/RFID/HWwallet devices
- Mitigate malware risk on insecure PCs & phones
- DEX for P2P / R2R exchange