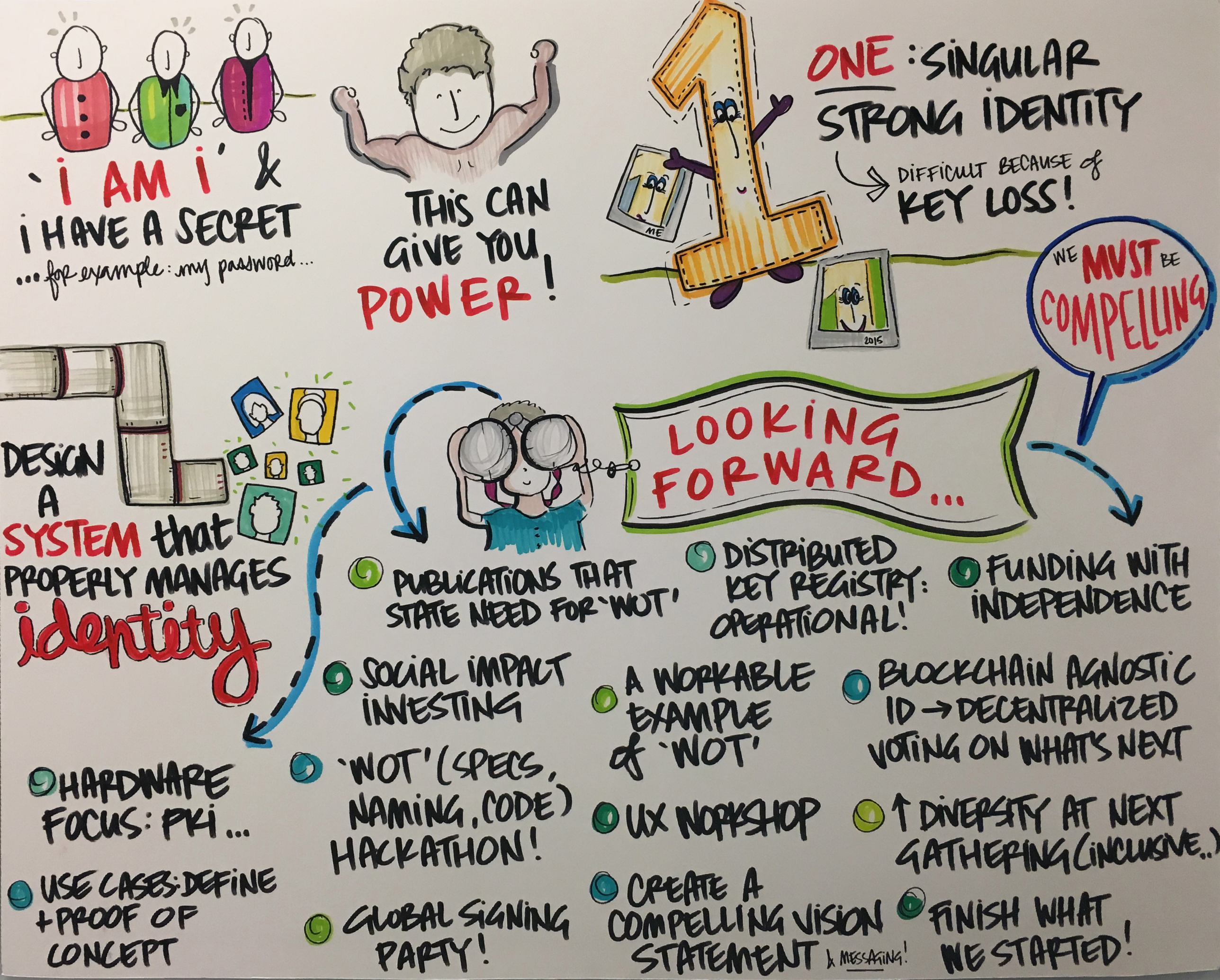
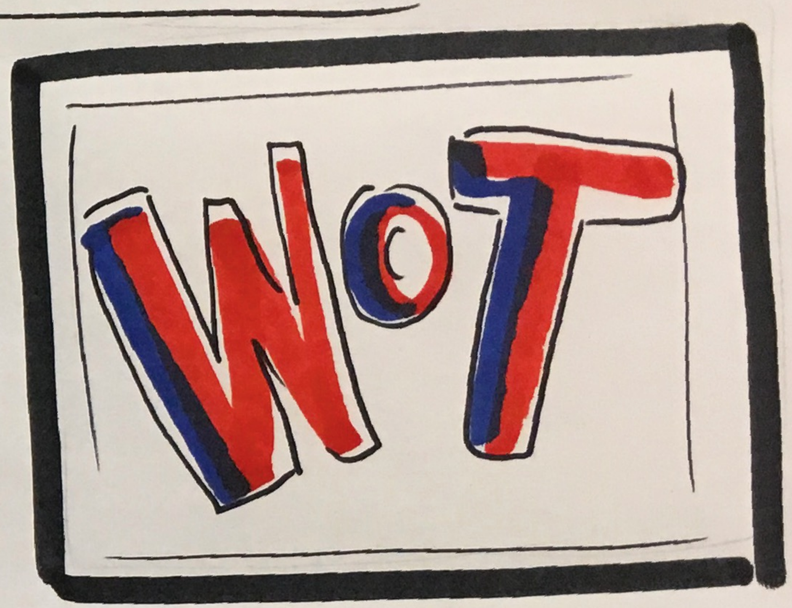
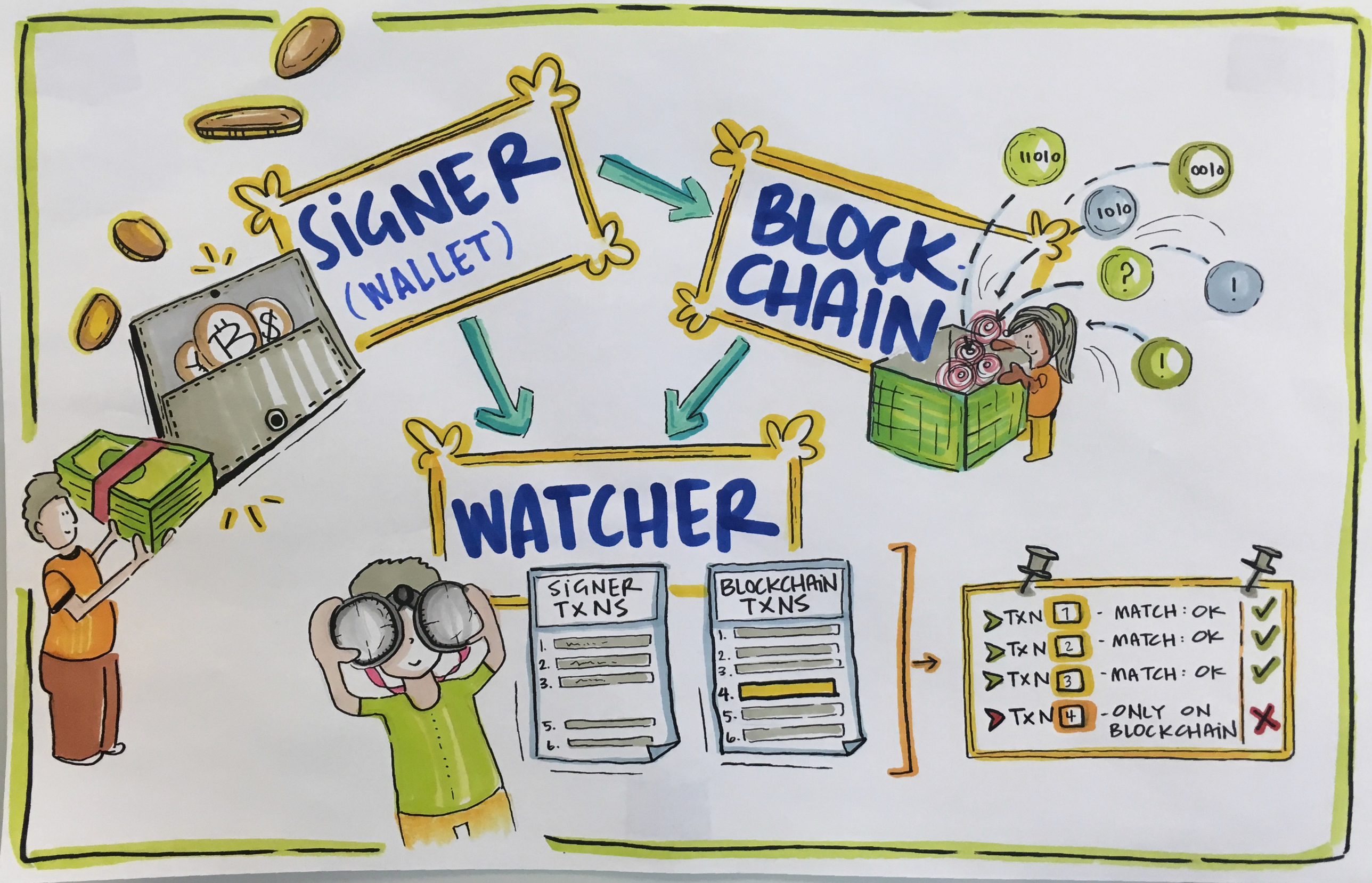
Welcome Back
JULY 2016
OVERNIGHT insights
...TO DAY 2 OF REBOOTING WEB OF TRUST
WHERE DO WE WANT TO BE IN JULY '16?
...THINK BROAD!
...SELF SOVEREIGN IDENTITY
PLAY AS A TEAM
& SUPPORT 'WHOEVER HAS THE BALL'
WHAT THE WORLD NEEDS... IS SOMETHING EASY to UNDERSTAND...
FOR HUNDREDS of MILLIONS OF PEOPLE WORLDWIDE
#1
WE NEED ONE MODEL
START with THE CUSTOMER'S WORLD at THE CENTER... NOT JUST YOURS
WHAT REQUIRES OUR IMMEDIATE ATTENTION? PRIORITIZE THIS!
BE AGILE in OUR APPROACH


'I AM I' &
I HAVE A SECRET
...for example: my password...
THIS CAN GIVE YOU POWER!
ONE: SINGULAR STRONG IDENTITY
DIFFICULT BECAUSE of KEY LOSS!
ME
2015
WE MUST BE COMPELLING
DESIGN A SYSTEM that PROPERLY MANAGES identity
LOOKING FORWARD...
PUBLICATIONS THAT STATE NEED FOR 'WOT'
DISTRIBUTED KEY REGISTRY: OPERATIONAL!
FUNDING WITH INDEPENDENCE
SOCIAL IMPACT INVESTING
A WORKABLE EXAMPLE of 'WOT'
BLOCKCHAIN AGNOSTIC ID → DECENTRALIZED VOTING ON WHAT'S NEXT
HARDWARE FOCUS: PKI...
'WOT' (SPECS, NAMING, CODE) HACKATHON!
UX WORKSHOP
↑ DIVERSITY AT NEXT GATHERING (INCLUSIVE..)
USE CASES: DEFINE + PROOF OF CONCEPT
GLOBAL SIGNING PARTY!
CREATE A COMPELLING VISION STATEMENT & MESSAGING!
FINISH WHAT WE STARTED!

# REBRANDING WEB OF TRUST...

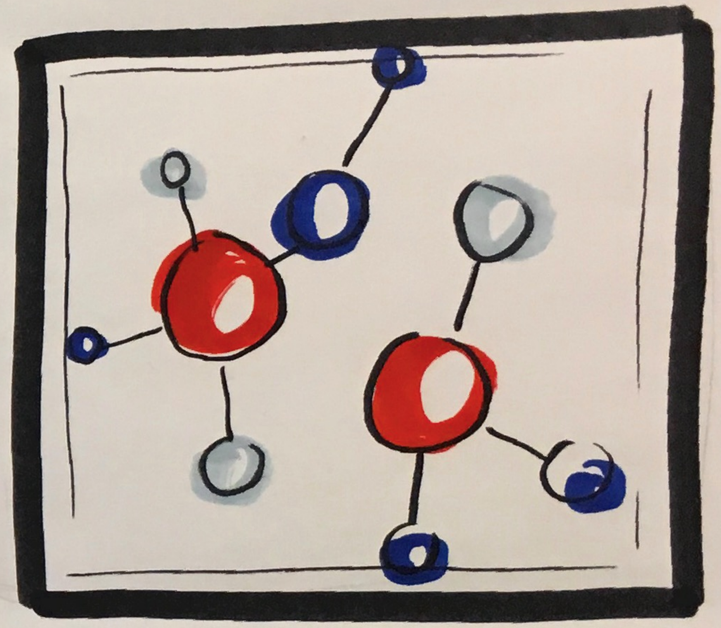
- PGP ORIGINS: ALL ABOUT KEY VALIDATION
- EXPAND WHAT 'WEB OF TRUST' IS
- 'WEB' = 'DECENTRALIZED'
- 'OF TRUST' = IDENTITY, KEYS, REPUTATION
- TIGHT CORE (SIMPLE, USEFUL) = IDENTITY / IDENTIFIER → + 'ATTRIBUTES & ASSESSMENTS'
- AS YOU INTERACT, YOU DEVELOP SUBJECTIVE THINGS AROUND THIS
  ... FOR EXAMPLE: TRIP ADVISOR
- PROPOSED NAMES: 'WOT': RECOGNITION .. TRUST .. INSIGHTS .. DISTRIBUTED IDENTITY .. ETC. (FULL LIST ON GOOGLE DOCS
- MODEL HAS 3 COMPONENTS: SIGNER (WALLET) + WATCHER + BLOCKCHAIN (SEE DIAGRAM) ..




SIGNER
(WALLET)
BLOCK CHAIN
11010
0010
1010
?
!
!
WATCHER
SIGNER TXNS
1.
2.
3.
5.
6.
BLOCKCHAIN TXNS
1.
2.
3.
4.
5.
6.
TXN 1 - MATCH: OK
TXN 2 - MATCH: OK
TXN 3 - MATCH: OK
TXN 4 - ONLY ON BLOCKCHAIN

# DPKI ...

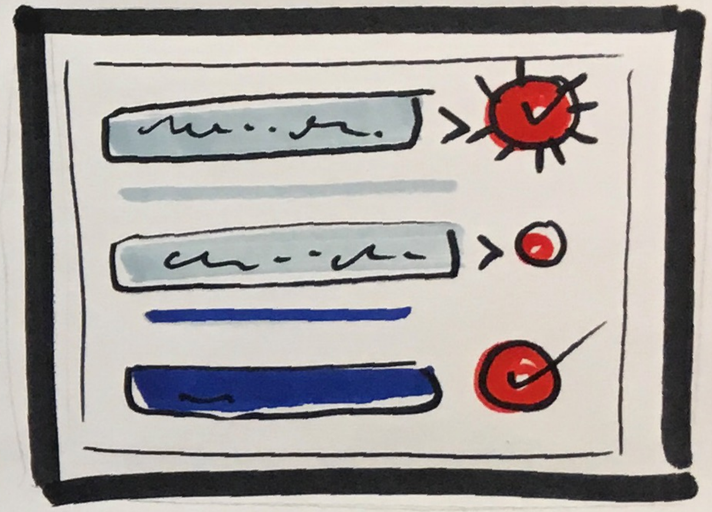
- DPKI: DECENTRALIZED PUBLIC KEY INFRASTRUCTURE
  .. SOLUTION TO 'WOT' REBRANDING
- PAIN POINTS: IDENTITIES ONLINE & OWNERS OF THOSE IDENTITIES
- HOW TO KNOW WHO TO TRUST / WHAT IDENTITY?
  .. WHO ACTUALLY OWNS THIS?
- EX: OWNER OF WEBSITE = CERTIFICATE AUTORITIES
  ... NOT YOU!
- DPKI IS ABOUT FIXING THIS MISMATCH PROBLEM
  → DECENTRALIZED SECURE KEY VALUE STORAGE : EX: BLOCK CHAINS
- BLOCKCHAIN ISSUES: WHAT HAPPENS IF CENTRALIZED? + CANT RUN ON CELL PHONE
- MINIMUM OF 3 ENTITIES: 'DEVELOPERS', 'NODES' W/ COPY OF BLOCKCHAIN, & MINERS
- GOAL: TO USE AGNOSTIC STANDARD INTERNET PROTOCOL
- CURRENT SYSTEM: DICTATES TRUST
  DPKI: UP TO YOU TO DECIDE WHO TO TRUST!



# CREATING DISTRIBUTED REGISTRY...

NOT KEY!

- NEED TO FIND TOKENS THAT ARE UNIFORM WITHOUT RELYING ON ONE CRYPTIC SYSTEM
- DISTRIBUTE PERMANENT IDENTIFIER THAT YOU HAVE CONTROL OF ... & BE ABLE TO DELEGATE THIS TO A SET OF REQUIREMENTS... THAT YOU THINK ARE VALID!



- DRIVEN BY CONSISTENCY OF THE UNIVERSE- THIS SUGGESTS YOU HAVE AN INTERNAL REGISTRY OF THE TOKEN & SO DOES EVERYONE ELSE
- GOAL: DELEGATE TO OTHER SYSTEMS TO MAINTAIN A CONSISTENT VIEW ACROSS NETWORKS OF WHAT 'TOKEN' MEANS
- EX: UPDATING TO GOVERNMENT LOOKS VERY DIFFERENT THAN BLOCKCHAIN

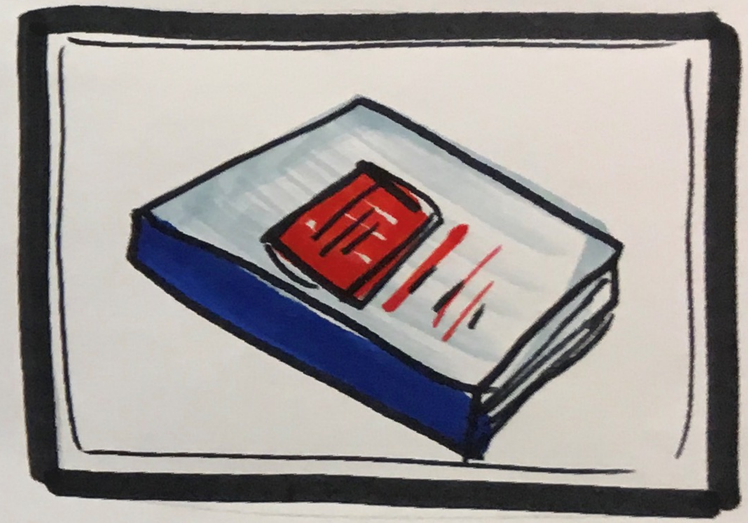
# USE CASES...

"OPPORTUNITY CREATED BY WOT TO CONTROL/ LEVERAGE PERSONAL DATA" (EX: FB!)

... EX: FACEBOOK ($FB) UNDERSTAND CONTROL/ LEVERAGE OF PERSONAL DATA...

.. PROPOSED SOLUTION: IDENTIFY REAL WORLD PROBLEM & CROSS REFERENCE WITH WOT FOR UNIQUE USERS

.. BOT SCENARIOS ENABLE CHOICE!



"SELECTIVE DISCLOSURE"

... EX: DELINQUENCY, ID AT BAR/CLUB, SHORT TERM CONTRACTS AT AIRBNB (GATHER MORE INFO THAN NEEDED)

... ANOTHER EX: WANT TO GIVE SOME INFO, NOT ALL

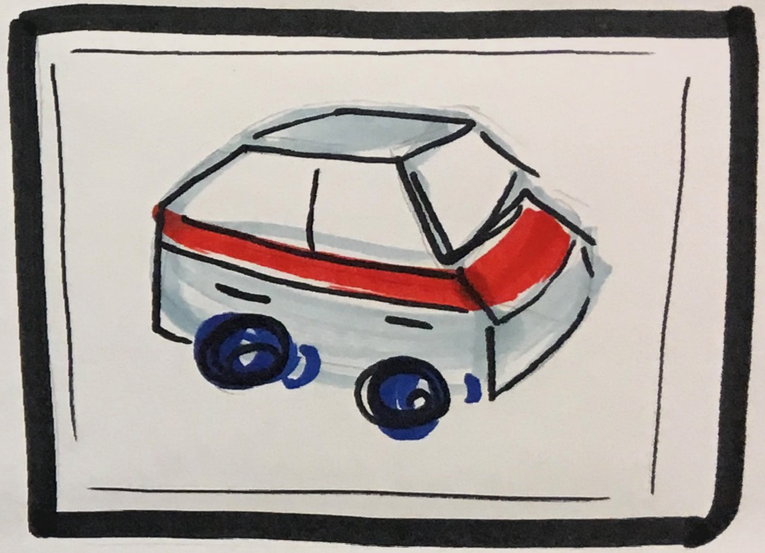
"REFUGEES" ...

"MISSING LEGAL IDENTITIES"

EX: SOCIAL WORKERS CAN TIE THEIR NAMES TO CHILD & VOUCH FOR IDENTITY

# MAKING BETTER CAR-BUYING! DECISIONS...

- WEB OF TRUST: CONNECTING KEY TO OWNER
- OUR EXAMPLE/FOCUS AREA: BUYING A CAR FROM FAR AWAY LOCATION WITH LIMITED INFO
  .. SIGNALS ARE INTERPRETED DIFFERENTLY (CONDITIONS OF THE CAR, ETC...)
- SYBIL: WHAT'S THE PAIN IN THE SYSTEM
- FOCUS ON WHAT IS THE BEHAVIOR WE WANT?
- OUR TAKEAWAY... "EVERYDAY .. I AM FACED WITH TOUGH CHOICES. RELY ON OTHERS WHEN REQUIRED TO UNDERSTAND MY OPTIONS & MAKE CHOICES...."



# SMART SIGNATURES...

- PUB KEY: EXTREMELY LIMITED
- USE CODE: REPLACE 'AUTHORIZE ME' WITH COMPUTER CODE
- MULTI-SIGNATURES: GOOD USE CASE
- DELEGATION: NUANCED SET OF RULES - WE WANT TO PUT THIS IN AS LOGIC
- DEBATE ON HOW TO IMPLEMENT, BUT PUB KEY ⇒ VALIDATION FUNCTION → TAKES CONTEXT & 'WITNESS' (DATA) ⇒ HASH THIS TOGETHER TO CHECK KEY/SIGNATURES
- DELEGRATION: 'WITNESS' IS BUILT INTO CODE - SIGNATURE ENCOMPASSES THIS..
- VERIFICATION = HARD TO HANDLE
- NEXT STEPS: WRITE CODE & SEE WHAT FAILS (MULTI-SIGNATURE) = OBVIOUS NEED ...

'OUR SUCCESS BY

① JUNE 2016
PGP 25th AN.

WOT VISION ST

CREAT PITCH

ORK BACK
OM THIS DATE

PRIL MAY ↓↓↓
JUNE '16.

CONTRIBUTIONS
"WHAT WOULD MAKE YOU FEEL THAT 'WE' WERE SUCCESSFUL.

By June 2016:
At least two people funded to work on IETF DPKI spec.

2016
Publication Restating the Need for web of trust

"NEED FOR WOT" PUB'S

DISTRIBUTED PKI.

SAMPLE APP

ACCOMPLISH:
Have some sample app that doesn't have to be perfect, but actually works and shows to end users how the new WoT can work.

[By PGP 25th]
Distributed Key Registry with Protocols Operational + Well-Used

DISTRIBUTED KEYS REGISTERY"

BASIC REFUGEE APP

IETF-2 FUNDED

DECENTRALIZED 'WANTS' VOTING

1 POC

Open for (Blockchain Bitcoin ID)
1. Signatures of People
Wanking to see their built WoT

DPKI spec + distributed regist IMPLEMENTED

① (a great) SHIP DPKI (after reviewing Literature)

Define Great Use Cases for WoT Identity Not well served by current methods + build one PoC

5 BUS. CASES OPEN SOURCE MVP'S

Revolution in USABILITY!!
This is essential and Requires Resources
it is taken srsly not forgotten

1) Something usable with growing user-base
USABLE

Well designed, usable, OPEN Source MVPs of the 5 use cases

# NEXT EVENT. IDEAS

(2)

DESIGN SHOP
HAKKERTHON
ETC

WOT PLUS"

A Web of — definition for gathering real world information that are verified by a trust network

Digital Hackathon for Web of trust plus

Remote Hackathon

to expand on the meaning of WOT

Next Event:
Fundraiser to raise $$ to implement ideas

Form small groups to finish what we started here.

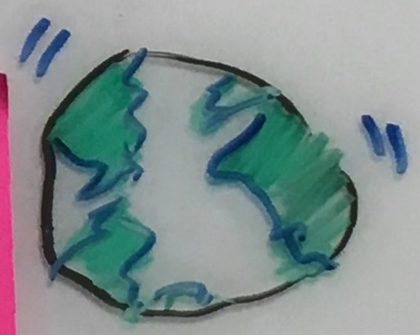
FINISH IT

(2) Workshop Focus on designing specific systems focusing on UX.

UX FOCUS

Design Shop Focused on Chosen Use Cases

RWOT PGP 25th Anniv. Global Signing PARTY



Piggy back on IIW #22 to get work done & move forward

HARDWARE FOCUSED HACKATHON / WKSHP FOR PKI + SELF SOVEREIGN ID

H/WARE
PKI +
SELF SOVEREIGN ID.

Compelling EXPERIENCE USE CASE

# IDEAS FOR FUNDING OUR WORK/SHOPS GOING FORWARD

3

RESOURCING ETC.

FIND $ WHO ARE SUFFERING FROM WOT ISSUES

OPEN SOURCE STARTUPS.

VCs who are investing in blockchain startups — form consortium to fund open source open standards that startups will all benefit from

3 COMMIT TO STARTING AN INVESTMENT COMMITTE FOR POTENTIAL PIPELINE, CONSORTIUM.

SOCIAL INNOVATION FUNDS — 'WE ARE THE-C

'INDEPENDENT AUDITS'

(INDEPENDENT) AUDITS!!11!

"PAY FOR ATTENDENCE! — BOOTH"

EUROPEAN DARPA COMMISSION

$

If you com to the event to talk about your startup, you have to either pay a registration fee or leave.

RESPECT NETWORK will PLEDGE funding for future RWOT events

3 European. DARPA / Relevant. European Commission

Willing to use social capital/network to bring diverse ppl (women POC etc) to a gathering that is practively designed to include & not alienate them + move it forward

WRITE GRANT PROPOSALS.