



Blockchain technologies drive better security solutions

Journée Blockchain SIF
November 2016

Nicolas Bacca
@btchip

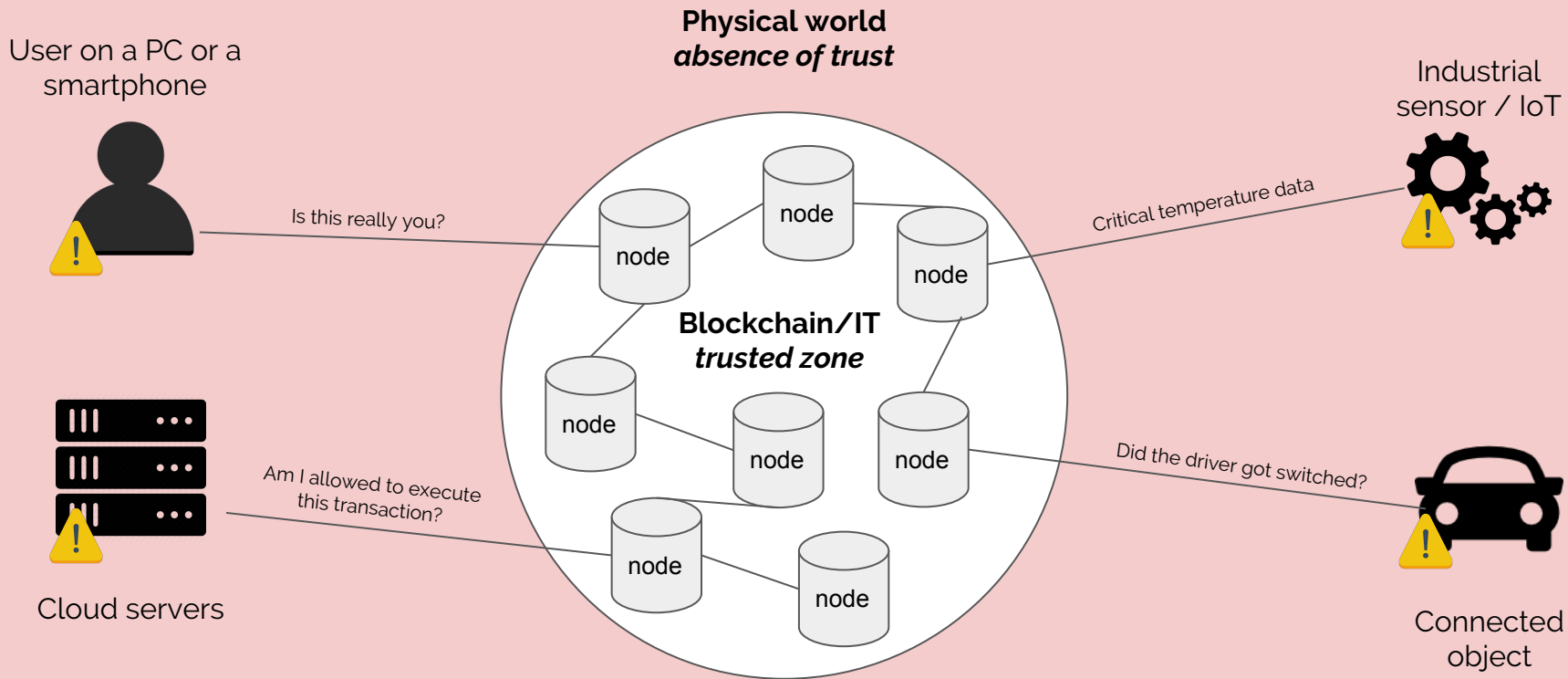
LEDGER TECHNOLOGY

A trust layer between the **blockchain**
and the **physical world**

For industrials, enterprises and consumers

Securing the first and last mile

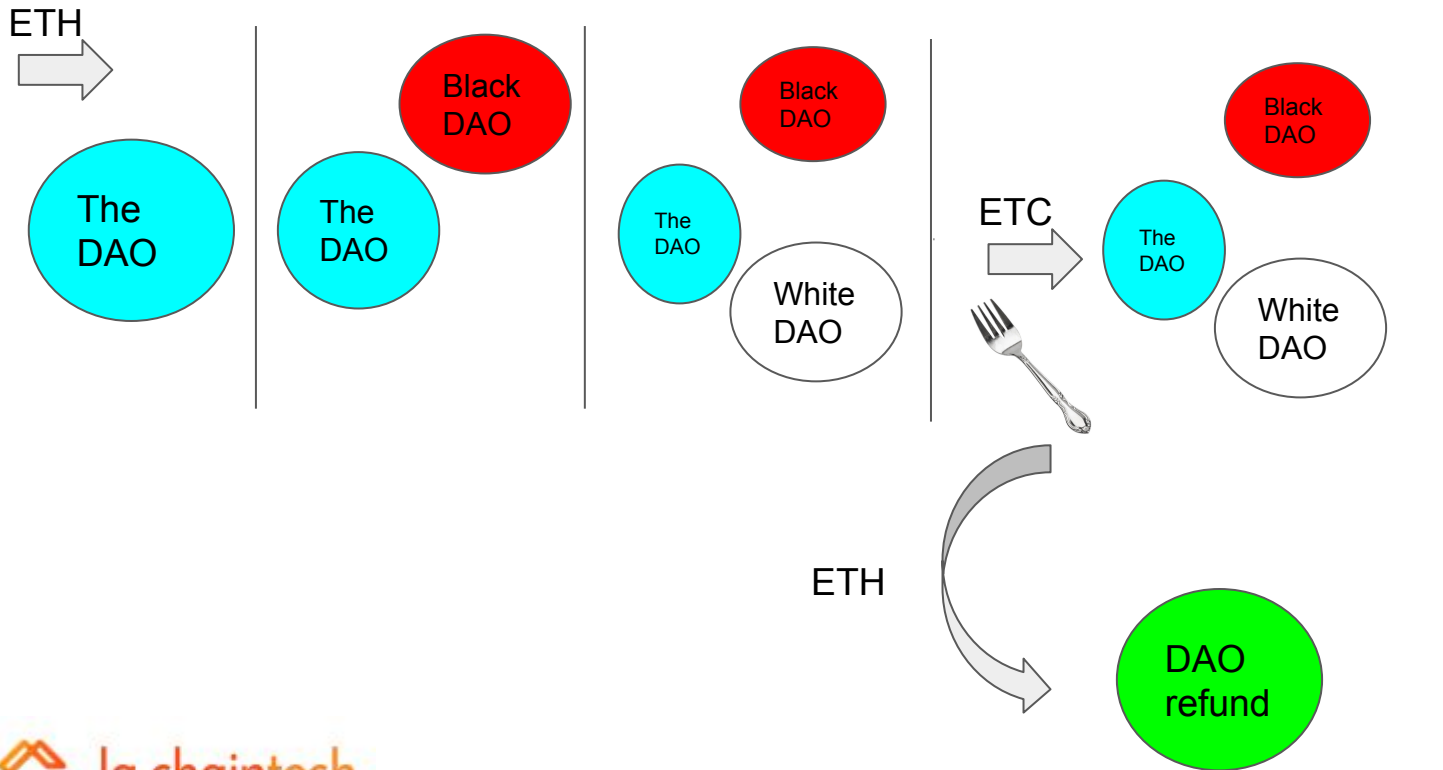
Without **trust**, data has no actionable **value**



Why ? Cryptocurrencies come with built-in bug bounties

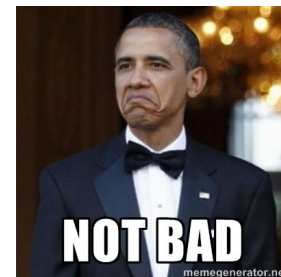


The DAO timeline



Creation of a new currency

Hacker exit



Aligned with the latest identity standards

Reducing dependencies on non deterministic events (randomness ...)

Solving the user keyring problem

Innovating with internet-ready security devices

The password is dead



REUSED



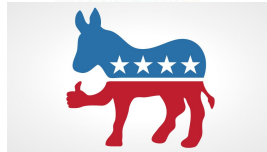
PHISHED



INTERCEPTED



KEYLOGGED



How can it be replaced ?

Hardware based cryptographic authentication for the webs

FIDO set of standards

Minimalist cryptography (one size fits all)

Multiple vendors

Slow but large traction (Google, Github)

The building block of modern security devices



Hard (impossible) to fully get rid of randomness

Generating unbiased randomness is a hard problem

Proving that randomness is unbiased is an even harder problem

Modern cryptographic algorithms are brittle, making it an easy attack vector

No evil, omnipotent wizards

Have a lot of time

Have a lot of resources (crunching weak randoms is easy, see Logjam)

Can interfere with standards (see DUAL_EC_DRBG)

Attacks on randomness provides good plausible deniability



Recognize the problem : make it easier to evaluate

Only depend on it when it's absolutely necessary (key generation)

Promote deterministic signatures (ECDSA / RFC 6979)

Avoid catastrophic algorithm failure on signature (see PS3 27C3)



An unfortunate side effect of non deterministic code

Predict code parameters (such as private keys) given external events

Extremely powerful and not taken care of enough (see “CSI meets public wifi”)

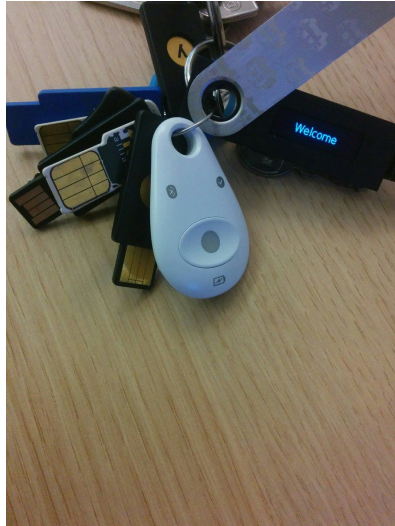
Important work being done by the community on Bitcoin curve with libsecp256k1

The user keyring problem

Too many keys, too many protocols

Hard to backup (additional weakness / hard to remember)

Too many devices



Deriving keys from a master key (BIP 32, Hierarchical Deterministic Wallets)

Using a nice property of Elliptic Curve keys

$$\text{Public}(\text{PrivateK} + (\%n)\text{Scalar}) = \text{PublicK} + (\text{point})\text{Scalar} * \text{Generator}$$

Can be extended/abused to RSA (find next prime ...)

Providing an easy way to remember the master key (BIP 39, Mnemonic Phrase)

Turning entropy into words, not the other way round (see Brainflyer)

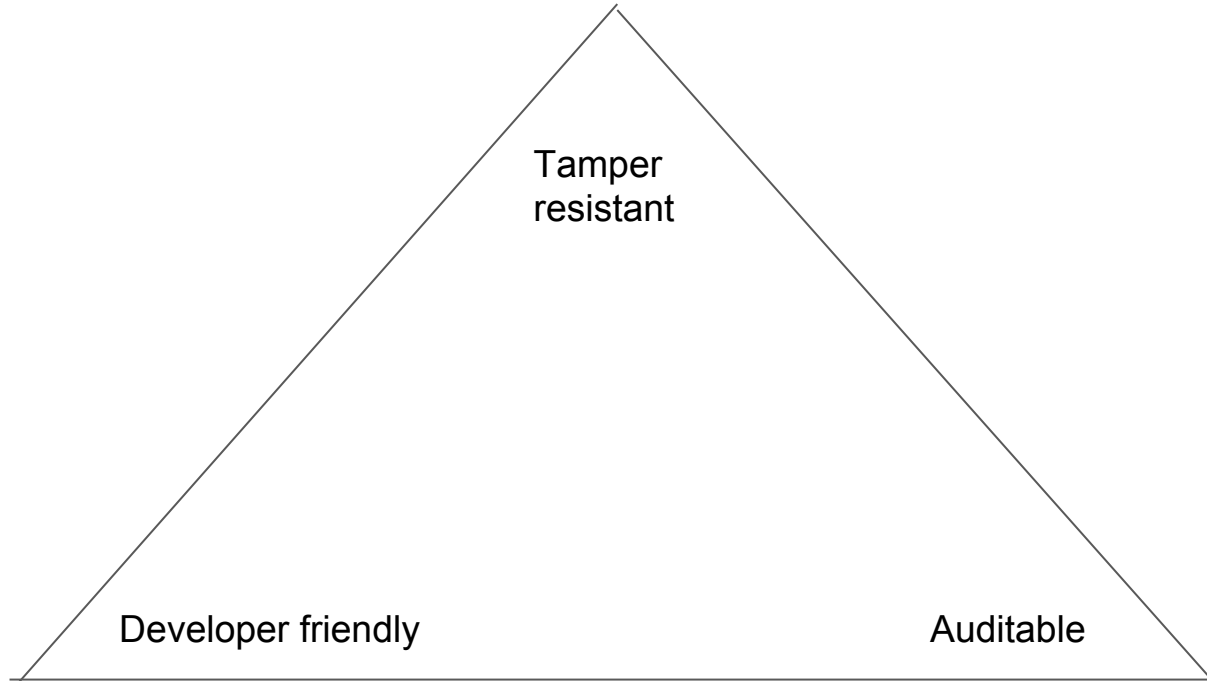
Why the Smartcard has to be reinvented

Not web-ready : designed to work in a trusted environment

Not user friendly (reader, drivers, middlewares)

Not developer friendly (Java Card if lucky)

Not customer audit friendly



What has been accomplished so far




Multiple devices with different tamper resistance properties

Web integration, reusing FIDO work on U2F (Ledger with MyEtherWallet)

Web ready : malware resistant

<Ad> New paradigms for native multi application platforms </Ad>

The exhaustive list of Blockchain security standards

 la chaintech <- (is not a security standard)

Moves at startup speed (ETH from EAL0 to EAL7 in 6 months, according to ETH)

Is battlefield tested (or assets are lost very quickly)

Bitcoin is a pretty good canary (see “Some SecureRandom thoughts” on Android)

Is interesting to look at for the general security / identity industry

On the other hand can also learn a lot from those industries wrt testing / evaluation



Thank you
@btchip