DOUBLE CHAIN

Trend of Entity Authentication for Finance services

2017.12.12

randyjeon@doublechain.co.kr

DOUBLE CHAIN

Contents

Anti-money laundering

- **Know your customer** (**KYC**) is the process of a business identifying and verifying the identity of its clients.

- used to refer to the bank and anti-money laundering regulations which governs these activities.

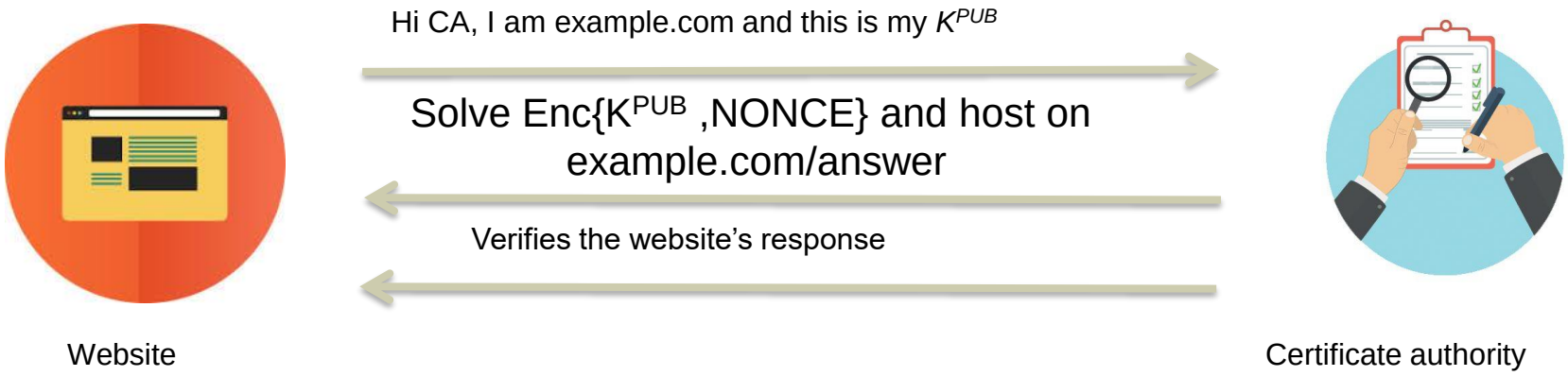
- Know your customer processes are also employed by companies of all sizes for the purpose of ensuring their proposed agents, consultants, or distributors are anti-bribery compliant. Banks, insurers and export creditors are increasingly demanding that customers provide detailed anti-corruptiondue diligence information.

- **ISO 37001:2016**
  - Anti-bribery management systems – Requirements with guidance for use

Current Public-key Infrastructure

DOUBLE CHAIN

- Public keys are needed to authenticate the web-server in TLS (HTTPS)
- How do we know what is the public key of a server?
  - “Certificate Authorities” to the rescue
  - Browsers trust some CA intrinsically
  - CA in turn perform check and issue X.509 certs to domains
- Domain validation is completely automated and instantenous



Why the current PKI has a problem?

DOUBLE CHAIN

- Reliance on a trusted CA can be a problem
  - Turn rogue
  - Can be hacked
  - Can make mistakes
  - Little transparency

- Breach of a single CA threatens the entire WWW
  - Any CA can issue certificate for any website in the world!

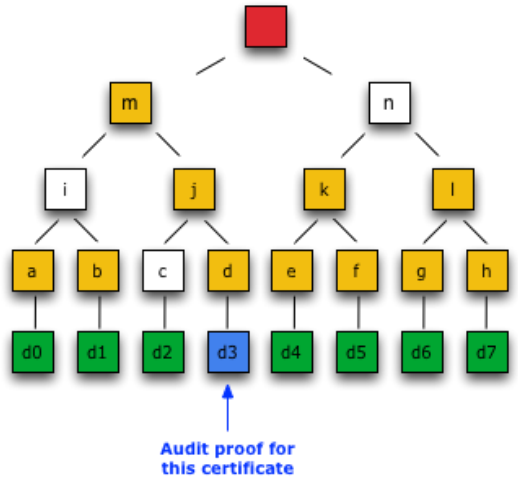
- Certificate transparency logs all public certificates on an immutable, append-only log
  - Kind of looks like a blockchain already

- But it's not distributed! Must trust Google or other CT log operators

Why Distributed ledgers(DLT) for PKI

DOUBLE CHAIN

- PKI is simply a consensus on domain-name::public-key mapping
  - Mapping can be distributed
  - Perspective or PGP's web-of-trust
  - Domain-validation method is fully-automated and instantaneous
  - Distributed nodes might make MITM and BGP hijacks even harder
- Public ledgers of certificates are already maintained for transparency
  - Certificate transparency is now mandatory
  - CA must log the cert
  - Cryptographic proofs that cert exists in the log (Merkle Trees)
- Financial incentives exists and are probably necessary
  - Major domains pay substantial amount for extended validation
  - Free certificates have been found to be abused by Malware/Phishing domains



Let's Encrypt has issued 15,000 SSL certificates to PayPal phishing sites

Security experts call on firm to refuse certificates for domains containing popular brand names

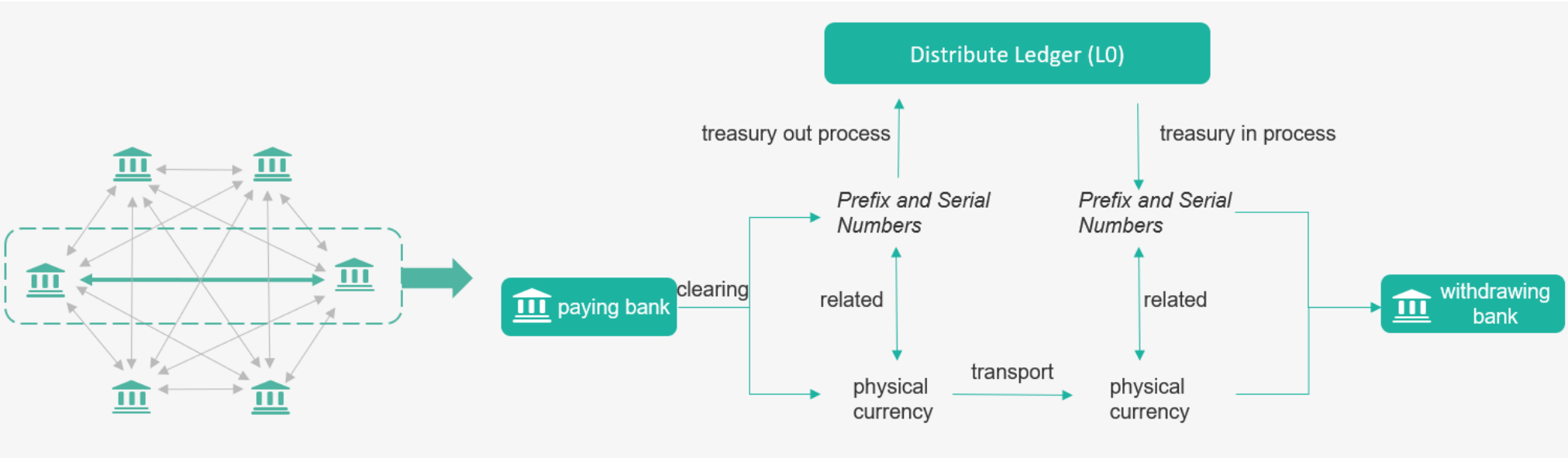
Existing solutions

DOUBLE CHAIN

- Namecoin
  - One can register a new domain name on the blockchain with its public key
  - More like certificate transparency
  - If I register Symantec.com, how does Symantec get its name back?
- Instant-Karma PKI
  - A smart contract between domain and CA about financial liability
  - Financial incentives for miners to find abuse/mis-issuance
  - Supports the CA system, instead of replacing it
- Lot of open questions like validation, revocation etc. but this is an important use case
- X.509 is already an ITU standard!
  - ITU should think about a new standardized PKI? (currently under CA-Browser forum)
  - Standardization questions: Level of proof? Crypto? Consensus algorithm?

Cross-bank transfer system

- Minimalist Model



ITU-T Focus Group FG DFS (Digital Financial Services)

DOUBLE CHAIN

- FG DFS - INTEROPERABILITY
  - Interoperability enables users worldwide to make electronic payment transactions with any other user in a convenient, affordable, fast, seamless and secure way – via a single transaction account.

- Regulations for Mobile Money
  - Mobile Money-Specific Guidelines and Regulations
  - Basic Characteristics of Regulations (Regulation, Law, Directive, Guidelines, Circular)
  - Operational Models: Bank-based vs Non-bank-based
  - Regulatory Safeguards, Agents

- Interoperability for Mobile Money
  - Types of Interoperability Regulations
  - Existing Interoperable Mobile Money Payment Schemes
  - Comparing Regulation and Market Types for Interoperable Mobile Money Schemes

ITU-T Focus Group FG DFC
(Digital Currency including Digital Fiat Currency)

DOUBLE CHAIN

- Main Objectives
  - Study the economic benefit and impact of introducing DFC over mobile money;
  - Investigate the ecosystem of digital fiat currency implementation for financial inclusion;
  - Map the functional network reference architecture and process components required to implement digital fiat currency and integration with existing payment systems for interoperability;
  - Identify use cases, requirements and applications of digital fiat currency;
  - Develop better understanding of the security, regulatory implications, consumer protection, fraud prevention and counterfeiting issues of DFS and how can digital fiat currency can address these concerns;
  - Identify critical sovereign security, transparency and verifiability of DFC technology and provide guidelines towards the escrow of critical software and hardware components to ensure trust and verifiability; and
  - Identify new areas for standardization in ITU-T study groups.

ITU-T Focus Group FG DFC
(Digital Currency including Digital Fiat Currency)

DOUBLE CHAIN

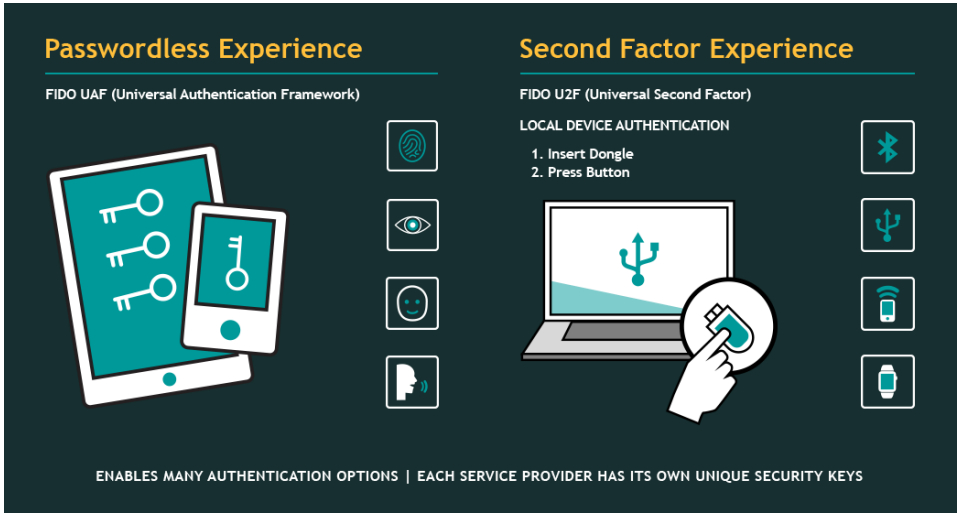
- Stakeholders
  - Central Banks
  - Telecom regulatory authorities
  - Financial service providers
  - Fintech Community
  - Payment Service Providers
  - Standard Setting Bodies
  - Academia

FIDO Alliance

DOUBLE CHAIN

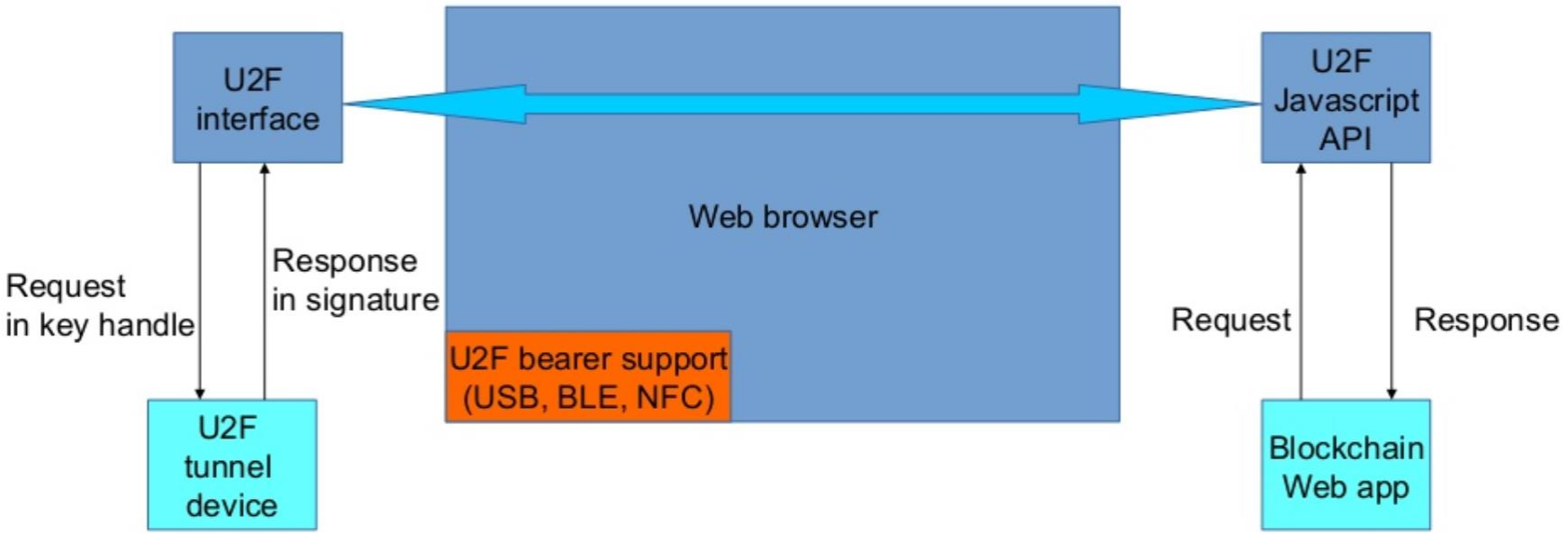
- Fido : Better identity, using strong cryptography
  - blockchain applications better trust, suing string cryptography
  - foundations of innovative privacy aware, user centric application relying on strong cryptography
  - Private keys are the corner stone of Blockchain application

- Asset ownership is linked to the ownership of private keys for all blockchains
  - Need for innovative solutions to create better backup schemes
  - Need to protect the user against malware



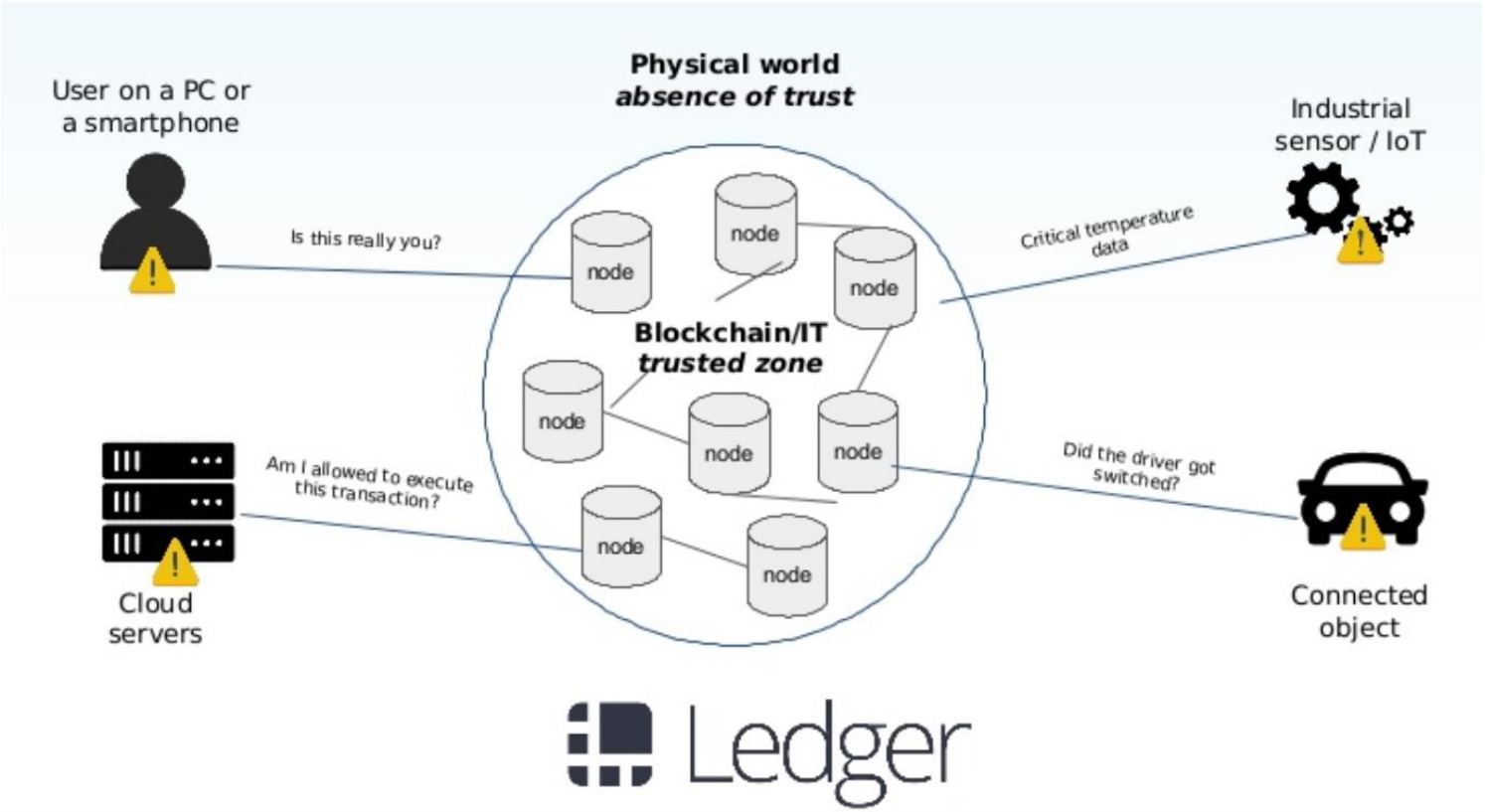
FIDO – Authentication

- U2F(Universal 2nd Factor Authentication)



FIDO with DLT

- Without trust, data has no actionable value



Combination of authentication method

DOUBLE CHAIN

- Conventional method
  - KYC (Know Your Customer)
  - PKI (Public Key Infrastructure)
  - OTP (One Time Passwords)
  - Biometrics
- DLT(Distributed ledgers Technologies) + PKI
- FIDO(Bio) + Blockchain (DLT)
- PKI+ FIDO(Bio) + Blockchain (DLT)


Thank you