Preamble

"I guess I need a blockchain right now"
The blockchain is really:

- interoperable
- permissionless
- borderless

at a cost.. complexity!

SMART FLIGHT INSURANCE

InsurETH

Winning project @ London Fintech Week Hackathon 2015
InsurETH - Insure your flight with Ethereum

InsurETH lets you insure your flight directly with an Ethereum smart contract.

- Total insurance: 1
- Active insurance: 0
- Total investors: 1
- Investment ratio: 100%

Invest into an automated flight insurance service

Deinvest all your investments into this contract

Flight Delays Suck!
You’ll love to be late! Get your instant payout in case your flight is late.

https://fdd.etherisc.com/
Cash on delivery

StackExchange
- no need for any human intermediary
- inherently p2p
- set of actions -> trigger payments
- strong transparency need (prone to corruptions)
Smart contracts!

- self-encourging logic [protocol level]
- trust-less [no intermediary]
- cheap [network fees only]
- transparent & immutable
DATA is the escrow!

Bringing data to blockchain is HARD!
Oracles...

(Our) definitions

- data-source - Augur, Bloomberg, Blockchain, WolframAlpha, the Web?
- query - a formula the data-source can understand
- oracle - the party in charge of connecting you to the data-source
Oraclize provides a connection between online data feeds / APIs and your Ethereum smart contract using cryptographic technique to prove the authenticity of data.

- 160K+ txs sent to the public Ethereum network since Sept 2015
- most widely used oracle system
- on-demand data = blockchain is not being spammed!
Network monitor

Ethereum Node
- Connected to IFS node
- Oracle Public Node - Verified
- 2165 KBytes

IFS
- Downloading file C:\Users\User\Documents\test.txt
- 2145 KBytes
- Connected to IFS node: 44.173.197.89

TLSkitty
- Verifying proof 79.30.143.18, 205.132.174.
- 4000 KBytes

Oracle honesty: Verified

Graph showing network activity and connectivity.
Attestation-as-a-service

- no tampering is possible on the oracle side
- neither the attester nor the datasource need to be blockchain-aware
- trust shifting from the oracle to a (semi-)trusted attester
  
- more attestors the better (how many funds do we want to secure?)
- very unlikely to have all attestors tampering with data
  
  (at the exact same time and in the exact same way)

  Assumption: few semi-trusted attestors >> many non-trusted oracle players

- very generic & flexible API
- provides automatic access to blockchain-agnostic datasources
- blockchain-aware integrations (Bitcoin, Ethereum, RSK.. & REST!)
- defining an open std for oracle comms!

Still.. not censorship resistant & no reponse guarantee
// Ethereum + Solidity
// This code sample & more @ dev.oraclize.it
import "github.com/oraclize/ethereum-api/oraclizeAPI.sol";

contract PriceFeed is usingOraclize {
  uint public ETHER;

  function PriceFeed() {
    oraclize_setProof(proofType/frontend | proofStorage_IPFS);
    update(0); // first check at contract creation
  }

  function callback(bytes32 myid, string result, bytes proof) {
    if (msg.sender != oraclize_cbAddress()) throw;
    ETHER = parseInt(result, 2); // save it as $ cents
    // do something with ETHER
    //update(60); // recursive update disabled
  }

  function update(uint delay) {
    oraclize_query(delay, "URL",
                   ":3000/price?fsym=ETH&tym=USD&ago=5min"));
  }
}
Estonian e-residency digital ID card

~12,000 e-residents across the world
Global: 25%+ outside Europe!

easy online registration + collect card at local embassy
open standard, RSA signatures (smart contracts can verify them!)

The elegant solution to the "identity problem" (KYC, voting, wallets, ..)
"Proof-of-identity" project

A single set of infrastructure services providing e-residency aware features to any blockchain service/app

Received a $30k grant from Wanxiang BlockGrantX #4

https://github.com/oraclize/dapp-proof-of-identity

Ethereum address <-> E-residency identity (serialNumber)
Is that e-residency identity certificate still valid?

Problem: Certificate Revocation List lives offchain
Solution: Oraclize can be used as a connector (smartcontract <-> CRL)

Easily check an Estonian digi-id certificate

winning project at the London Fintech Week Hackathon 2016
Banks 2.0

will NOT be custodians but FACILITATORS

(you stay in control of your funds)
be - your own bank

This Bank 2.0 model is the daily interface you use to interact with your funds.

Today: facilitates access to your ID-controlled Blockchain-based Wallet

Tomorrow: loans, other off-chain financial services, ..

Summary/take home:

- blockchain is not a good fit for everything
- real-world apps need reliable data via oracles
- huge value in on-chain interoperability
- blockchain enables banks to be facilitators only
- the e-residency card is a good solution for the identity problem (open standards are good!)
Questions?

Dev center @ dev.oraclize.it

Twitter @OraclizeIT

Thomas Bertani