Privacy on a Blockchain

Cees van Wijk

Blockchain innovation week

ING


2020


GUARANTEED
Your Recipe

EXPLORE DECENTRALIZED APPLICATIONS

Discover the possibilities of the Ethereum blockchain with the definitive registry of ĐApp projects. Learn more about ĐApps

Browse the ĐApps | Submit a ĐApp

Upcoming events

Apr 17 – FilmTech Meetup #9 **Apr 19** – Synchronize 2018 **Apr 24** – Oslo Blockchain Day **Apr 26** – Blo

View all events | Submit an event

Featured ĐApps

View all >

Decentraland
A virtual world run on open standards

Axie Infinity
Collect and raise fantasy creatures

Userfeeds
Content ranking system for communities

Sponsored With

Ramen Coin

The FIRST and ONLY Proof of Ramen Cryptocurrency. Play our ETH dApp!
http://ramencoin.me

Collections

Hottest

View all >

Staticoin
The stablecoin solution for traders and

BetĐapp
Parimutuel sports betting platform

Kript
Mobile App for crypto investment

CCCoin
Image creation, curation, and sharing

Donamin
Conscious dealmarket with online marketing

MetaGame
Own and trade your favorite Dapps

2

ING

Pilots & live trades

HOLLAND FINTECH

HOME ABOUT US MEMBERSHIP OUR NETWORK INSIGHTS EVENTS MORE

ING BANK

ING releases blockchain solution: zero-knowledge proof

November 21, 2017 / In Insights, Member News, News

During the first Enterprise Ethereum Alliance Event, I Knowledge Range Proof solution. This solution should solv use of blockchain by offering data privacy protection.

Search for ...

Newsletter Sign-Up

Latest

22 European states commit to blockchain development
April 16, 2018

Accenture to open its Asia-Pacific FinTech Innovation Lab 2018
April 13, 2018

GSMA launches global mobile money certification scheme

EMERCE BLOCKCHAIN

HOME / BLOCKCHAIN / ING WIL MEER DOEN MET BLOCKCHAIN

Redactie Emerce
NIEUWS - 31 januari 2018 - 08:53

ING wil meer doen met blockchain

ING wil zich de komende tijd vooral bezighouden met blockchaintechnologie. Dat zegt CEO Ralph Hamers in een toelichting op de jaarcijfers.

Door innovaties verandert het bankieren razendsnel. Blockchain kan een grondige verschuiving teweegbrengen in de financiële dienstverlening, zegt Hamers

De Telegraaf NIEUWS SPORT ENTERTAINMENT FINANCIEEL MEER

ING en ABN laaiend enthousiast over sojatest met blockchain

Door RUBEN EG
22 jan. 2018 in FINANCIEEL

AMSTERDAM - De komst van blockchain als nieuwe ruggengraat van de financiële wereld komt naderbij met een geslaagde proef van ING en ABN Amro met een 'complexe' sojatransactie.

www.businessinsider.com/ing-seeks-to-make-blockchain-tech-more-usable-2017-11?international=true&r=US&IR=T

BUSINESS INSIDER TECH FINANCE POLITICS STRATEGY LIFE ALL

ING seeks to make blockchain tech more usable

Maria Terekhova
Nov. 17, 2017, 9:30 AM 778

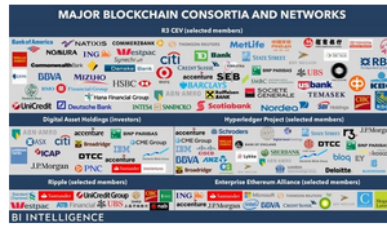
BUSINESS INSIDER TECH FINANCE POLITICS STRATEGY LIFE ALL

ING and Credit Suisse make blockchain progress

ger
018, 10:18 AM 1,960

FACEBOOK LINKEDIN TWITTER EMAIL

This story was delivered to BI Intelligence "Fintech Briefing" subscribers. To learn more and subscribe, please click here.



BI Intelligence

Credit Suisse and ING Group have completed the first live securities lending transaction together with fintech innovator HQLA-X. The project commenced in April 2017 and also includes CIBC, Commerzbank, and UBS.

ING

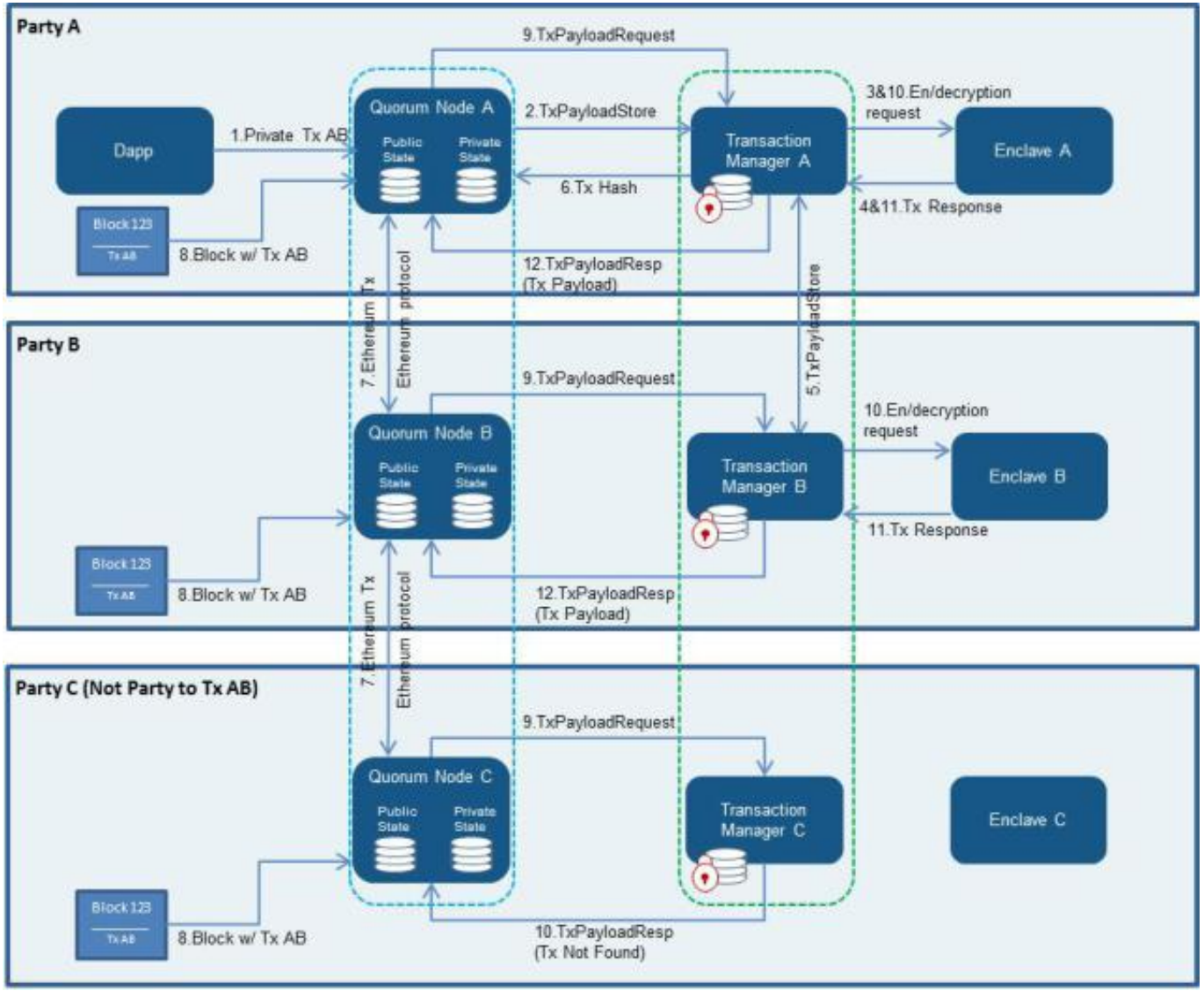
2 major challenges:

1. Privacy
2. Scalability

Privacy solutions

- Selective transaction sharing (Channels, private transactions etc.)
- Intel SGX
- Cryptography:
  - Homomorphic encryption
  - Ring signatures
  - Zero Knowledge Proofs

Quorum: only store a hash on the blockchain



Quorum: private tx

```
contract Calculator {

    uint counter = 0;

    function increment() {
        counter++;
    }
}
```

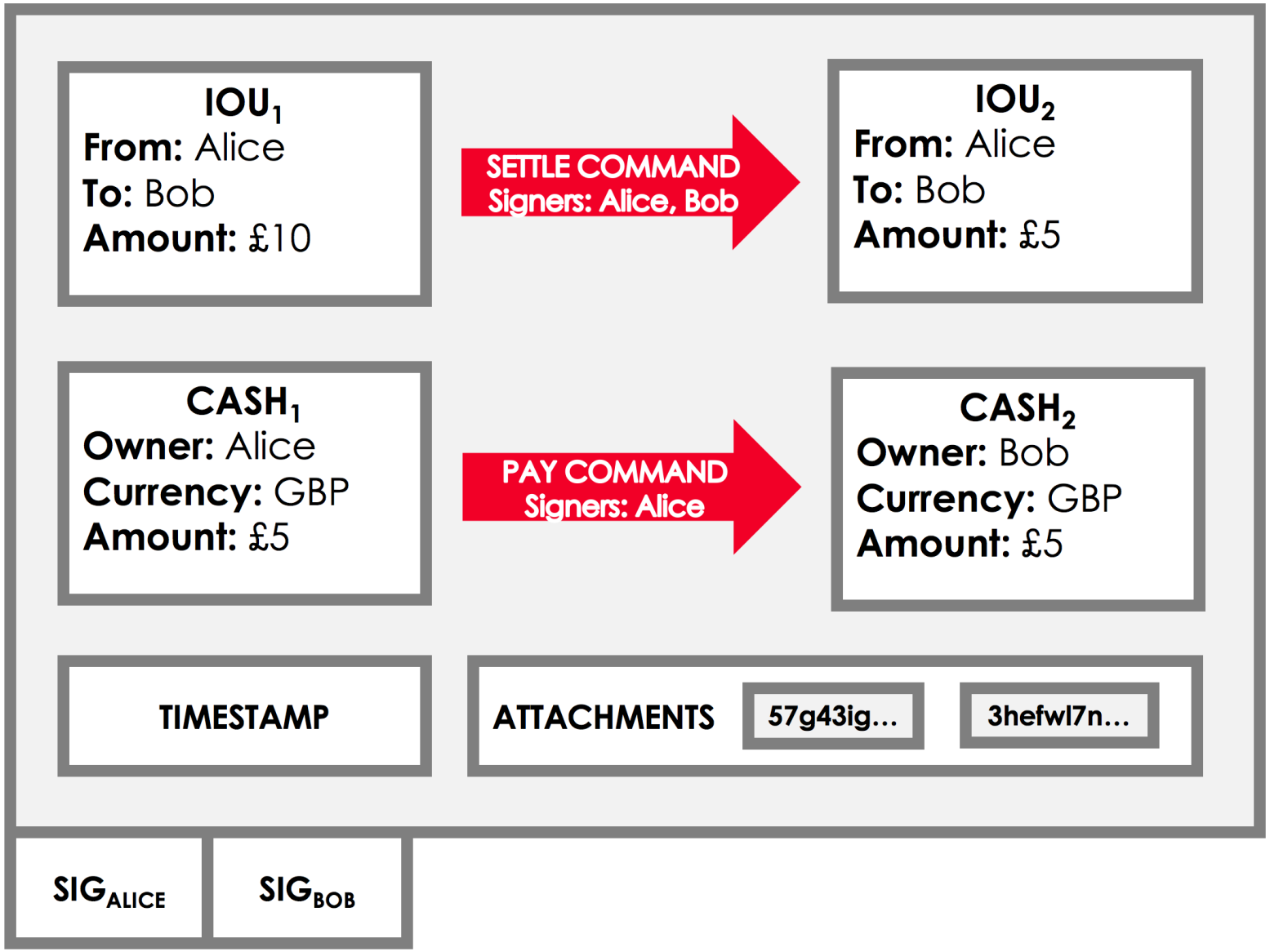
	Node1	Node2	Node3	Node4	Node5	Node6	Node7
Tx1 privateFor all	1	1	1	1	1	1	1
Tx2 privateFor Node1, Node2	2	2	1	1	1	1	1
Tx3 privateFor Node3, Node4, Node5	2	2	2	2	2	1	1
Tx4 privateFor node1, Node4	3	2	2	3	2	1	1
Tx5 privateFor Node5, Node7	3	2	2	3	3	1	2
Tx6 privateFor All	4	3	3	4	4	2	3
Tx7 public	4	3	3	4	4	2	3

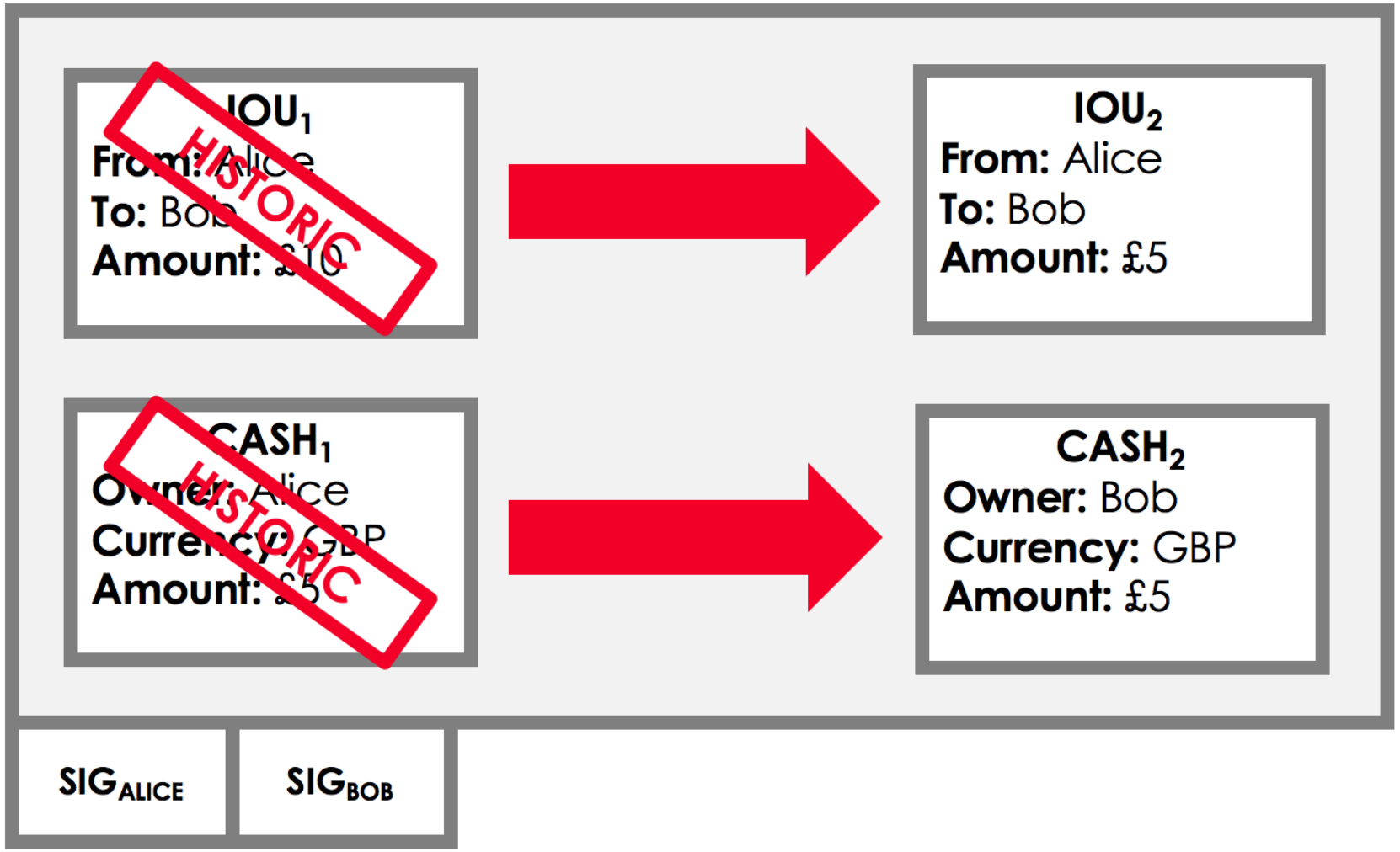
ING

UTXO in BitCoin

1	**Inputs: empty** **Outputs: 12,5 → Raoul**	**SIGNED(Trader**
2	**Inputs: 1[0]** **Outputs: 10 → Cees, → 2,5 Raoul**	**SIGNED(Raoul)**
3	**Inputs: 2[0]** **Outputs: 4 → Mark, → 6 Cees**	**SIGNED(Cees)**
4	**Inputs: 2[1]** **Outputs: 1,5 → Mark, → 1 Raoul**	**SIGNED(Raoul)**

(Simplified version of actual system functions)


IOU1
From: Alice
To: Bob
Amount: £10
SETTLE COMMAND
Signers: Alice, Bob
IOU2
From: Alice
To: Bob
Amount: £5
CASH1
Owner: Alice
Currency: GBP
Amount: £5
PAY COMMAND
Signers: Alice
CASH2
Owner: Bob
Currency: GBP
Amount: £5
TIMESTAMP
ATTACHMENTS
57g43ig…
3hefwl7n…
SIGALICE
SIGBOB

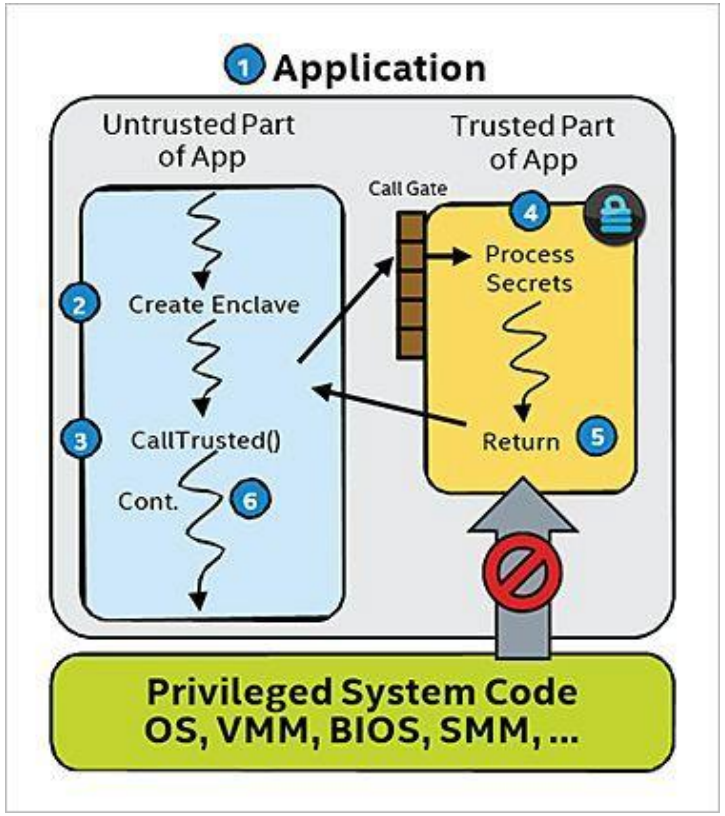

IOU1
From: Alice
To: Bob
Amount: £10
HISTORIC
IOU2
From: Alice
To: Bob
Amount: £5
CASH1
Owner: Alice
Currency: GBP
Amount: £5
HISTORIC
CASH2
Owner: Bob
Currency: GBP
Amount: £5
SIGALICE
SIGBOB

Intel® Software Guard Extensions (Intel® SGX)

Problem: Corda verifies transaction chains. This potentially conflicts with privacy.

Solution: Run verification in SGX enclave.

SGX concerns: special hardware, vendor lock-in, key management, side channels



SPECTRE

MELTDOWN

ING

GitHub, Inc. (US) | https://github.com/lsds/spectre-attack-sgx

spectre-attack-sgx

Sample code demonstrating a Spectre-like attack against an Intel SGX enclave.

Overview

Given our ongoing research on Intel SGX here in the LSDS group at Imperial College London, a question that occurred to us immediately on first hearing of the recent Meltdown and Spectre attacks is *what are the security implications of speculative execution side channels for Intel SGX enclaves*?

This repository contains a proof-of-concept attack (`SGXSpectre`) showing it is indeed possible to use a speculative execution side-channel to leak data from an Intel SGX enclave.

Attack Outline

The attack is similar conceptually to the conditional branch misprediction Spectre attack of Kocher et al. The main difference is that we move the secret data (`secret`) and the victim function (`victim_function`) and overflow array (`array1`) inside the enclave. The attacker executes `victim_function` using an ecall, passing it the index `x` used to index into `array1` .

Code Layout

- `SGXSpectre/main/main.c` : Contains the untrusted code to create the enclave and mount the SGXSpectre attack.
- `SGXSpectre/enclave/enclave_attack.c` : Contains the enclave secret data and victim function.

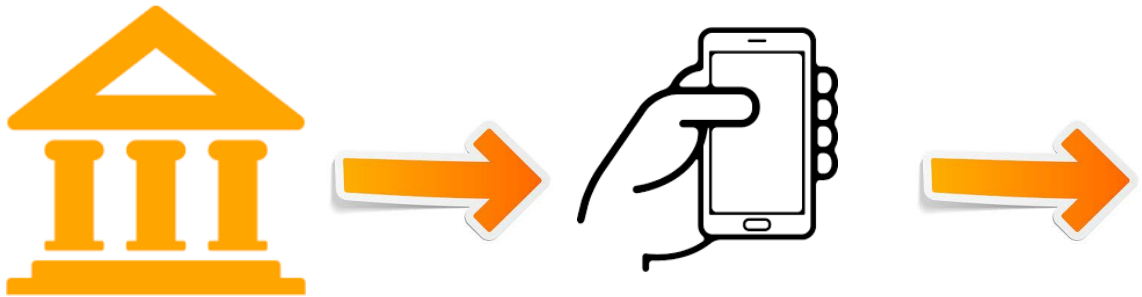
ING

Zero Knowledge range proofs

Intro

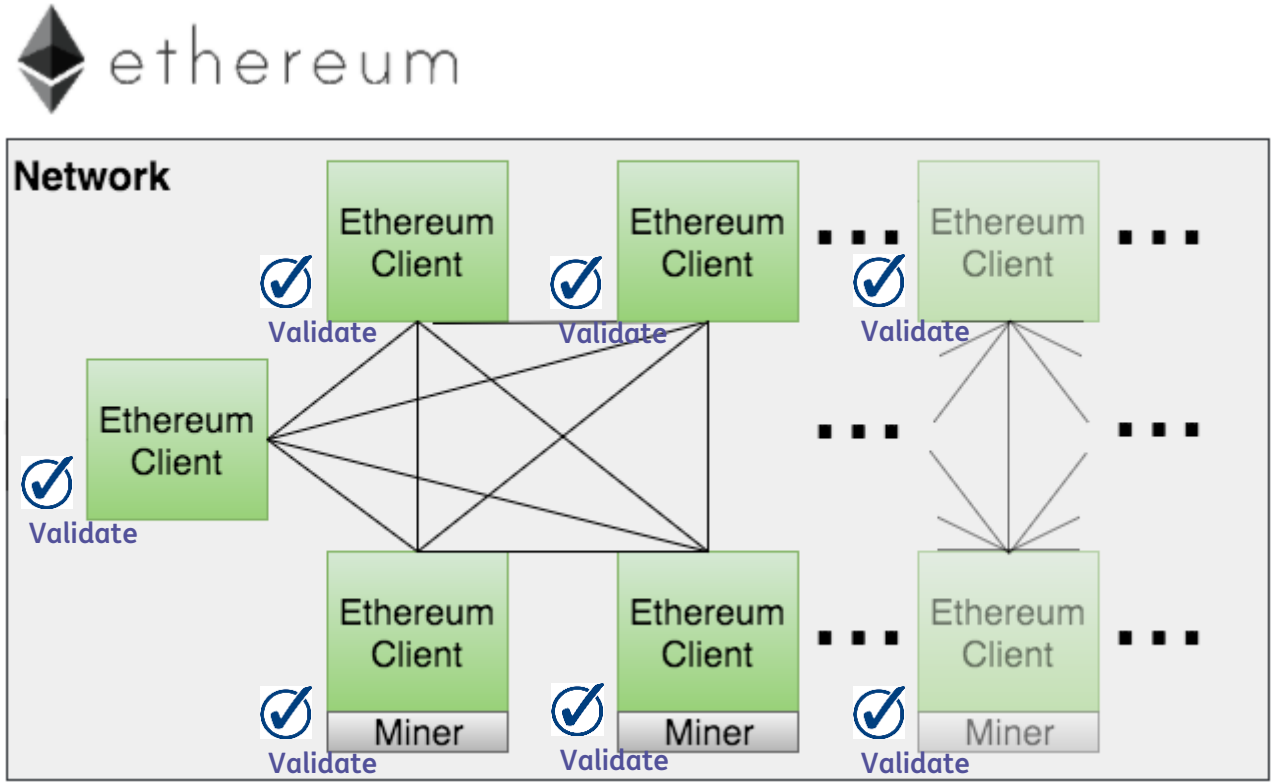
- ING Built a pre-compiled contract in Go-Ethereum that allows the entire network to verify that a secret number is in a known range.

- For example validate a:
  - Proof of age
  - Proof of salary bandwidth
  - Proof of location
  - Proof that a payment is within limits



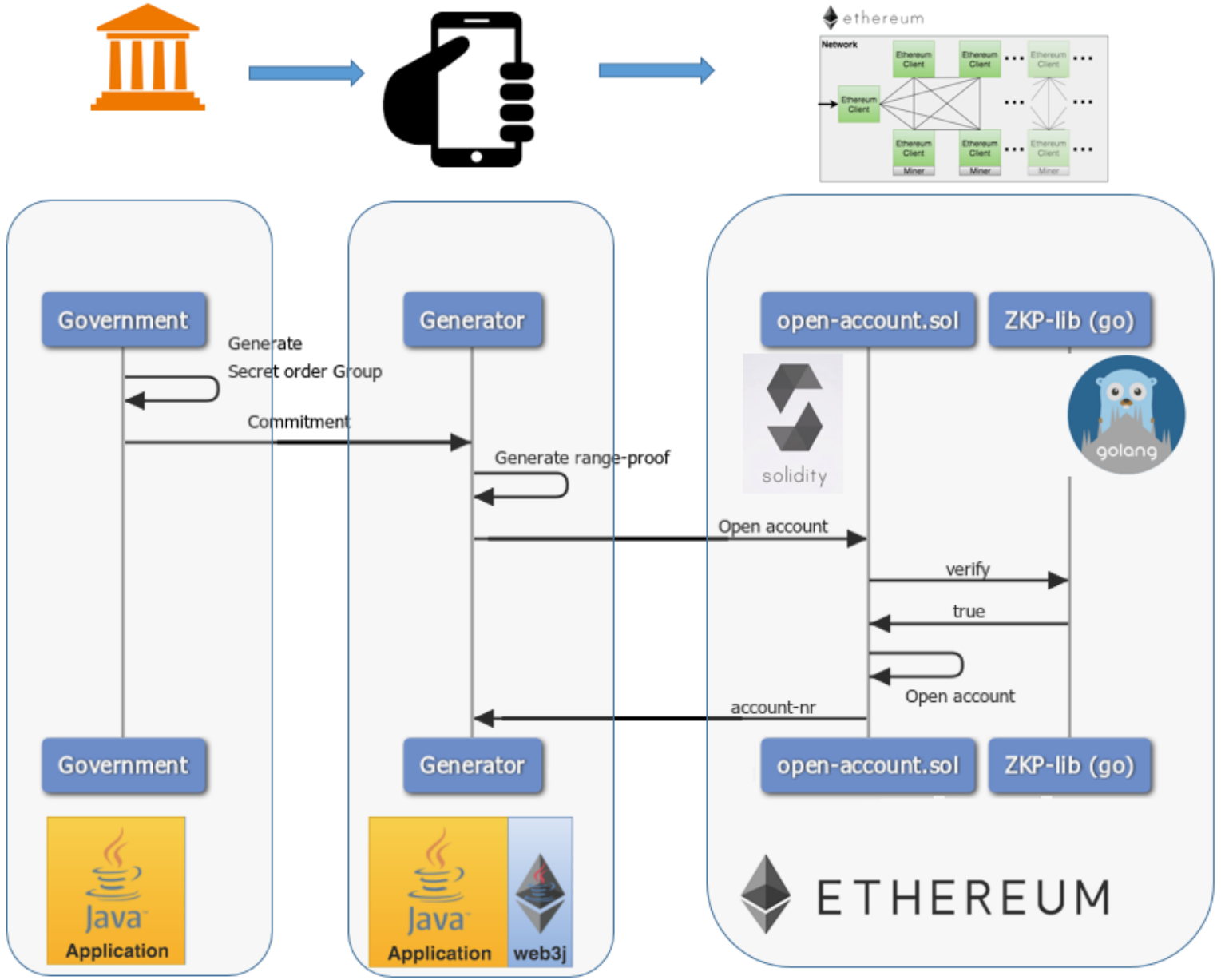
Provide commitment

Create range-proof



Pre-compiled contract

- Running native go is faster than running Solidity in the EVM
- Less gas consumption (than running in Solidity)
- The proof uses very large numbers (larger than int256)




Vitalik "Not giving awa...
@VitalikButerin
Follow
Range proofs for ethereum using RSA multiplicative groups and a clever "prove a number is positive by giving its square root" protocol:
Blockchain transactions just got a whole lot safer
ING's blockchain team has announced a major breakthrough that will help overcome one of the biggest obstacles to using blockchain in financial services: protecting d...
ing.com

Monero & zCash

zCash

- ZK-SNARKS

Monero

- Ring signatures
- Homomorphic encryption
- Zero Knowledge range-proof

Platform comparison

Platform comparison

	Corda	Fabric	Ethereum	Quorum
Consensus	Pluggable	Pluggable	PoW	Pluggable
Privacy	Confidential identities, selective multicasting, SGX	Channels	ZK-SNARKS (available soon)	Private transactions, SGX, ZSL
Scalability	++	++	22 TPS	++
Smart contract language	Java (any JVM language)	Go & Java	Solidity & Serpent	Solidity/Serpent

Questions

ING