How Much Should we Trust and How Much Should we Distribute?

Srdjan Čapkun

ETH zürich

Blockchains are distributed (by definition)

Blockchains are distributed (by definition)

- *Don't guarantee confidentiality*
- *Don't scale well for all applications*
- *Services around blockchains are not easily distributed*

Data sources:

data that is used in smart contracts needs to be correct

Exchanges:

store funds, perform transactions (custody) => trust

Light Clients:

Clients don't store full ledger or run consensus => trust in full clients / miners

Performance:

The more you distribute, the slower you are

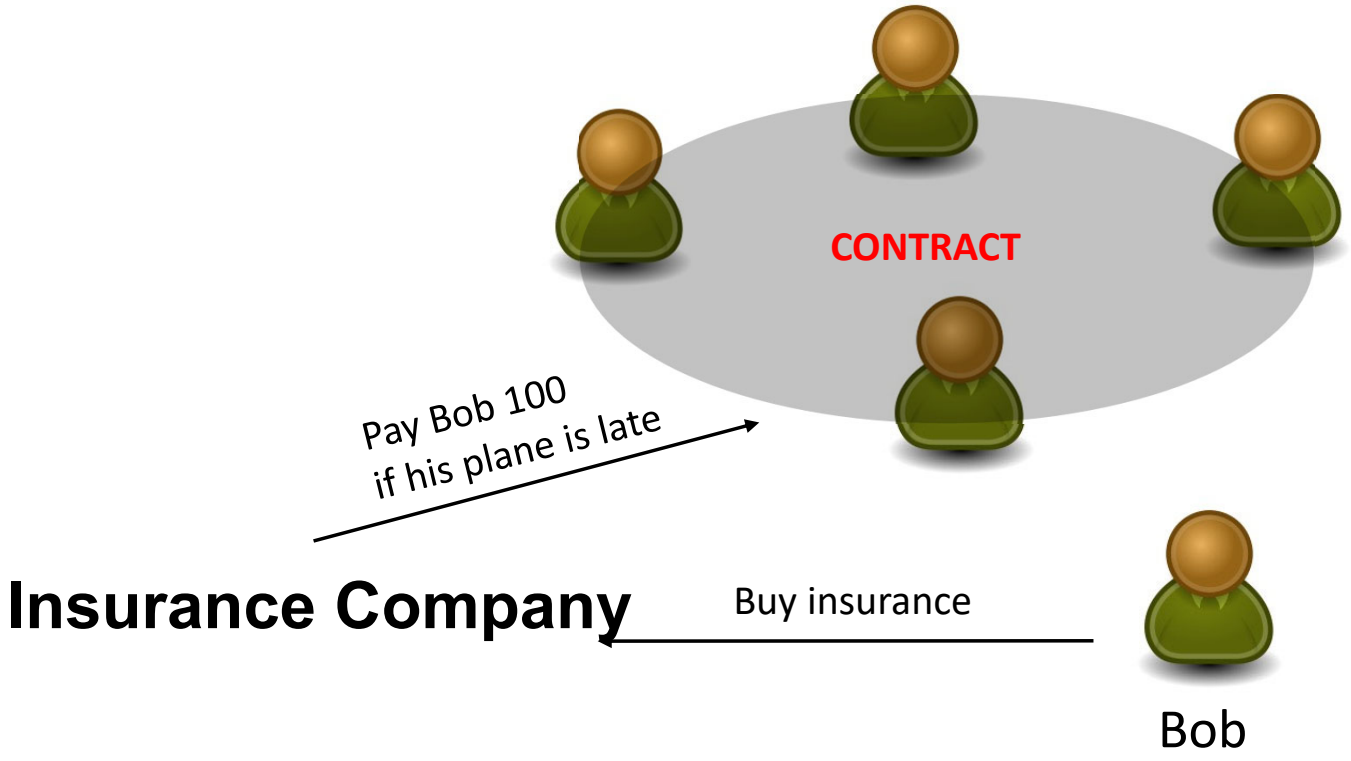
Can Traditional Approaches Help?

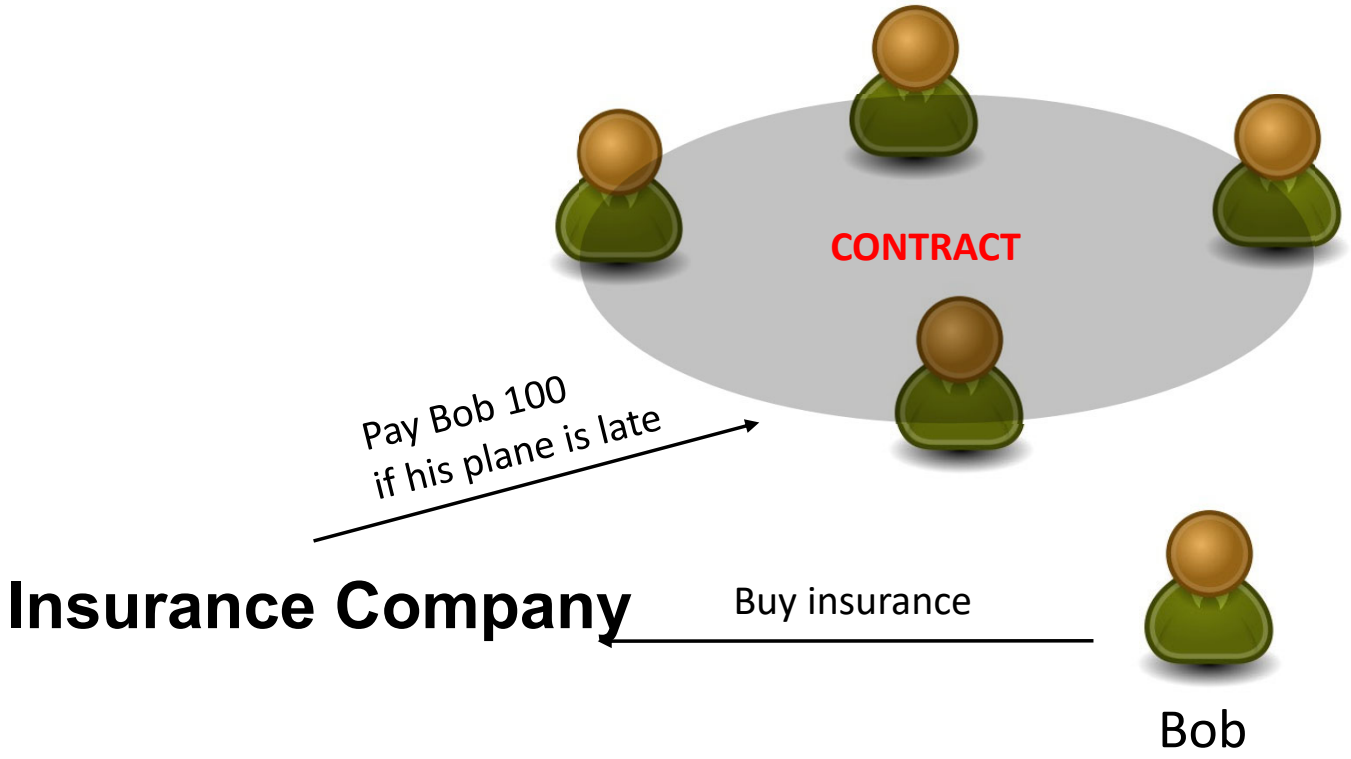
- Threshold and ZK crypto schemes (to protect secrets)
- Multi-Party computation (to guarantee resilience to byzantine behavior)
- Distributed Protocols e.g., Consensus [aka Ledgers, Blockchains]

All useful, but

- performance issues
- need to be tailored for individual application (e.g., ZK Snarks in Zcash, PoW, …)
- cannot easily be combined to achieve all the goals of the application

Example 1: Data Sources (i.e., Oracles)


CONTRACT
Pay Bob 100
if his plane is late
Insurance Company
Buy insurance
Bob



How does the Blockchain know that Bob's plane was late?

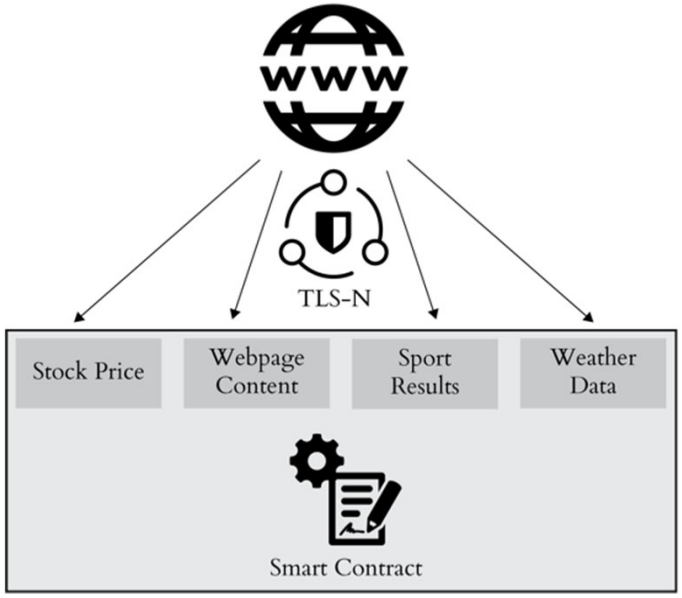
- *Use Trusted Authorities / Oracles (centralization)?*
- *Use TEEs, e.g., TownCrier (**SGX-based**)*
- *Use publicly available information [**trust the crowd / web**]?*

*Problem: TLS doesn't support **non-repudiation** (i.e. when your client talks to server, no signature of interaction)*

TLS-N: A TLS Extension for **Non-Repudiation**

Evidence of interaction
(***signed transcript***)

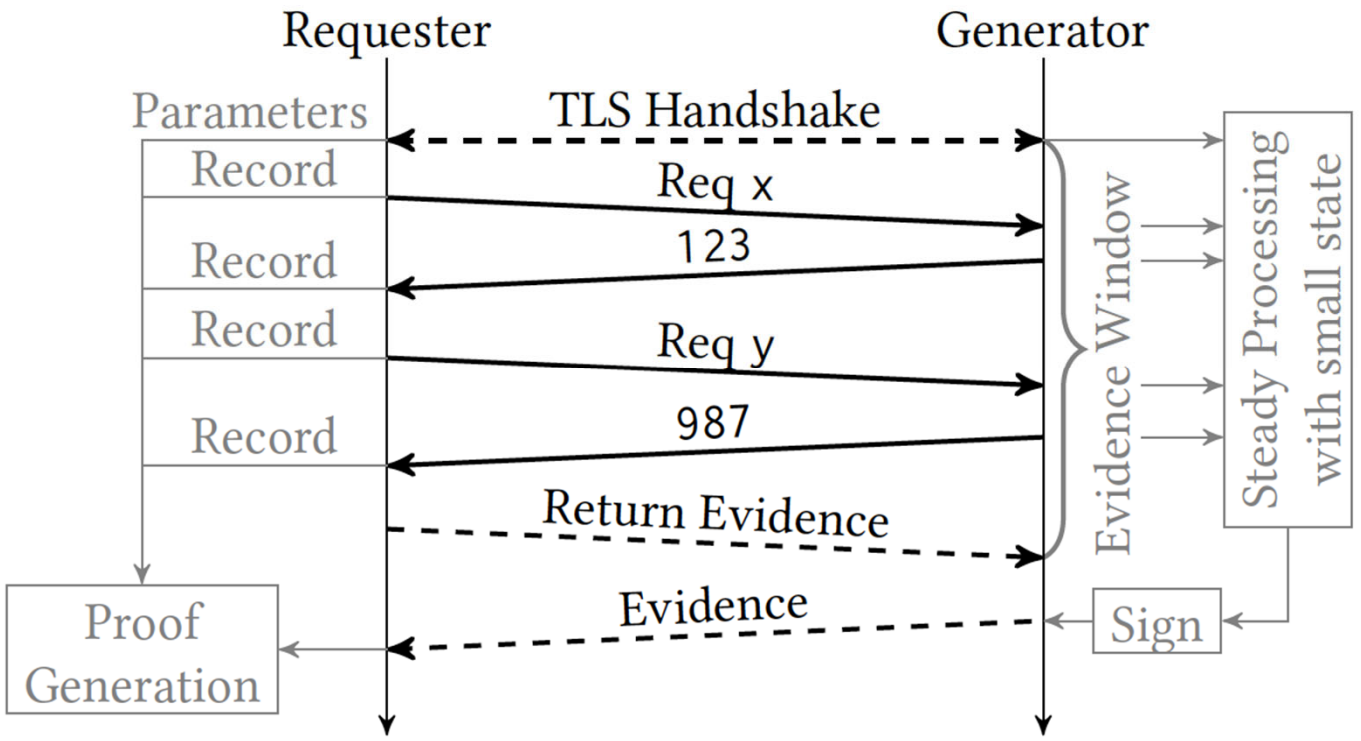
Client ⟵ Server



TLS-N therefore acts as a practical decentralized blockchain oracle

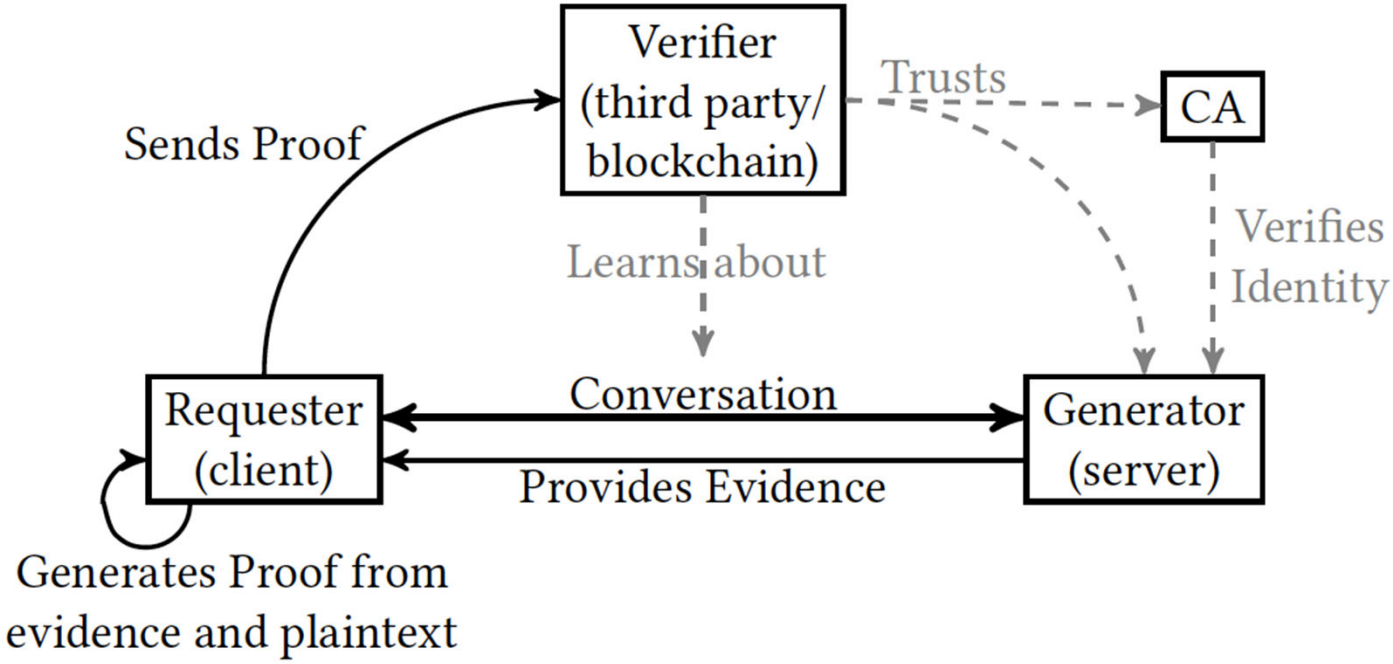
Provides a proof of a total order of messages sent and received by a party - Non-repudiation of conversation (NRC).

TLS-N: A TLS Extension for **Non-Repudiation**

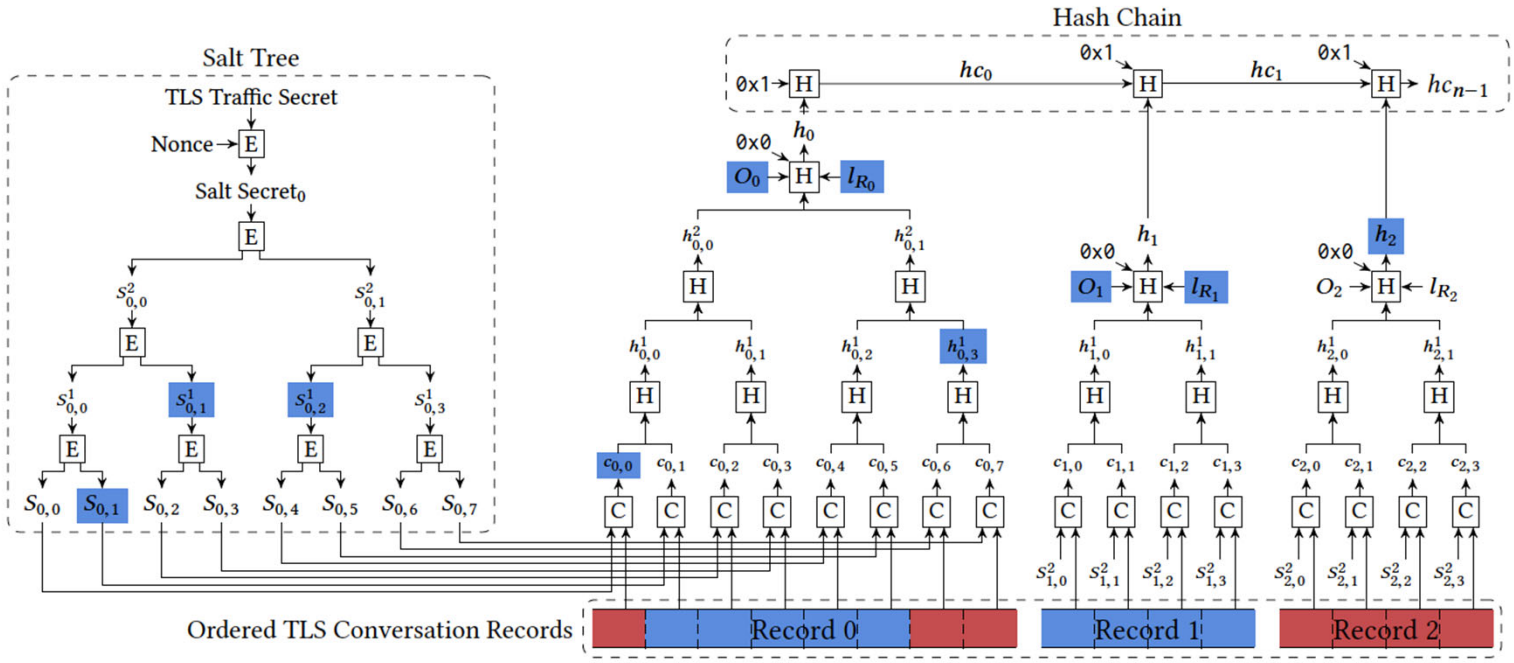


But what about private data that the client doesn't want to include in the proof?

TLS-N: A TLS Extension for **Non-Repudiation**



TLS-N: A TLS Extension for **Non-Repudiation**



Record size: 16kb, chunk size: 8 - 64B (high granularity)

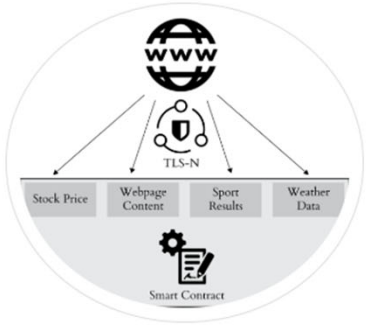
Content Extraction Signature / Redactable Signature

Hubert Ritzdorf, Karl Wüst, Arthur Gervais, Guillaume Felley, Srdjan Capkun
TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing
in Proceedings of the Network and Distributed System Security Symposium (**NDSS**), 2018

Securely share TLS-based content.

TLS-N is the first TLS extension that provides non-repudiation and thereby enables parties to verify each others TLS connections and its contents.

Learn More Details.



The Features

Content Signing

TLS-N allows to generate a proof over the contents of a TLS session. Third parties can then verify the contents given existing TLS assumptions.

Blockchain Integration

TLS-N proofs can be verified by a permissionless blockchain without additional trusted third party, thereby allowing decentralized oracles.

Privacy

When a proof is generated, parts of the TLS session (e.g., passwords, cookies) can be hidden for privacy reasons, while the remaining content can be verified.

www.tls-n.org

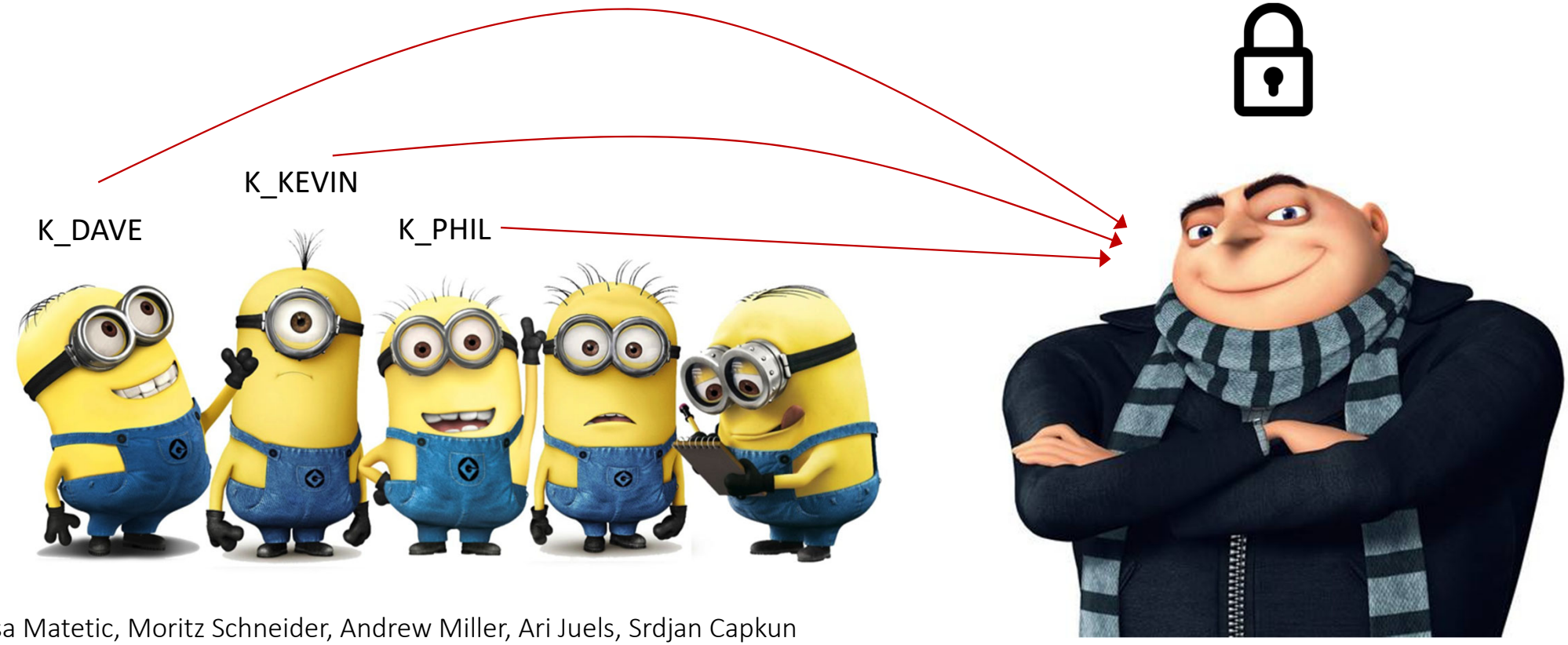
Fully Distributed Blockchain Oracle

Implementations for OpenSSL and Mozila NSS

Example 2: Custody and Delegation

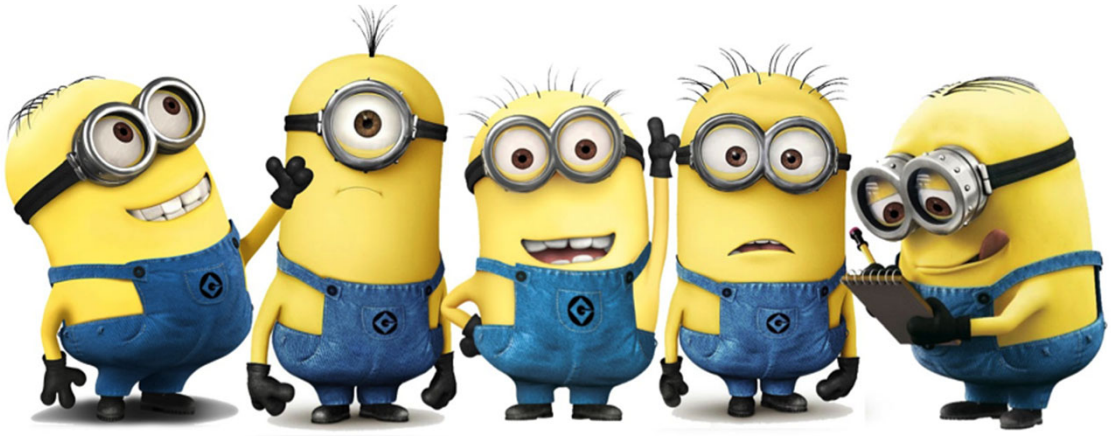
or better say, what do I do with my keys?

Store your keys with a trusted entity (but limit what they can do with it)



Sinisa Matetic, Moritz Schneider, Andrew Miller, Ari Juels, Srdjan Capkun
DelegaTEE: Brokered Delegation using Trusted Execution Environments
in **Usenix Security** Symposium, 2018

Delegate with Restrictions

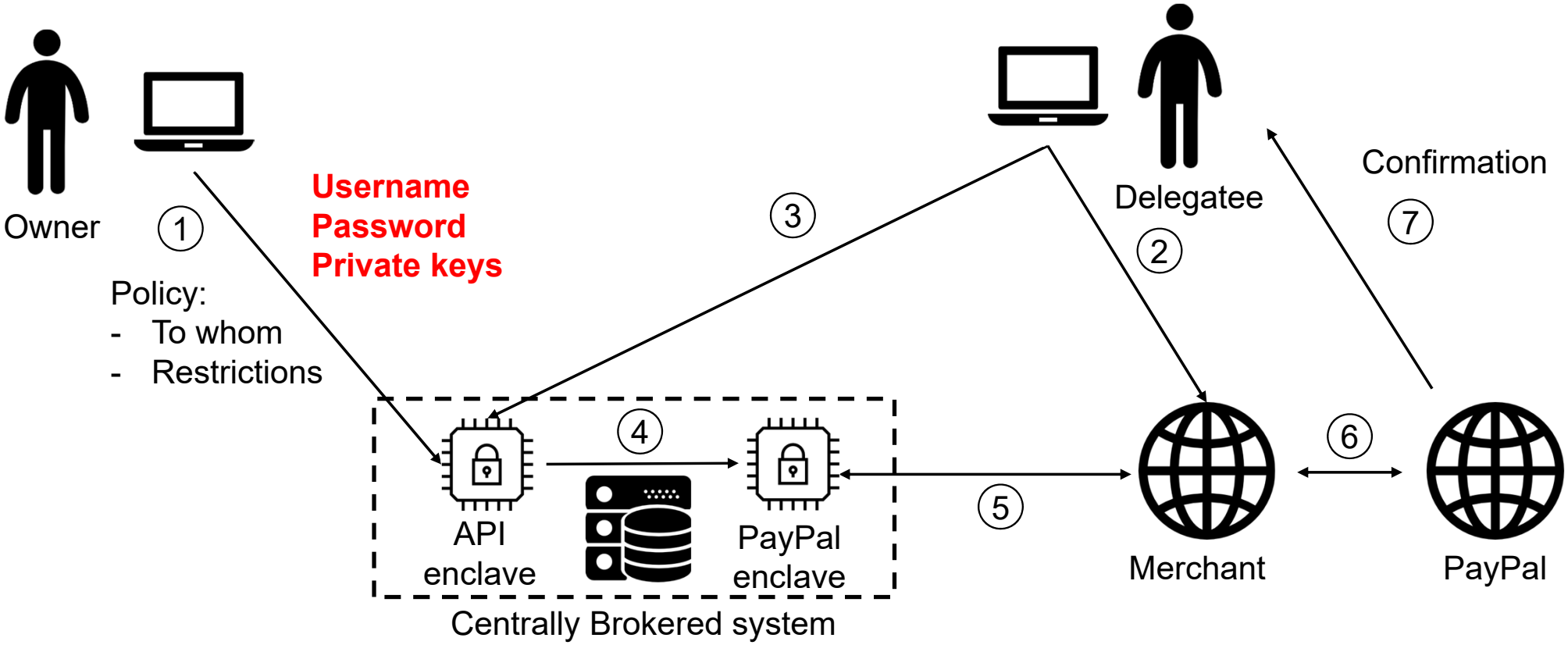


Sinisa Matetic, Moritz Schneider, Andrew Miller, Ari Juels, Srdjan Capkun
DelegaTEE: Brokered Delegation using Trusted Execution Environments
in **Usenix Security** Symposium, 2018

DelegaTEE - properties

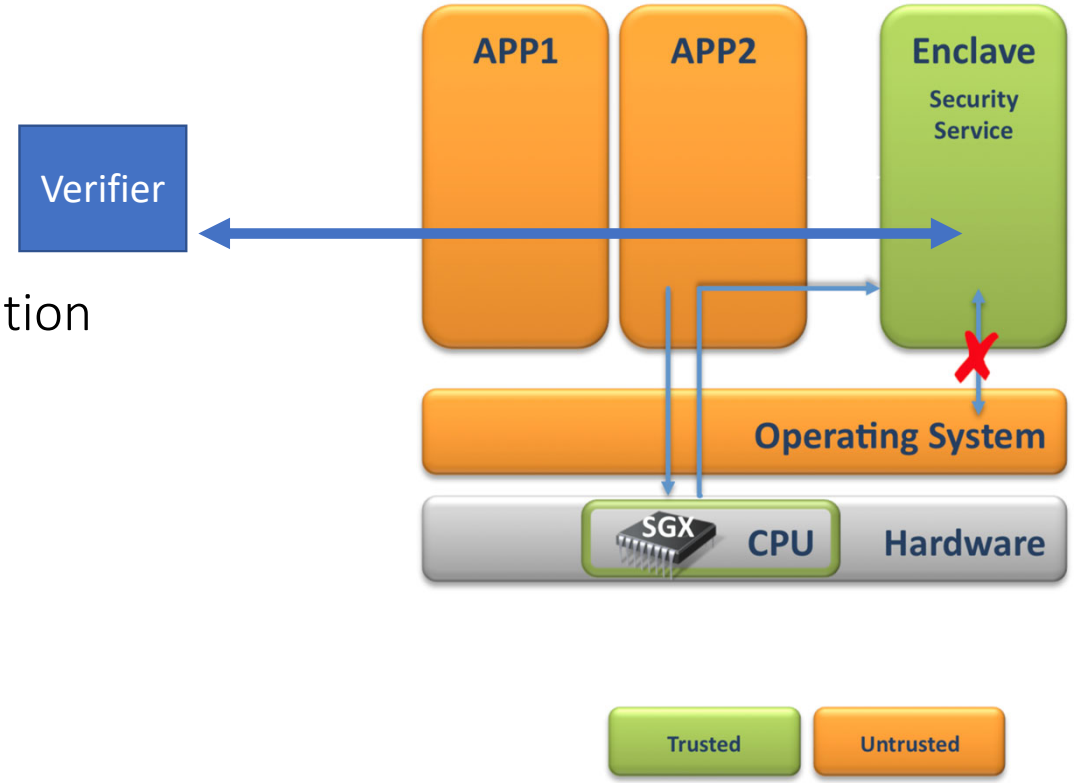
- The Owner's credentials remain confidential.
- The Owner can restrict access to his account, e.g., in terms of time, duration of access, no. of reads/writes etc. - with rich contextual policies
- The system logs the actions of Owners and Delegatees so that post-hoc attribution of their behaviour is possible (as a means of resolving disputes)
- The system minimizes the ability of a service to distinguish between access by the Delegatee and that of the legitimate Owner

- Owner does not have to always be online


Owner
1
Username
Password
Private keys
Policy:
- To whom
- Restrictions
3
Delegatee
2
Confirmation
7
4
API
enclave
PayPal
enclave
Centrally Brokered system
5
Merchant
6
PayPal

- TEEs e.g., Intel Software Guard Extensions (SGX)

- **Remote attestation**:
  Prove that correct "code.exe" is running inside enclave
- **Integrity**: cannot tamper with execution
- **Confidentiality**
- **Small TCB** inside enclave.



Images taken from software.intel.com

HOME
INTERIOR
DIY + GARDEN
SPORTS + LEISURE
TOYS
PET SUPPLIES
BABY + CHILD
BEAUTY + HEALTH
WATCHES + JEWELLERY
OFFICE
DIGITAL
MEDIA

Top 10 categories
LEGO
Bulbs
Alarm clocks
Electric toothbrushes
Bike lights
Humidifier accessories
Beard + Hair trimmers
Kitchen machine accessories
Socket strips
Night lights

Go to
Sale
Buy second hand
Vouchers
Magazine
Current ads
Community

Thank you for your order

You will receive an order confirmation e-mail shortly.

Order: 11620200

Payment

Your PayPal payment of CHF 28.25 incl. was confirmed.

Order overview and delivery status of the ordered products

Monitor the order status, expected delivery time and payment status in your customer account. Please keep in mind that an order comprising more than one item will only be dispatched when all products are available. Exceptions are direct deliveries made by some of our suppliers. There is an option of triggering a partial delivery in your customer account. Simply go to delivery details in the order overview. Should you have any questions regarding the delivery, please do not hesitate to contact our customer service.

Back to start page | Show order

Product information

360 Eye: Dyson's first robot vacuum cleaner

Edit

3. Payment

PayPal
Paypal is an international payment service allowing transactions to be made directly between vendors and buyers.
Paypal processes your payment before forwarding it to us.
Further information about this service is available on www.paypal.com.

Redeem your vouchers here

Edit

4. Delivery options

Without delivery note or receipt
Saturday deliveries permitted
Preferred delivery days: None (as soon as possible)

Edit

5. Order overview

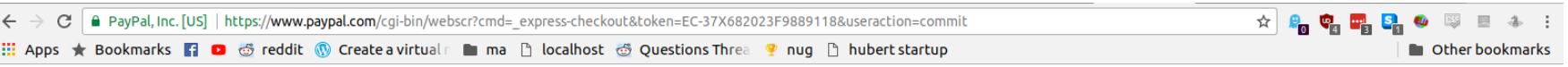
Description / Availability	Quantity	Price	Total
Tesa Powerbond Montageband Ultra Strong (19mm, 5m) 5 item(s) ready for delivery from our warehouse	1	18.70	18.70

Total Products	18.70
Payment fee	0.55
Minimum order surcharge (omitted from 50.-)	9.00
Total excl. VAT	26.15
Total incl. VAT	**28.25**

If not stated otherwise, all prices are including VAT and in CHF
By placing your order you accept our General terms and conditions. If your order contains tobacco products or alcoholic beverages, you hereby confirm to be 18 years or older.

Show my purchase in my public profile

Pay



PayPal

Bei PayPal einloggen

E-Mail-Adresse

Passwort

Eingeloggt bleiben und schneller zahlen

Nicht auf gemeinsam genutzten Geräten aktivieren

Einloggen

Pay with DelegaTEE

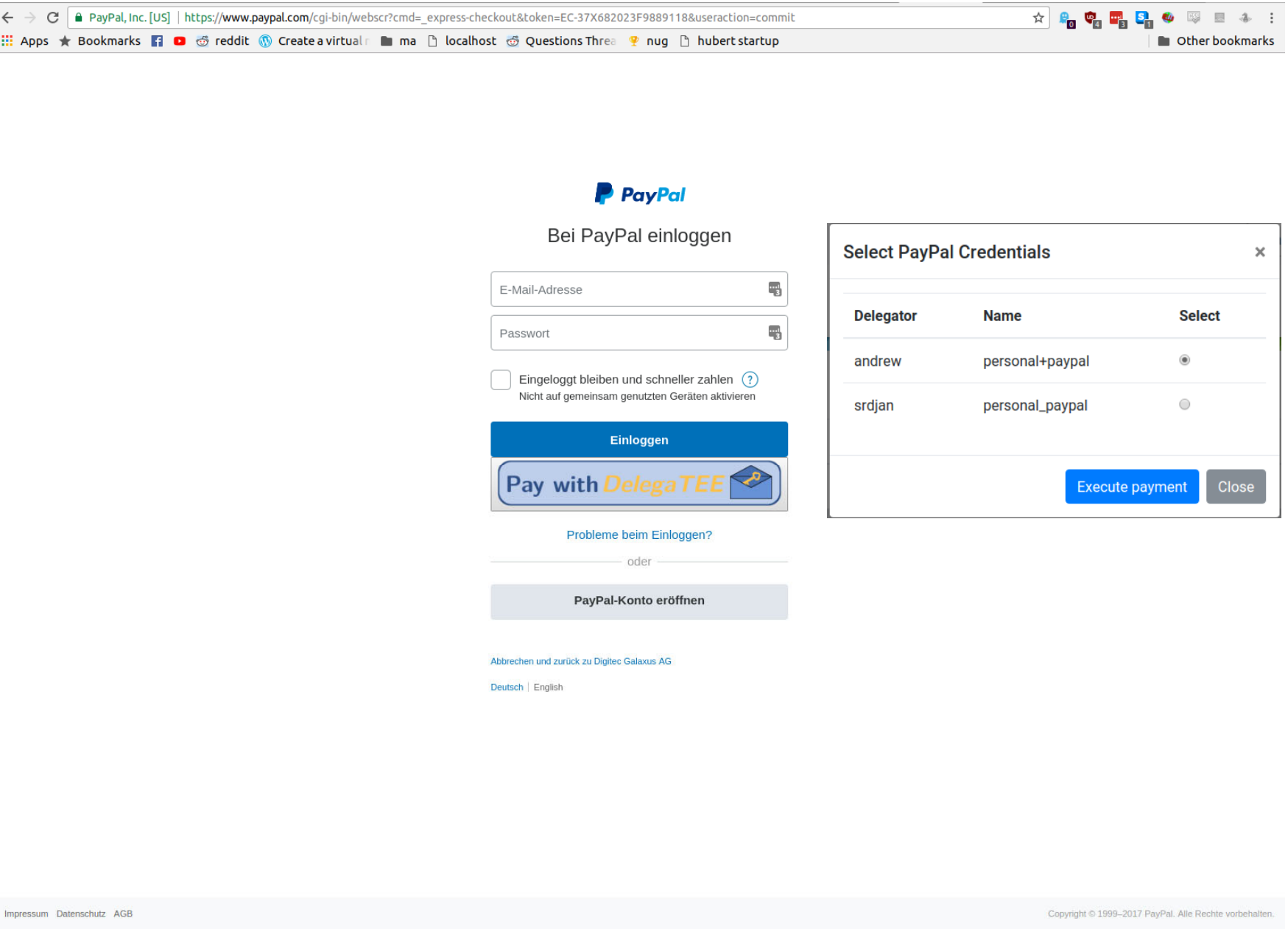
Probleme beim Einloggen?

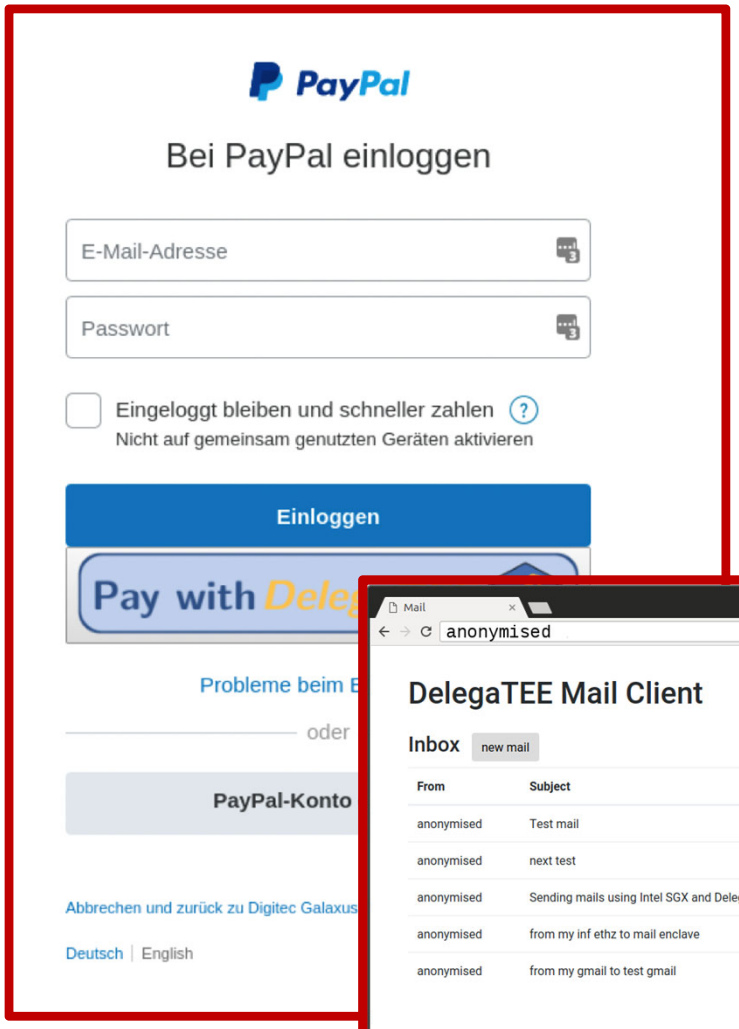
oder

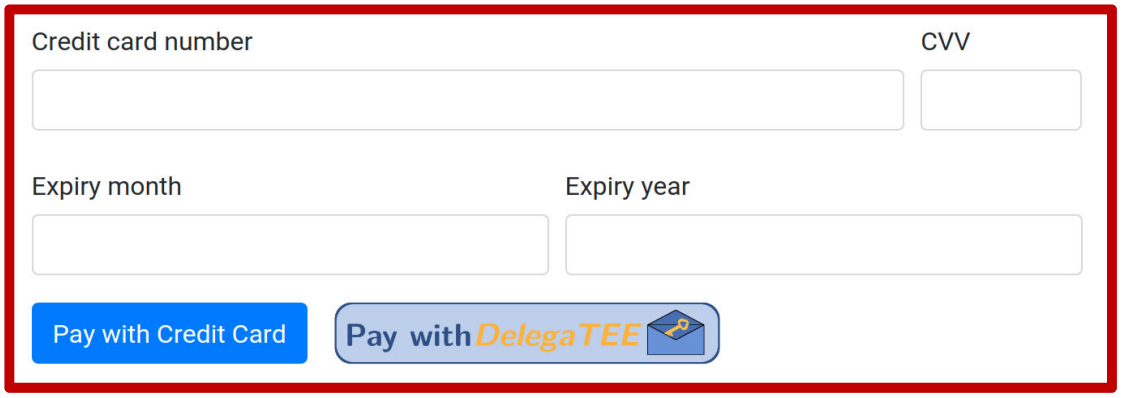
PayPal-Konto eröffnen

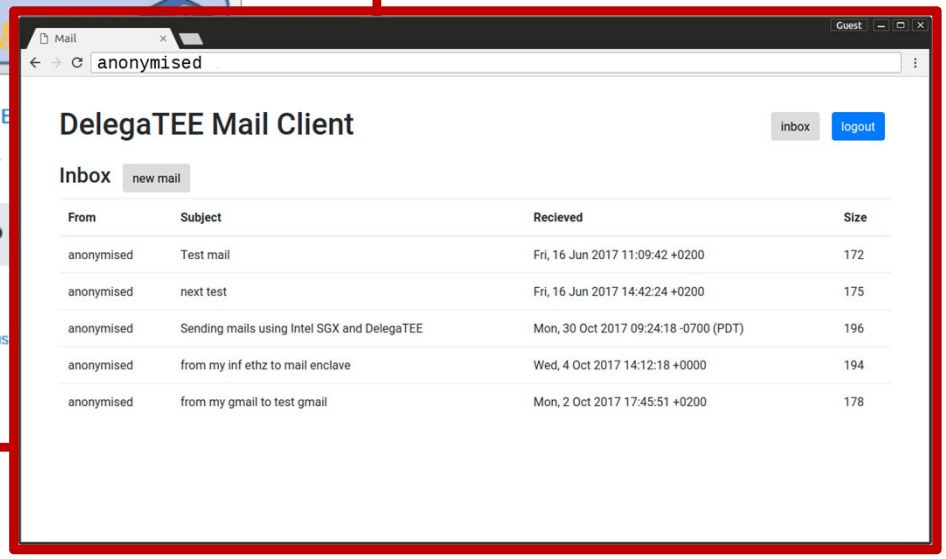
Abbrechen und zurück zu Digitec Galaxus AG

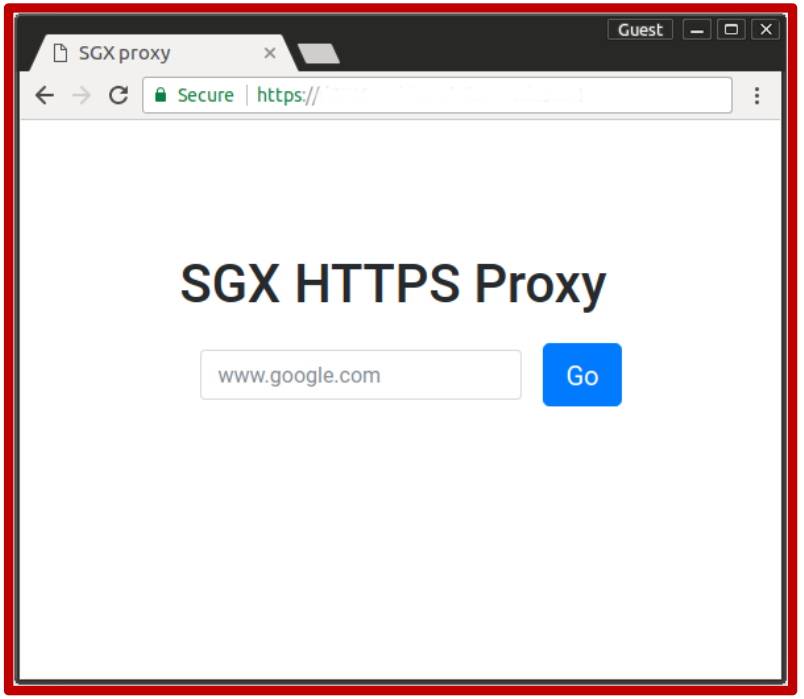
Deutsch | English

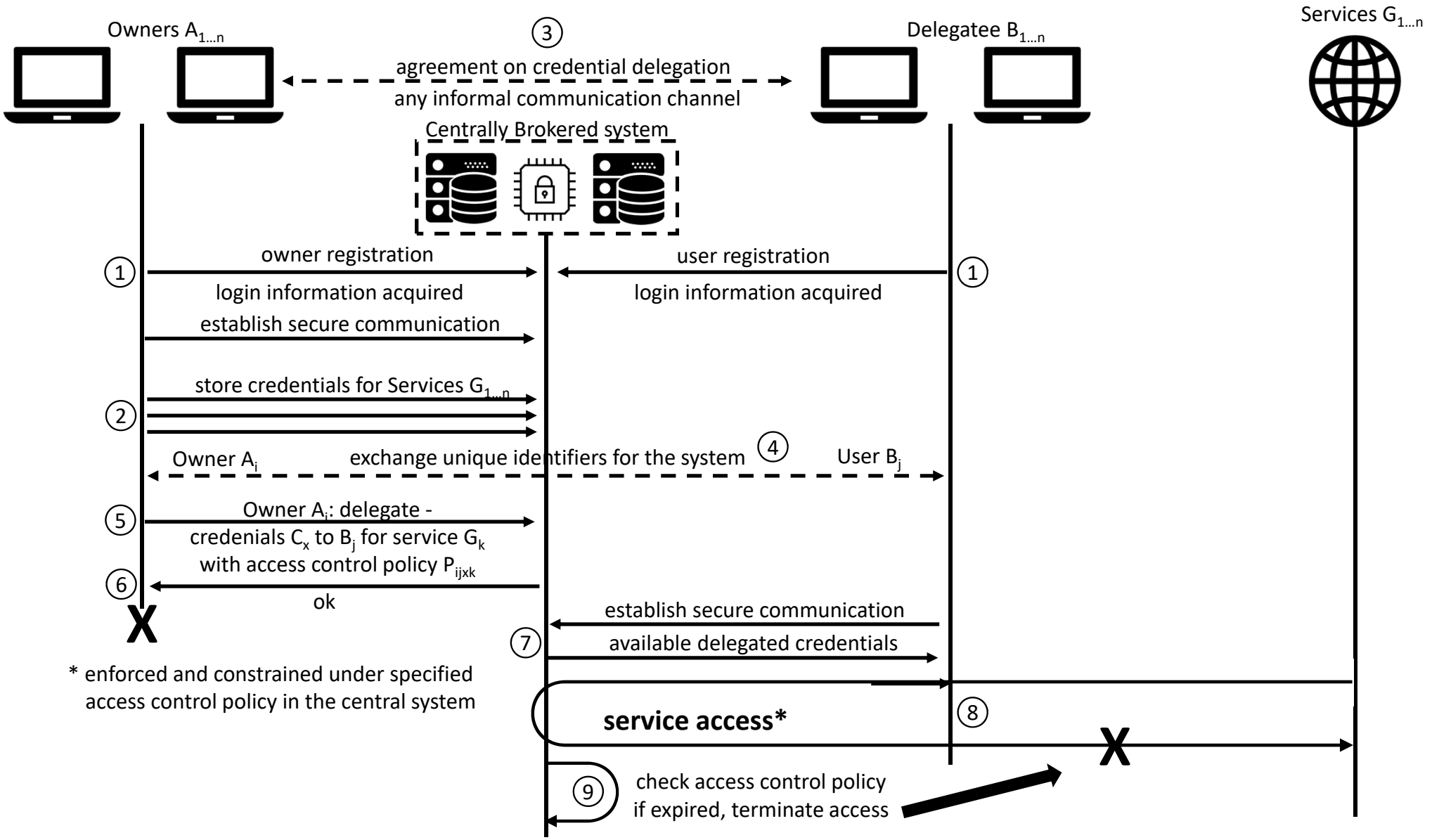

PayPal, Inc. [US] | https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=EC-37X682023F9889118&useraction=commit
Apps
Bookmarks
reddit
Create a virtual
ma
localhost
Questions Threa
nug
hubert startup
Other bookmarks
PayPal
Bei PayPal einloggen
E-Mail-Adresse
Passwort
Eingeloggt bleiben und schneller zahlen
Nicht auf gemeinsam genutzten Geräten aktivieren
Einloggen
Pay with DelegaTEE
Probleme beim Einloggen?
oder
PayPal-Konto eröffnen
Abbrechen und zurück zu Digitec Galaxus AG
Deutsch | English
Select PayPal Credentials
Delegator
Name
Select
andrew
personal+paypal
srdjan
personal_paypal
Execute payment
Close
Impressum
Datenschutz
AGB
Copyright © 1999–2017 PayPal. Alle Rechte vorbehalten.


PayPal
Bei PayPal einloggen
E-Mail-Adresse
Passwort
Eingeloggt bleiben und schneller zahlen
Nicht auf gemeinsam genutzten Geräten aktivieren
Einloggen
Probleme beim E
oder
PayPal-Konto
Abbrechen und zurück zu Digitec Galaxus
Deutsch | English


Credit card number
CVV
Expiry month
Expiry year
Pay with Credit Card
Pay with DelegaTEE

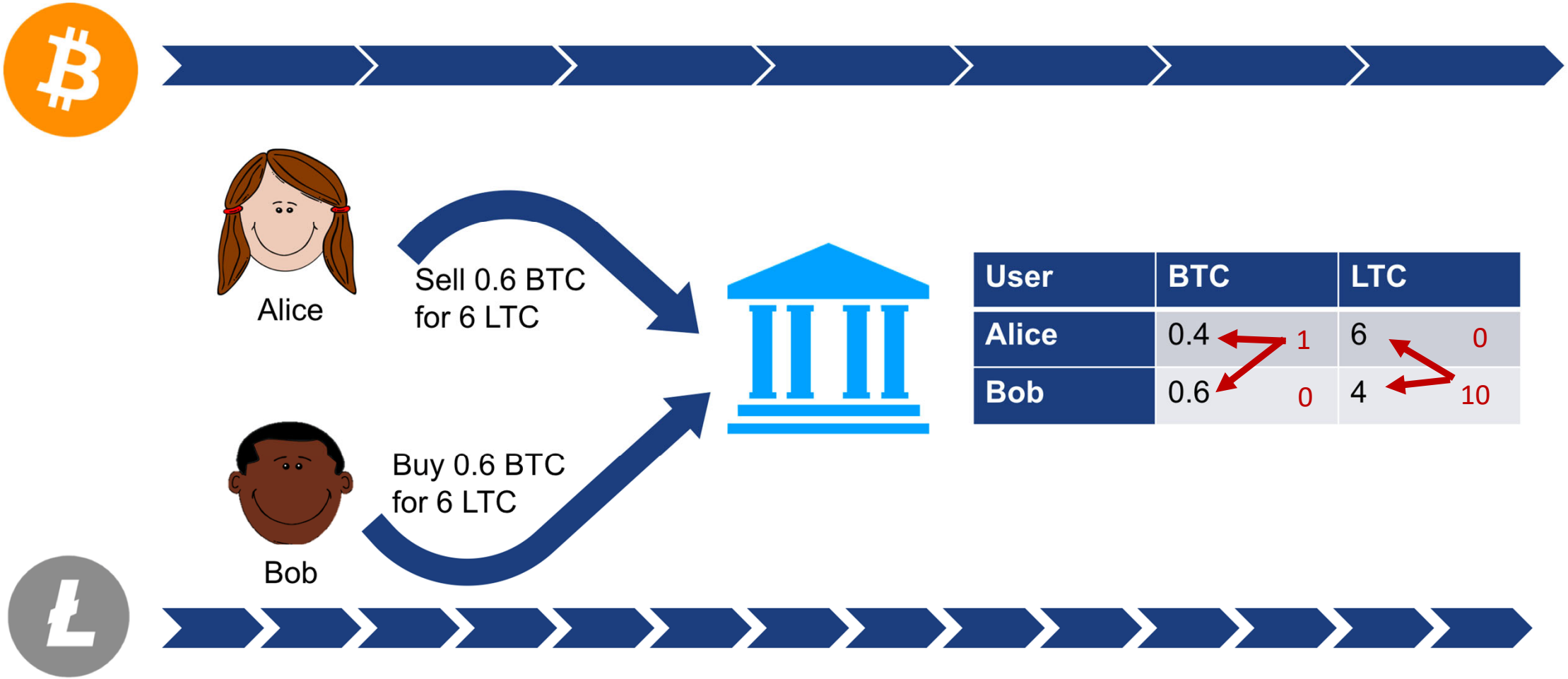

Mail
Guest
anonymised
DelegaTEE Mail Client
inbox
logout
Inbox
new mail
From
Subject
Recieved
Size
anonymised
Test mail
Fri, 16 Jun 2017 11:09:42 +0200
172
anonymised
next test
Fri, 16 Jun 2017 14:42:24 +0200
175
anonymised
Sending mails using Intel SGX and DelegaTEE
Mon, 30 Oct 2017 09:24:18 -0700 (PDT)
196
anonymised
from my inf ethz to mail enclave
Wed, 4 Oct 2017 14:12:18 +0000
194
anonymised
from my gmail to test gmail
Mon, 2 Oct 2017 17:45:51 +0200
178


SGX proxy
Guest
Secure
https://
SGX HTTPS Proxy
www.google.com
Go


Owners $A_{1...n}$
3
agreement on credential delegation
any informal communication channel
Delegatee $B_{1...n}$
Services $G_{1...n}$
Centrally Brokered system
1
owner registration
login information acquired
user registration
login information acquired
1
establish secure communication
store credentials for Services $G_{1...n}$
2
Owner A_i
exchange unique identifiers for the system
4
User B_j
5
Owner A_i: delegate -
credenials C_x to B_j for service G_k
with access control policy P_{ijxk}
6
ok
establish secure communication
7
available delegated credentials
* enforced and constrained under specified
access control policy in the central system
service access*
8
9
check access control policy
if expired, terminate access

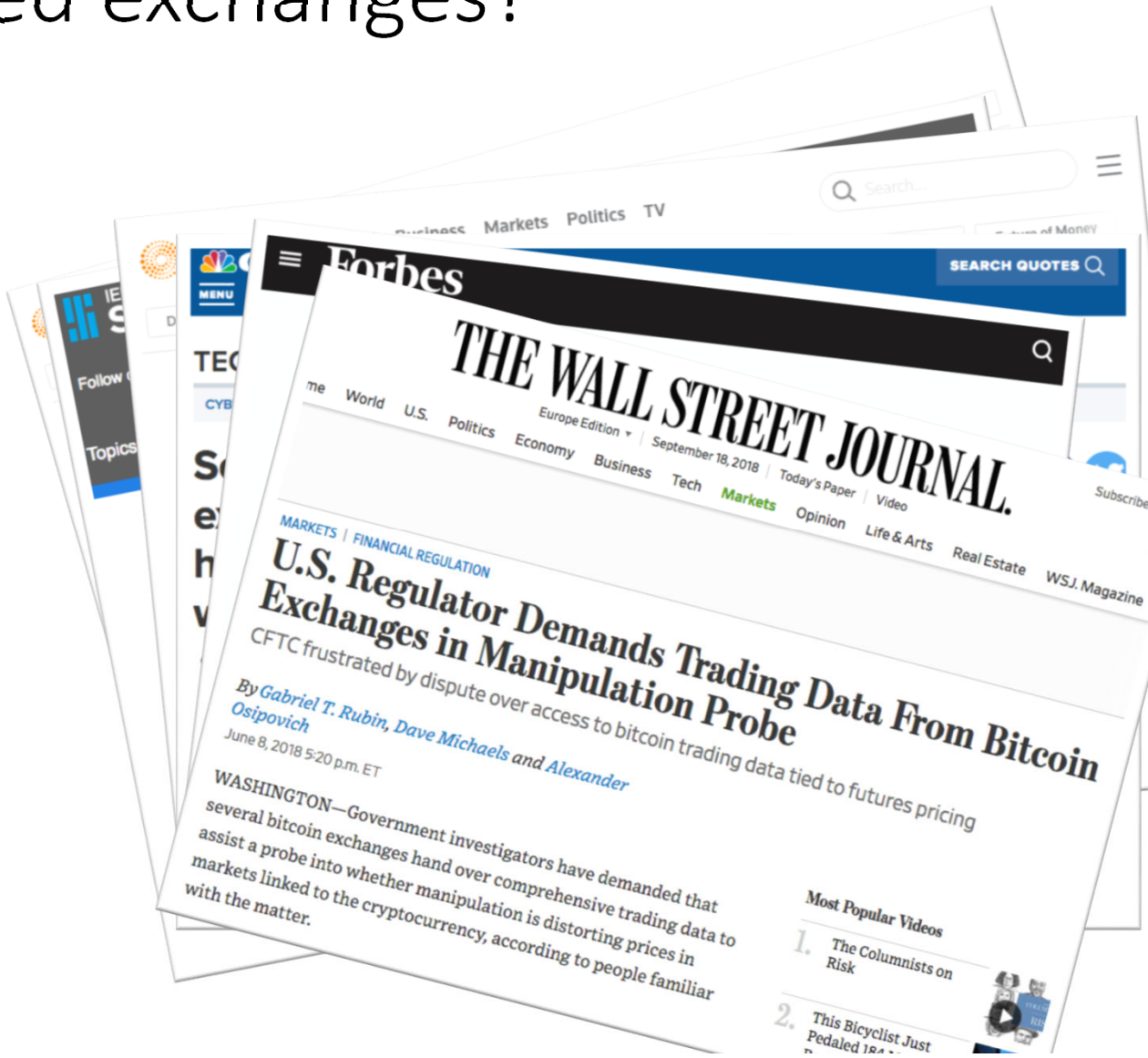
Example 3: Trustless Exchange

What's an Exchange?



Can we trust centralized exchanges?

- Custodial risk:
  - More than 30 incidents since 2011
  - Over $2 billion in losses
- Manipulation risk:
  - Front-running
  - Order book manipulation



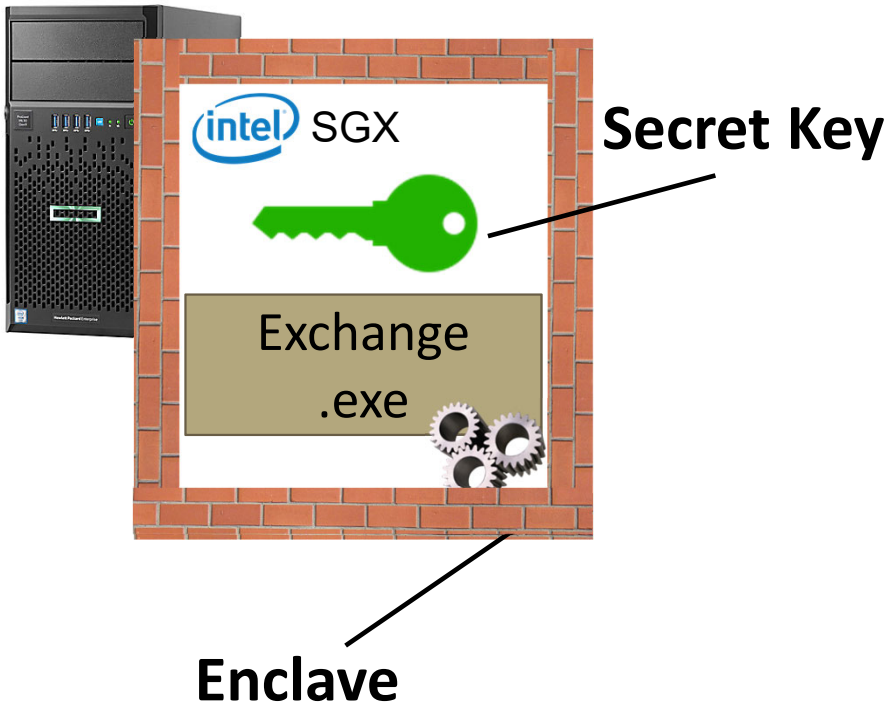
Decentralized exchanges?

- Run as smart contract on blockchain
- No custodial risk
- But:
  - Front-running and order book manipulation possible
  - No support for blockchains without smart contracts (Bitcoin, Litecoin, etc…)
  - No support for trading across blockchains, e.g. Bitcoin/Ethereum
  - Slow
  - Expensive

Tesseract: a TEE supported exchange

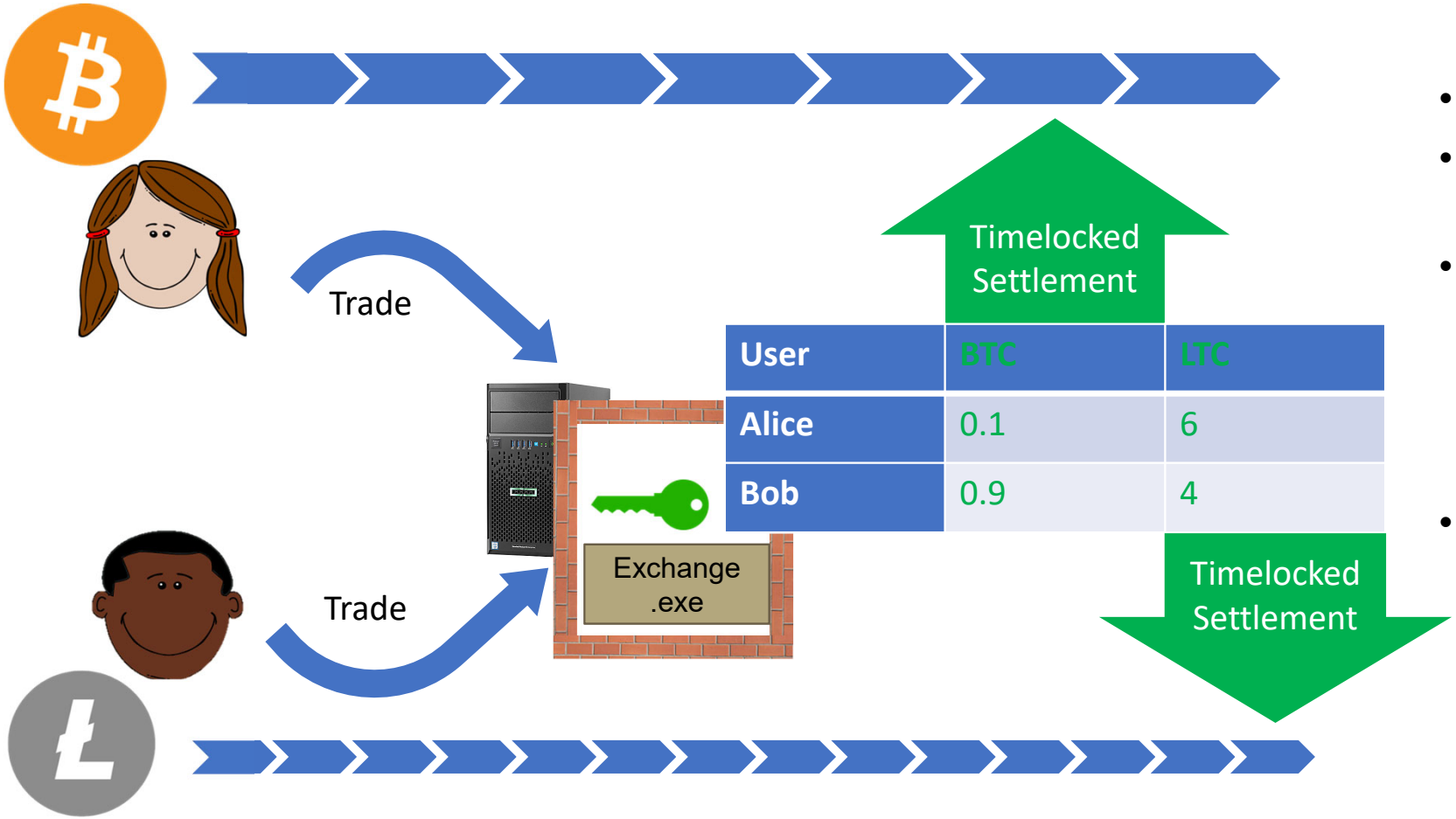
- Centralized exchanges require complete trust from user
- Decentralized exchanges solve custody issue, but
  - still require trust (manipulation)
  - are impractical
- Tesseract gives best of both worlds:
  - No custodial risk:
    - Operator has no access to funds
    - Fail-safe: Users get money back in case of unavailability
  - No manipulation risk
  - Cross-chain trading
  - Speed and cost comparable to centralized exchanges

Ingredient 1: Trusted Execution Environment



- **Remote attestation**: Prove that correct "Exchange.exe" is running inside enclave
- **Integrity**: Cannot tamper with execution of "Exchange.exe"
  - Order processing inside enclave
    ⇒ No orderbook manipulation possible
- **Confidentiality**: Secret Key controlling funds only known inside enclave
  - Operator does not know key
- **Small TCB** inside enclave. Use array of modern techniques (testing, fuzzing, verification, …) to ensure correctness.

Main Idea: Time-locked Atomic Cross-chain Settlement



- Blockchain is slow.
- Must **batch-settle** trades for good speed
- Settlements are **timelocked**: If exchange becomes unavailable for e.g. 24 hrs, users get their money back
- Settlements are **atomic** across chains to prevent race conditions

Continued development

FNSNF
Fonds national suisse
Schweizerischer Nationalfonds
Fondo nazionale svizzero
Swiss National Science Foundation
BRIDGE

CORNELL TECH

ETH zürich

IC3 The Initiative For CryptoCurrencies & Contracts

Tesseract

Tesseract is a **better cryptocurrency exchange design** that combines the **functionality and performance** of centralized exchanges with the **security** of decentralized exchanges.

We are working to commercialize the technology with the support of the SNF BRIDGE program.

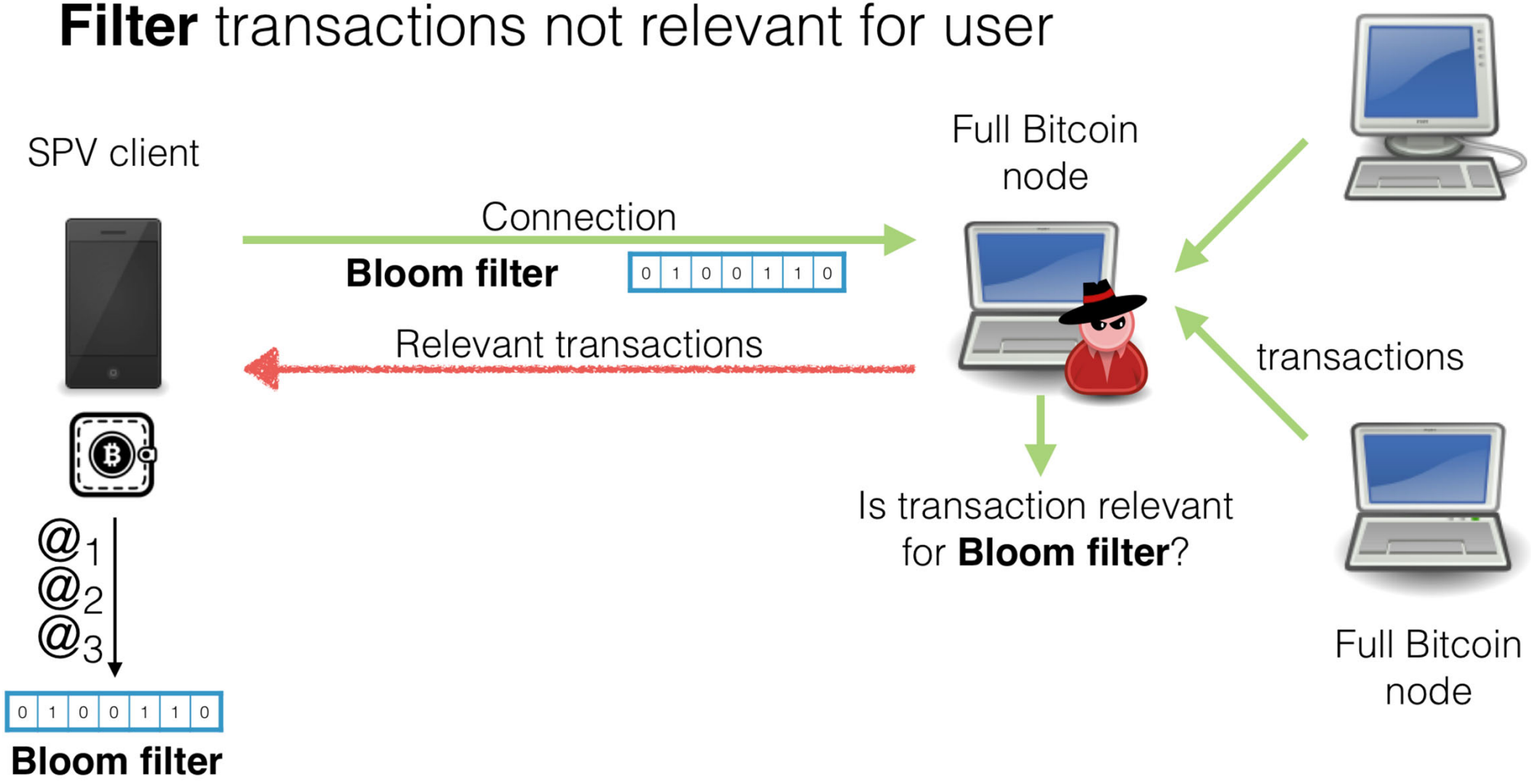
Lorenz Breidenbach
https://lorenzb.com/

Example 4: Privacy for Light Clients

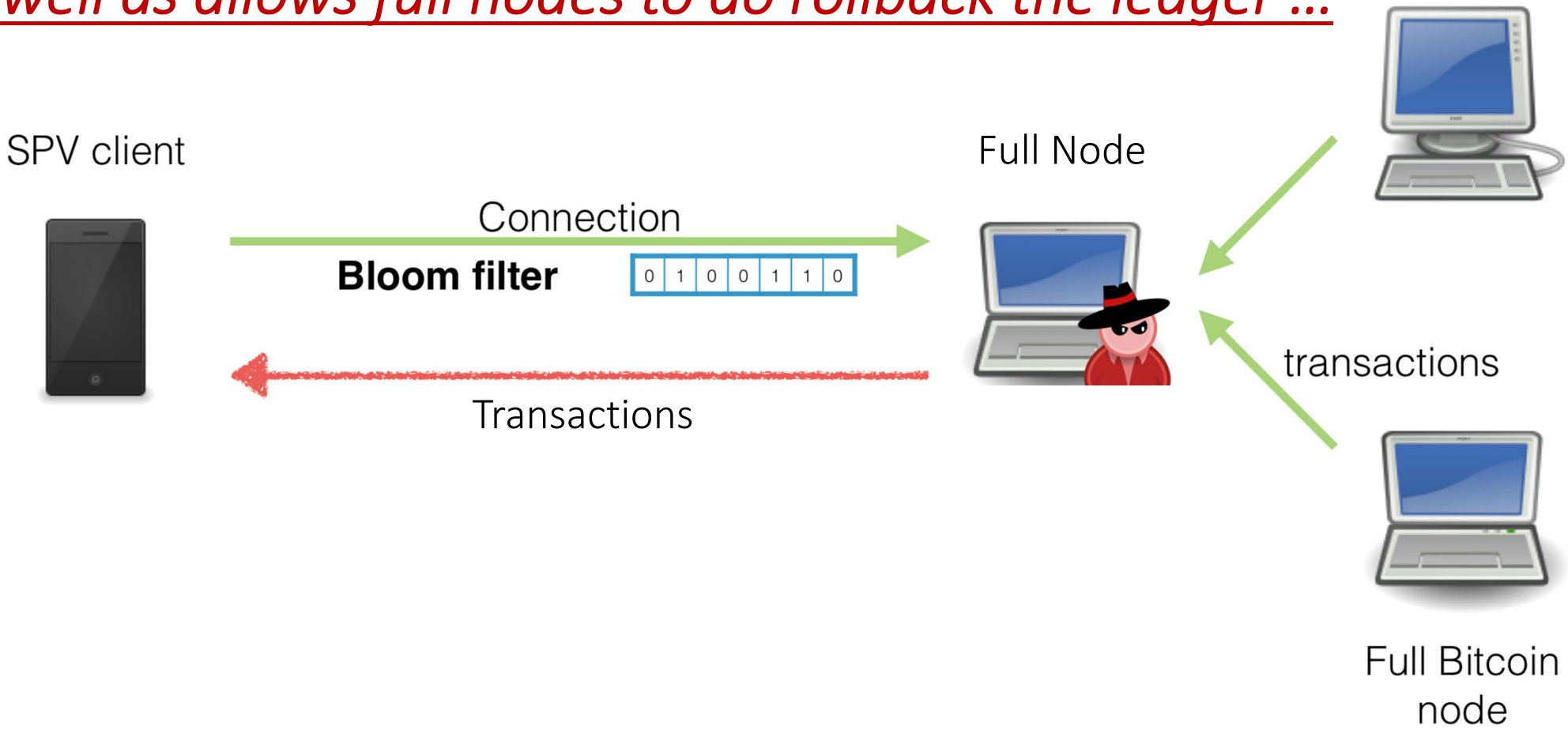
i.e., do you trust 'full nodes' with your privacy?

Simple **P**ayment **V**erification (SPV)

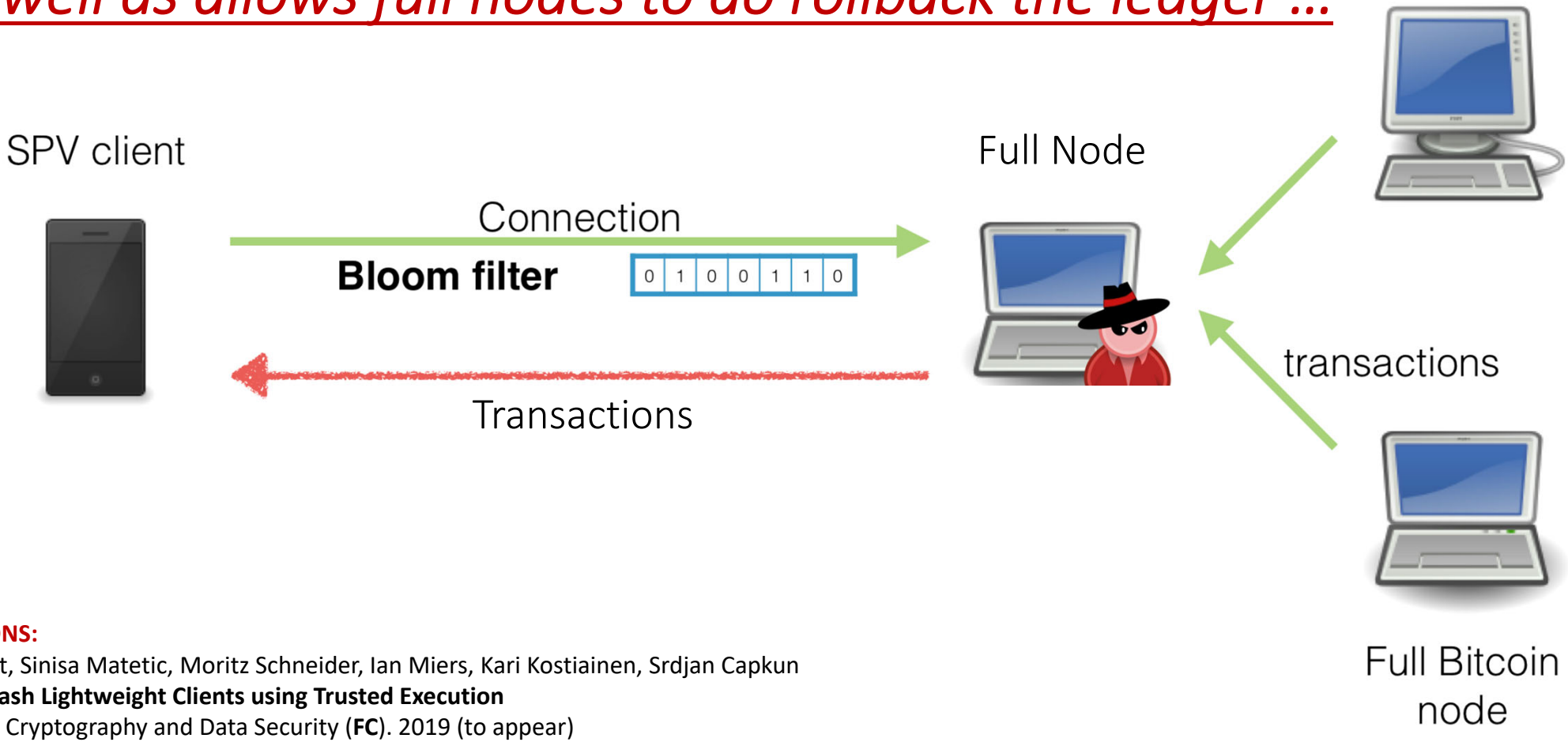
Filter transactions not relevant for user



This leaks information about Client's funds and identity as well as allows full nodes to do rollback the ledger …



This leaks information about Client's funds and identity as well as allows full nodes to do rollback the ledger …



SOLUTIONS:

Karl Wüst, Sinisa Matetic, Moritz Schneider, Ian Miers, Kari Kostiainen, Srdjan Capkun
ZLiTE: Zcash Lightweight Clients using Trusted Execution
Financial Cryptography and Data Security (**FC**). 2019 (to appear)

Sinisa Matetic, Karl Wüst, Moritz Schneider, Kari Kostiainen, Ghassan Karame, Srdjan Capkun,
BITE: Bitcoin Lightweight Client Privacy using Trusted Execution
Usenix Security 2019 (to appear)

Blockchains are distributed (by definition)

- *Don't guarantee confidentiality*
- *Don't scale well for all applications*
- *Services around blockchains are not easily distributed*

To increase performance, reduce # of nodes

- *Increase trust in each node*
- *Increase trust in services that cannot be distributed*

=> Trusted Execution Environments (i.e., TEEs)?

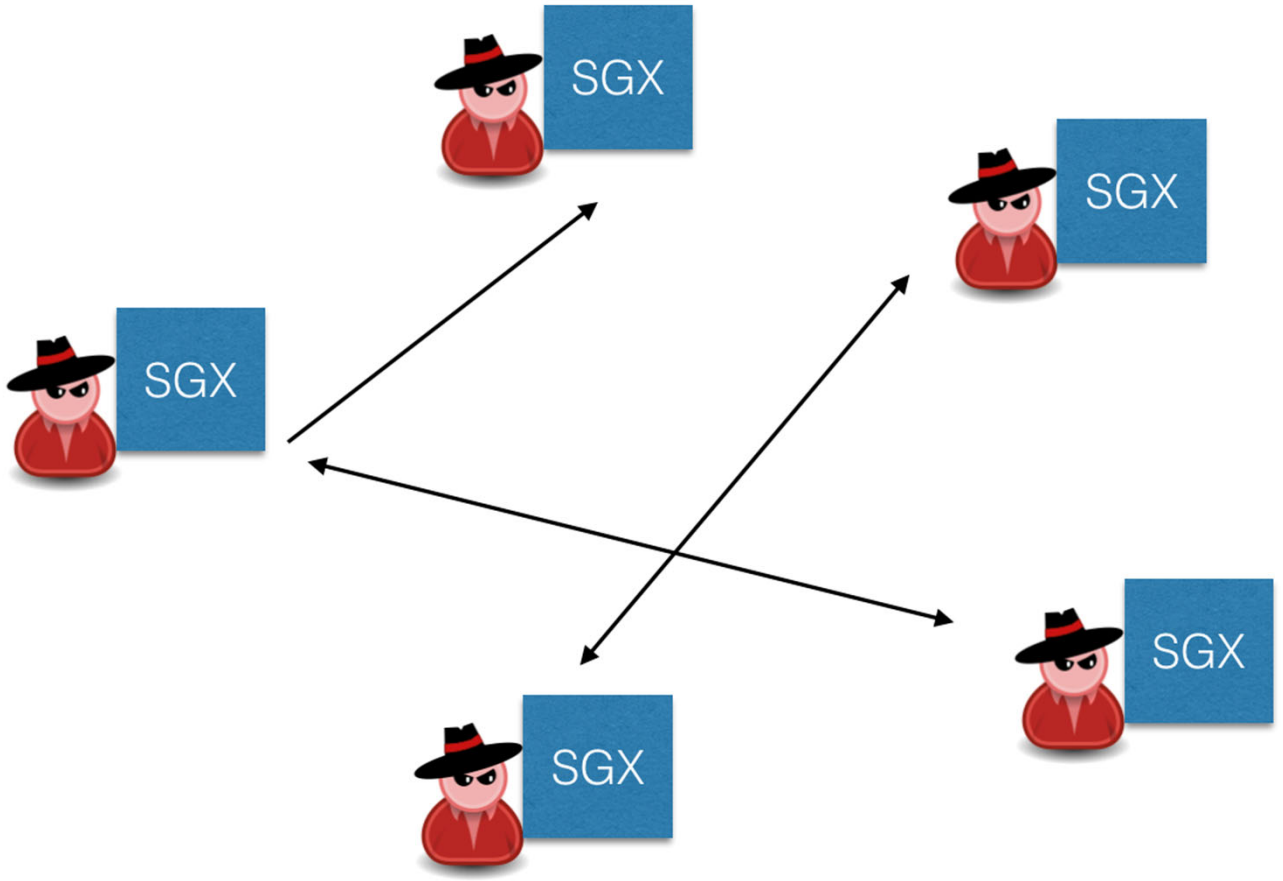
Trusted Execution Environments

Threat	SGX	IBM4765	TPM	TXT+TPM	TrustZone	XOM	Aegis	Bastion	Sanctum
Malicious OS									
direct probing	✓[a]	N/A[c]	N/A[c]	✓[e]	✓[a]	✓	✓[c]	✓[b;i]	✓[a]
page faults	✗	N/A[c]	N/A[c]	✓[e]	✓	N/A	✗	✗	✓
cache timing	✗	N/A[c]	N/A[c]	✓[e]	✗	✗	✗	✗	✓
Malicious Containers									
direct probing	✓[a]	✓	N/A[d]	N/A[d]	N/A[f]	✓	✓[c]	✓[a]	✓[a]
cache timing	✗	✓	N/A[d]	N/A[d]	N/A[f]	✗	✗	✗	✓
Malicious Hypervisor									
direct probing	✓[a]	N/A[c]	N/A[c]	✓[e]	✓[a]	N/A[h]	N/A[h]	N/A[h]	✓[a]
Malicious Firmware									
direct attack	✓[a]	N/A[c]	✓	✓	N/A[f]	N/A[h]	N/A[h]	✓	✓
Physical DRAM attack									
read	✓[b]	✓	✗	✗	✓[g]	✓[b]	✓[b]	✓[b]	✗
write	✓[b]	✓	✗	✗	✓[g]	✓[b]	✓[i]	✓[i]	✗
rollback	✗	✓	✗	✗	✓[g]	✗	✓[i]	✓[i]	✗
address read	✗	✓	✗	✗	✓[g]	✗	✗	✗	✗
Direct Memory Access									
malicious peripherals	✓[b]	✓	✗	✓	✓	✓[b]	✓[b]	✓[b]	✓
HW TCB size	CPU package	Chip package	Mother-board	Mother-board	CPU package	CPU package	CPU package	CPU package	CPU package
SW TCB size	Containers	FW; OS	All SW	OS; APP	FW; OS; APP	APP + HYP	APP + kernel	APP + HYP	APP + monitor

[a] Access check on TLB deployed.
[b] DRAM is encrypted and protected.
[c] Hypervisor and OS are measured and trusted.
[d] Concurrent containers not supported.
[e] Hypervisor and OS preempted at late launch.
[f] Secure world is trusted.
[g] Secure world in on-chip SRAM.
[h] No hypervisor or firmware support.
[i] Merkle tree over DRAM, HMAC.

Table 2.3: *Overview and comparison of Hardware-based TEEs in relation to SGX. Closely resembles [53].*

But we don’t want to rely on a single TEE



[stay tuned – more results coming in this space]

Positive:

- *Fewer nodes, faster consensus*
- *Faster execution of contracts*
- *Confidentiality!*

Need to be careful:

- *Enclave is trusted, not the platform*
- *Rollback Attacks*
  (OS can roll back local and global state)
- *Recent Microarchitectural Attacks*

Distribution increases Trust

But there are limits to what can be distributed

Prediction: a middle ground that balances trust in HW, distribution and Trusted Parties will emerge as the "sweet spot"

<u>Prediction:</u> a middle ground that balances trust in HW, distribution and Trusted Parties will emerge as the "sweet spot"

[stay tuned – more results coming in this space]

Selected Publications:

- Karl Wüst, Kari Kostiainen, Vedran Capkun, Srdjan Capkun
  PRCash: Fast, Private and Regulated Transactions for Digital Currencies
  In Proceedings of the International Conference on Financial Cryptography and Data Security (**FC**). 2019 (to appear)
- Karl Wüst, Sinisa Matetic, Moritz Schneider, Ian Miers, Kari Kostiainen, Srdjan Capkun
  ZLiTE: Zcash Lightweight Clients using Trusted Execution
  In Proceedings of the International Conference on Financial Cryptography and Data Security (**FC**). 2019 (to appear)
- Aritra Dhar, Ivan Puddu, Kari Kostiainen, Srdjan Capkun
  ProximiTEE: Hardened SGX Attestation and Trusted Path through Proximity Verification
- Sinisa Matetic, Moritz Schneider, Andrew Miller, Ari Juels, Srdjan Capkun
  DelegaTEE: Brokered Delegation using Trusted Execution Environments
  in **Usenix Security** Symposium, 2018
- Hubert Ritzdorf, Karl Wüst, Arthur Gervais, Guillaume Felley, Srdjan Capkun
  TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing
  in Proceedings of the Network and Distributed System Security Symposium (**NDSS**), 2018
- I. Bentov, Y. Ji, F. Zhang, Y. Li, X. Zhao, L. Breidenbach, P. Daian, and A. Juels.
  Tesseract: Real-Time Cryptocurrency Exchange using Trusted Hardware, 2017
- Sinisa Matetic, Mansoor Ahmed, Kari Kostiainen, Aritra Dhar, David Sommer,
  Arthur Gervais, Ari Juels, Srdjan Capkun
  ROTE: Rollback Protection for Trusted Execution
  USENIX Security Symposium, 2017
- Arthur Gervais, Ghassan Karame, Damian Gruber, Srdjan Capkun
  On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients
  In Proceedings of **ACSAC**, 2014

http://www.syssec.ethz.ch/research/publications.html

https://www.zisc.ethz.ch