TRIDEnT: Towards a Decentralized Threat Indicator Marketplace

Nikolaos Alexopoulos, Emmanouil Vasilomanolakis, Stéphane Le Roux, Steven Rowe, Max Mühlhäuser

ACM SAC 2020 DAPP Track

TECHNISCHE
UNIVERSITÄT
DARMSTADT

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Telecooperation Lab

AALBORG UNIVERSITET

école
normale
supérieure
paris—saclay

université
PARIS-SACLAY

lsv

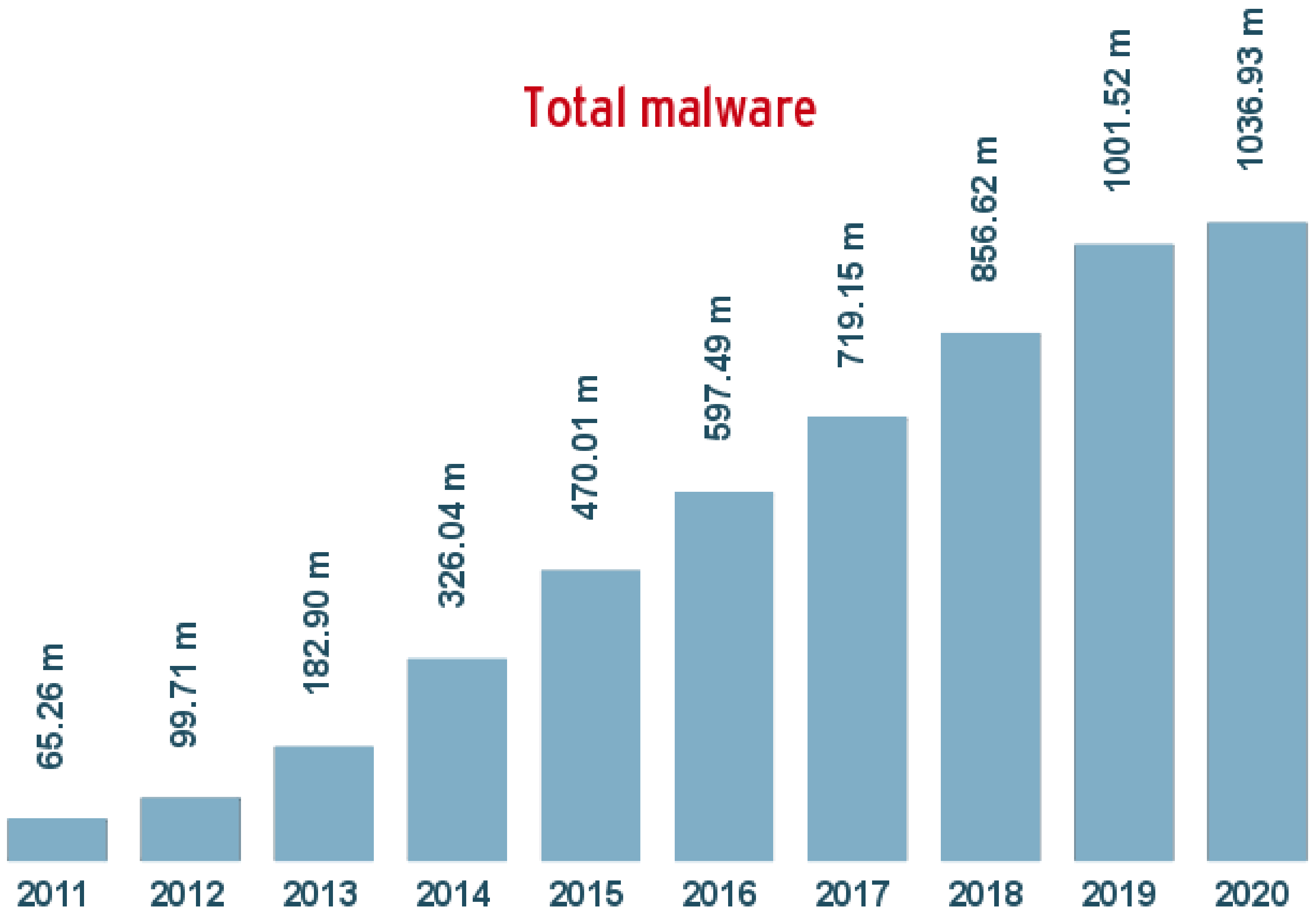
cnrs

Presentation structure

- Motivation
- Background
- Problem statement
- Related work
- The TRIDEnT approach
- Evaluation
- Limitations
- Conclusion

Andy Greenberg/WIRED: "Hackers Remotely Kill a Jeep on the Highway—With Me in It"

Threats are increasing



Last update: March 23, 2020

Copyright © AV-TEST GmbH, www.av-test.org

https://www.av-test.org

… and attacks are costly

- Average cost of a single security incident: 108k USD for SMBs (<1k employees), 1.4M USD for enterprises [2019 Kaspersky]. 1M USD [2018 Radware]
- Average damage from zero-day attack: 149k USD for SMBs, 2M USD for enterprises. [2016 Kaspersky]

[2019 Kaspersky] Kaspersky Labs. "IT security economics in 2019"

[2016 Kaspersky] Kaspersky Labs. "Report: Measuring the Financial Impact of IT Security on Businesses"

[2018 Radware] Radware blog. "The Million-Dollar Question of Cyber-Risk: Invest Now or Pay Later?"

Threat indicators [CISA 2015]

"Information that is necessary to describe or identify:

- […] a method of defeating a security control or exploitation of a security vulnerability
- […] the actual or potential harm caused by an incident
- […] any other attribute of a cybersecurity threat […]"

Examples:

- Malware indicator for file hash
- Zero-day vulnerability

Why sharing is caring

- Mitigation: If an org. detects/(falls victim) other orgs can be ready (e.g. zero-day, phishing email etc.).
- Detection (more subtle): Large-scale attacks may not be detectable without sharing (e.g. login attempts at different banks)

TI sharing drastically increases the effort/reward ratio for attackers

But organizations are reluctant

- Bad publicity / stock market
- Free-riding
- Leaking sensitive information
- …

Problem statement

- How to facilitate TI sharing?

?

Solutions in the wild

- "Most companies engage in informal peer-to-peer exchange of threat intelligence (65 percent of respondents) instead of a more formal approach" [2018 Ponemon]
- Exchange services and consortia (MISP, IBM's X-ForceExchange, Facebook's ThreatExchange)
- Government initiatives and legislation (e.g. Swiss SIGS ISAC, US CISCP)

[2018 Ponemon] Ponemon Institute. "Third Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way"

Open challenges

- Big companies have P2P channels e.g. Facebook may talk with Google about stuff. But what about smaller organizations (SMBs)?
- Trust in central party required (SPoF, legislative boundaries etc.)
- Free-riding

Related work in academia (selected)

- Gal-Or and Ghose [2005]: game-theoretic model --> information sharing beneficial **BUT** no additional incentives and anti-free-riding mechanisms --> not truthful
- Fung et al. [2011]: trust is important --> trust management system helps

[2005] Esther Gal-Or and Anindya Ghose. "The economic incentives for sharing security information."
[2011] Carol J Fung, Jie Zhang, Issam Aib, and Raouf Boutaba. "Dirichlet-based trust management for effective collaborative intrusion detection networks."

The TRIDEnT research question

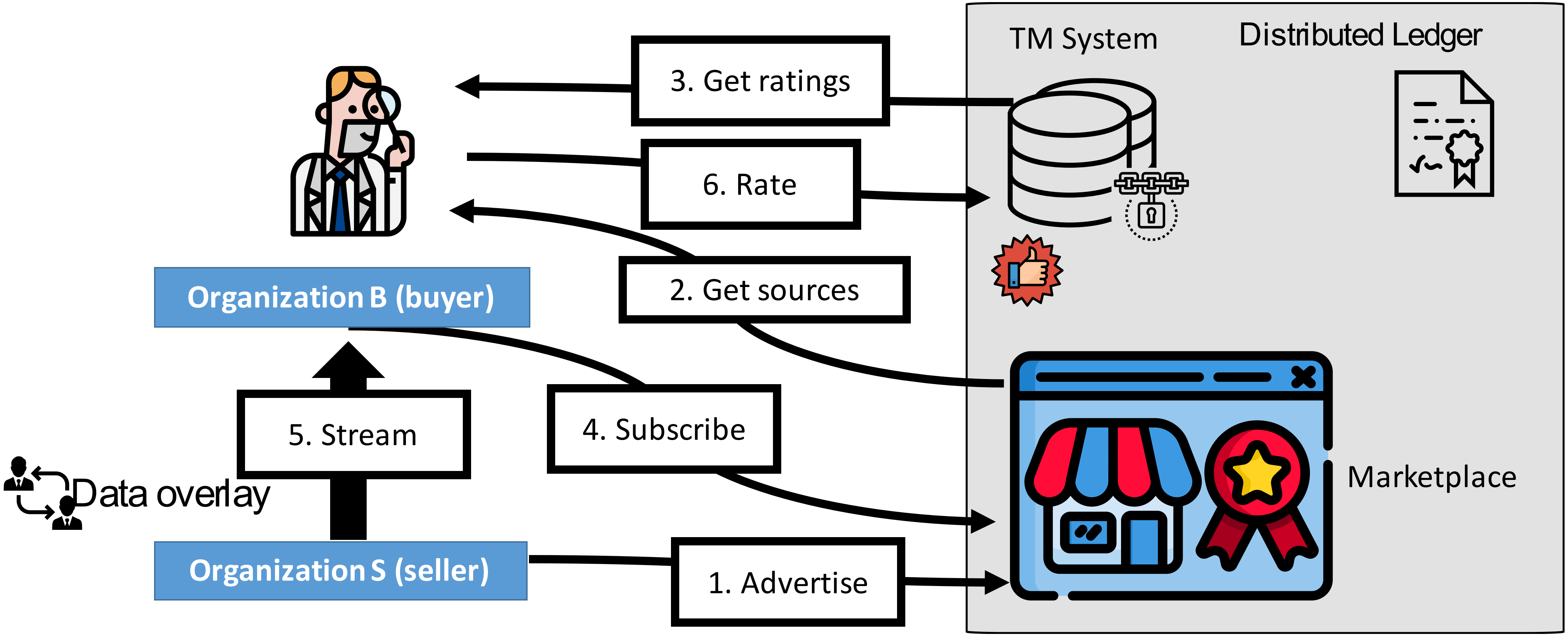
Is it possible to enable TI sharing?

- Without a central trusted party
- With built-in trust management and incentive mechanisms
- With low cost

The TRIDEnT approach in summary

- Use smart contracts to design a platform without a trusted moderator
- Tailor a marketplace for P2P streaming
- Bake in some simple incentive mechanisms and a trust management system
- Develop a prototype on Ethereum and test performance / costs
- More details in the following slides but make sure to check out our paper!

The TRIDEnT workflow

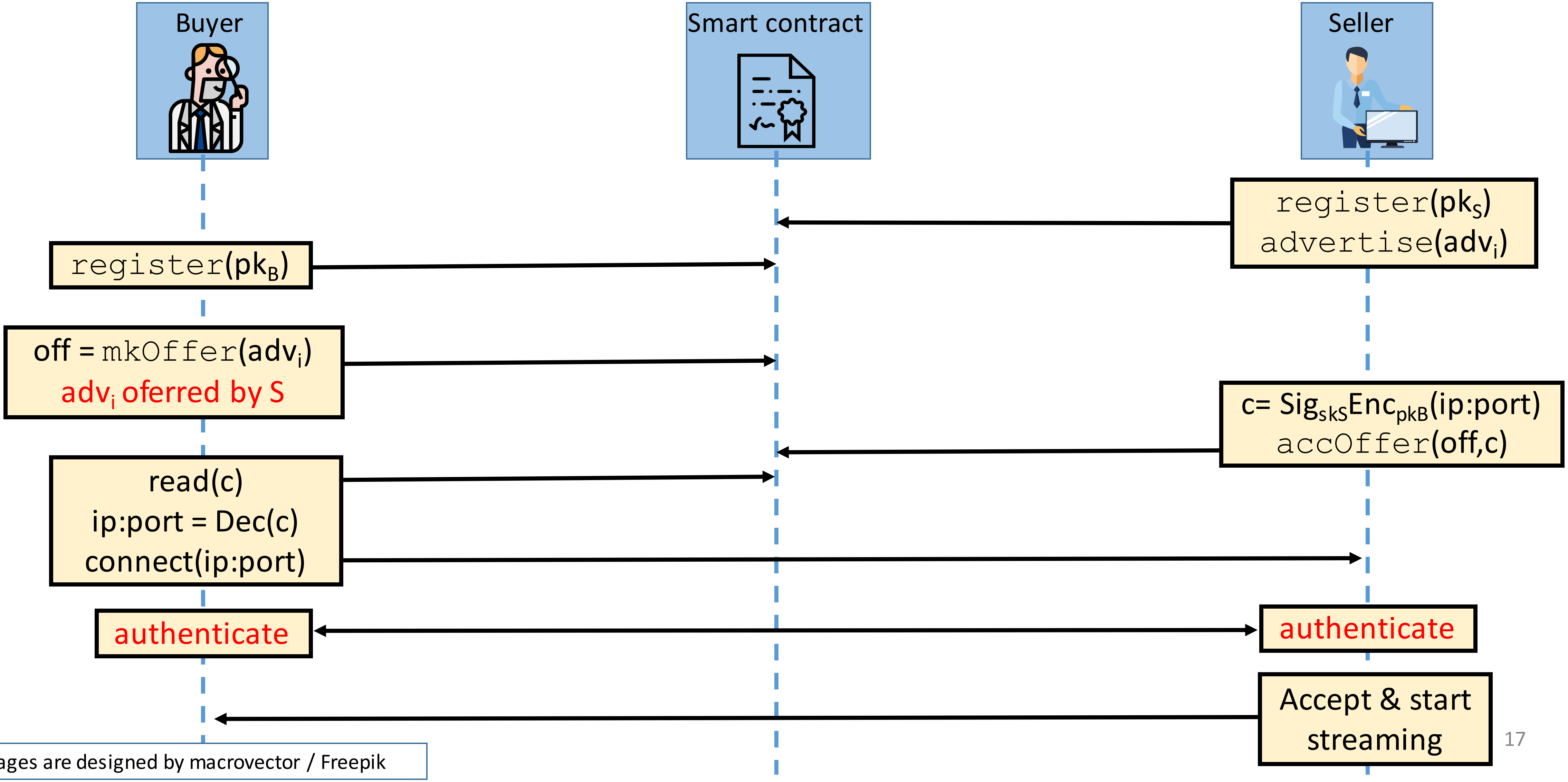


The basic functions of TRIDEnT

Function	Description	Constraints
`register`	Used for initial registration – burns currency	
`advertise`	Create new advert with chosen tags	
`rmAdvert`	Remove advert (+ related offers and subs)	
`mkOffer`	Create offer for advert	Deposit has to be made
`delOffer`	Delete offer	Caller == advert publisher
`accOffer`	Delete offer and create sub	Caller == advert publisher
`unsubscribe`	Delete sub	Caller == (advert publisher OR subsc.)

`rate`	Add rating	# ratings/sub == 1
		Caller == subscr.
		Timer not expired

Stream Establishment under the hood



Buyer

Smart contract

Seller

`register`(pk_S)
`advertise`(adv_i)

`register`(pk_B)

off = `mkOffer`(adv_i)
adv_i oferred by S

c= $Sig_{skS}Enc_{pkB}$(ip:port)
`accOffer`(off,c)

read(c)
ip:port = Dec(c)
connect(ip:port)

authenticate

authenticate

Accept & start streaming

*Some images are designed by macrovector / Freepik

Trust management design

- Trust bootstrapping: baseline trust via proof-of-burn
- Rating: incentive to rate with small deposit
- Local trust computation*: Bayesian evidence-based representation (CertainTrust)

* TRIDEnT is agnostic to the local trust computation algorithm that runs on the client side

Attacks and defenses

- Bad-mouthing and sybil attacks
  - Proof-of-burn incurs non-negligible cost for new identities
- Stream reselling
  - Trust required in both directions

Implementation on Ethereum

- Smart contracts in 427 lines of Solidity v0.4.25 (deployed and available on etherscan)
- Micro-transaction channels with micro-Raiden
- Client-side application in 2k lines of Javascript (Nodejs)

Gas costs

Function	Gas	Cost (Gwei*)	Cost (EUR-current*)	Cost (EUR-peak*)
deploy	3 994 723	15 978 892	2.04	99.68
register	54 672	218 688	0.03	1.36
advertise	173 279	693 116	0.09	4.32
rmAdvert	41 257	165 028	0.02	1.03
mkOffer	194 381	777 524	0.10	4.85
delOffer	25 820	103 280	0.01	0.64
accOffer	756 014	3 024 056	0.39	18.86
unsubscribe	34 139	136 556	0.02	0.85
rate	46 663	186 652	0.02	1.16

* 1 Gwei = 10^(-9) ETH
Considered Gas price = 4 Gwei
1 ETH = 127.86 EUR as of Mar. 24th 2020
Peak cost: Gas price = 22 Gwei, 1 ETH = 1134.20 EUR (Jan. 2018)

Limitations

- Privacy solutions (e.g. anonymization) implied but not implemented
- Stream reselling attack may require additional countermeasures
- Evaluation only "in the lab"

Conclusion

- Smart contracts can be a useful building block for incentives in TI sharing

TRIDEnT: Towards a Decentralized Threat Indicator Marketplace

Nikolaos Alexopoulos, Emmanouil Vasilomanolakis, Stéphane Le Roux, Steven Rowe, Max Mühlhäuser

ACM SAC 2020 DAPP Track

Mail questions to: <alexopoulos@tk.tu-darmstadt.de>

TECHNISCHE UNIVERSITÄT DARMSTADT

ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit

Telecooperation Lab

AALBORG UNIVERSITET

école normale supérieure paris–saclay

université PARIS-SACLAY

cnrs