NEXT
GENERATION
INTERNET

Open Call 2

Responsibility to protect population through peer governance and trusted community (P2PR2P)

Deliverable 3: Experiment Results and Final Report

Authors	Dr. Félix Blanc (coordinator, Danaides, felix@danaides.org); Pr. Richard Brooks ; M.A. Delphine Frenoux ; M.A. Stephanie Lamy ; M.A. Candice Duprix & M.A. Adeline Demoncy,
Due Date	November 2, 2021
Submission Date	November 30, 2021
Keywords	security; privacy; accountability; anonymity; trust; DLT; distributed governance

Deliverable 3: Part I

Analysis, results, and wider impact

1 Abstract

Danaïdes develops the P2PR2P (Peer-to-Peer Responsibility to Protect) software, which provides a secured platform that enables responsible and accountable common-pool-resources governance for humanitarian and human rights collective action. The project used FABRIC testbeds to validate the P2PR2P features with innovations and impact on three topics: (1) data protection and ownership through privacy features; (2) system accountability through audit trail using DLT technology and integrated KPIs.; (3) distributed governance to maximize user trust within the system. Clemson University, the US partner on this project, implemented the app, executed tests on a distributed network testbed, and analyzed data outputs with Danaides.

2 Project Vision

Danaides is a French NGO that has forged a partnership with Clemson University (US) and Sciences Po Toulouse (France) to develop the P2PR2P (Peer-to-Peer Responsibility to Protect) software, a secure common-pool-resource governance tool that manages user-driven requests and offers, matches and dispatches knowledge, relationships, and other humanitarian aid or content. Using distributed ledger technology, P2PR2P applies a trust economy model where decentralised hubs coordinate small transnational networks that share common goals.

The Clemson University Holcombe Department of Electrical and Computer Engineering works with Danaides to develop applications of advanced security and privacy technologies that protect at-risk populations stranded in hazardous environments. The integration of computer networking technologies into social science based applications has become essential, since the Internet has become a social construct built on a technical substrate.

P2PR2P captures all transactions and thereby formalises ad-hoc transnational networks of individuals working to ensure human security in complex/conflict environments. This helps integrate the “informal aid economy”, and enables the formalised groups to gain leverage with institutions governing human security.

P2PR2P users are given ownership of the intervention by adopting a “commons approach” where resources contributed are pooled, and pool usage is governed by a network of peers (P2P). Elionor Ostrom’s Nobel Prize winning work on commons theory has extensively enriched human security practices, such as sustainability and development. However, the commons approach to managing humanitarian aid and the human rights space, especially with regards to the United Nations principle of the Responsibility to protect (R2P), has been under-utilised.

Conceptualising humanitarian assistance through commons economic theory is challenged by preconceived notions that afflicted populations are in a constant position of demand for State goods and services, instead of peers capable of contributing and governing the resources necessary to accomplish collective action. Aid industry practices rarely attribute value to the beneficiaries when these contribute information or other resources necessary to organise assistance efficiently. This top-down approach undermines community-level resilience. The P2PR2P integrity model values a beneficiary’s contribution to the collective aid effort. Reciprocity between beneficiaries and donors engaged in collective action creates potential for peer governance of common resources. On an operations/coordination level, the commons approach to the humanitarian/human rights space in conflict/complex environments is complicated by remoteness, privacy and security issues. We tackle these difficulties by delivering accountability and resource sustainability through technology (DLT) and safety and connectivity issues are addressed by providing secure, robust, and context appropriate communication.

Co-funded by the Horizon 2020 Framework Programme of the European Union

This project has allowed us to test the robustness of P2PR2P on the FABRIC testbeds to verify our privacy and accountability technologies. This allowed us to evaluate their impact on peer-to-peer governance of humanitarian aid as common-pool-resources and test our assumptions using a human user network in Sub-saharan Africa.

P2PR2P displays 6 main features:

- **Peer governance**: Our deployment protocol guarantees ownership and control of community rules.
- **Security**: P2PR2P technology hides participant and server physical locations from unwanted surveillance.
- **Efficiency**: Demand-driven aid between peers eliminates unnecessary donor/beneficiary transactions, removes bottlenecks, and reduces duplication/overhead.
- **Accountability**: P2PR2P features an indelible secure audit trail (better-than blockchain distributed ledger).
- **Measurability**: P2PR2P captures all transactions and maintains forensics-grade meta data. KPIs are integrated.
- **Sustainability**: P2PR2P technology is a resource saving, resilient infrastructure.

3 Details on participants (both EU and US)

I. Experiment Coordination
Project leader: Dr. Félix Blanc

Dr. Félix Blanc is co-founder at Danaides.org and currently Faculty Teacher at Sciences Po Toulouse (Master Governance of International Relations headed by Pr. Benjamin Gourisse). From 2009 to 2014, he was a young expert at the Institute of Advanced Strategic Studies (IRSEM, Ministry of Defense, Paris) and research fellow at the Getulio Vargas Foundation in 2017. From 2014 to 2019, he was head of the desk Public policy and Institutions at Internet sans frontières (NGO, Paris).

He holds a M.A. and a Ph. D. in political science from the Ecole des Hautes Etudes en Sciences Sociales (Paris).

He has expertise in legal and ethical aspects of armed conflict, Internet technologies and digital rights. As a young expert for the Ministry of Defense, he conducted research on parliamentary control over military affairs and ethical dilemmas raised by weaponized drones. With the French NGO Internet Without Borders, he has worked on programs dealing

Co-funded by the Horizon 2020
Framework Programme of the European Union

with privacy, data protection and Internet governance including a four-year project sponsored by the U. S. State Department's Bureau of Democracy, Human Rights, and Labor. At Internet Without Borders, he conducted a jurisdictional survey for Ranking Digital Rights's Corporate Responsibility Index and expert research on submarine cables and Internet governance (privacy, affordability, connectivity, neutrality). He organized several sessions on global infrastructure and human rights at the RightsCon summit and the Internet governance forum.

II. Experiment 1: Verify the security and privacy of our network connections

Project leader: Pr. Richard Brooks

Pr. Richard Brooks is a professor of computer engineering with Clemson University, Clemson, SC, USA.

He has a BA from The Johns Hopkins University and a PhD from the Louisiana State University.

His research concentrates on information assurance, battlespace coordination, behavior pattern extraction/detection and game theory. His network security research projects have included funding from NSF (analyzing wired and wireless denial of service vulnerabilities), DoE (authentication and authorization of exa-scale storage systems), BMW Corporation (controlling dissemination of intellectual property), and the US State Department (creating anonymous communications tools for civil society groups). It frequently looks at attacks that disable security measures by working at a different level of the protocol stack. His Internet freedom work involves interactions with at risk populations working for freedom of expression.

Dr. Brooks has used the GENI testbed in the past for network security experimentation. He has specifically used GENI to stage and analyze live distributed denial of service (DDoS) attack experiments and experiment on increased communications anonymity. Clemson was a major participant in the GENI program. Clemson is one of the development centers for the FABRIC testbed and Dr. Brooks is one of the investigators in the NSF FABRIC across borders project. He is a member of their design and development ecosystem. These ties allowed Danaides to be integrated into the FABRIC deployment process as an early beta test use case.

III. Experiment 2: Audit trail verification and system accountability

Project leader: Delphine Frenoux

Delphine Frenoux is an economist who worked for 10 years in the French Development Agency's Group (AFD).

She graduated from the Political Sciences Institute in Aix-en-Provence and holds a Master Degree in Economics of Development from the CERDI, a Research Center on International Development attached to the CNRS (French National Center for Scientific Research).

She joined the AFD in 2007 as Investment Officer at the regional office of Proparco for Southern Africa, based in Johannesburg. In 2009, she became Project manager at the Banking and Microfinance Department of Proparco in Paris. During 5 years, she structured debt financing and equity investments in Africa and Emerging economies (Brazil, Turkey, Argentina…). After a break of 2 years in Brazil where she joined KPMG Strategy Group in Rio de Janeiro as a senior consultant in corporate strategy, she returned to AFD at the Research department as a Macroeconomist in charge of sovereign and country risks analyses (Brazil, Egypt, Mozambique, Chad and Cameroon notably).

She is now an independent consultant. She developed a full investment memorandum and business plan for the MUCODEC, which is the main microfinance network in the Republic of Congo. She also taught Macroeconomics at the University of Auvergne. And in her spare time, she is Deputy Mayor of the 3rd sector in Marseille in charge of Finance and Social Economy.

Those experiences gave her a solid expertise both on the macroeconomic and microeconomic aspects of economic development.

IV. Experiment 3: Establish the quality of distributed governance strategies designed to maximize user trust within the system.

Project leader: Stephanie Lamy

Stephanie Lamy co-founded Danaides with Dr. Félix Blanc and currently Faculty Teacher at Sciences Po Toulouse (Master Governance of International Relations headed by Pr. Benjamin Gourisse). Previously she acquired 15 years of experience as a senior manager (commercial, logistics and staff) with an expertise in change management in the luxury retail industry. In 2011 she pivoted her career to strategic communications in order to support civil society actors organising humanitarian aid to conflict zones such as Yemen, and founded the NGO Global Relief Libya. From 2012 to 2016 she was Internet Without Borders (ISF) Secretary General.

In 2019 Ms. Lamy obtained a Master 2 (research track) in Governance of International Relations from Sciences Po Toulouse and has written a book on civil society spaces and disinformation (Editions du Detour, to be published in January 2022) while pursuing a PhD.

Ms Lamy is an authority on disinformation campaigns and other deceptive collective actions. Her investigation into election meddling is cited by the Atlantic Council report “Anatomy of the Macron Leaks” and she has published a study on the US Stop The Steal campaign. Previously, her analysis of communications usage by civilians victims of conflict has been featured in numerous reports including a French ministry of defense study on social media use in conflict settings. She has co-authored a book on mass-surveillance and her work with Libyan and Yemeni civil society actors (humanitarian, media, civil security) prompted an invitation to participate in the working group of the Cyberdefense chair of the Saint-Cyr military academy in 2013-2014 and is the foundation of the P2PR2P platform.

V. Operational deployment & traffic generation

Project leaders: Candice Duprix & Adeline Demoncy

Co-funded by the Horizon 2020
Framework Programme of the European Union

Candice Duprix is an international consultant in the sector of international solidarity and also a temporary teacher for the Master Governance of International Relations at Sciences Po Toulouse.

After a background in event management in the organisation and management of large-scale trade shows, she has acquired expertise in logistics and project management. It was during her personal involvement as a volunteer with the French Red Cross that she decided in 2011 to make this commitment her new professional project.

After obtaining her Master's degree in International Cooperation and Solidarity (University of Evry), she quickly joined the associative sector which led her in 2013 to join the NGO CARE France with whom she worked for 6 years. As Africa Programs Manager, Candice Duprix has acquired expertise in the management and development of numerous complex, multi-partners and multi-sectoral projects, particularly in the Sahel in the fields of health, gender-based violence, education, resilience and economic recovery.

Today, she pursues her mission as an independent consultant by supporting various organisations in the design and piloting of their emergency and development projects.
Her mastery of the entire project cycle and her knowledge of the Chadian context and of Sahelian issues in general make her an asset for the operational deployment of the P2PR2P project.

Adeline Demoncy is a consultant specialised in strategy and development of international cooperation projects. She also teaches at Science Po Toulouse (Master Governance of International Relations).

Business School (Sup de Co) graduate, she worked for a few years in London as a Human Resources manager. Aware of the challenges of HIV/AIDS prevention at an early age she turned to a professional career and worked for more than 10 years in the fight against HIV in France and internationally.

In 2008, she obtained a Master's degree in Political Science at the Sorbonne, with a specialisation in International Cooperation, Humanitarian Action and Development Policy. She joined the French Ministry of Foreign Affairs in 2010. As a political advisor, she was in charge of steering the programmatic and operational strategy of the French Development Agency. In parallel, she works on the elaboration of the French humanitarian Strategy and is a member of the Crisis Centre with which she takes part in several emergency missions.
In 2015, she joined the French Agency for International Technical Expertise as Health Systems Strengthening Project Manager in Sub-Saharan Africa with a focus on the Sahel region, particularly Chad. She works on the engineering and implementation of international solidarity projects in partnership with civil society, NGOs and institutional partners.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4 Results

Overall results are as follows:

A. Experiment 1: Verify the security and privacy of our network connections

- FABRIC was used to run a series of network experiments that illustrated the security properties that were desired. Invasive network experiments. This involved using the P4 FPGA programming language to modify the network stack and introduce timing features. We found that timing features were, in essence removed by Tor infrastructure.
- Tor hidden services provide **much greater anonymity** than normal Tor use;
- Our users are provided **reliable anonymity by our current design** and Tor's countermeasures against side-channels are adequate for our application; however,
- The documented recent purchases of netflow data by third parties could be used to **deanonymize normal Tor use.**[1]

B. Experiment 2 : Audit trail verification and evaluation metrics to measure system operations accountability

a. Audit trail verification

The security properties that we prove analytically for our audit trail are:

- **Immutability**
- **Data integrity**
- **Non-repudiation, and**
- **Consensus.**

These properties were proved analytically rather than experimentally. For this portion, the failure of experimental attacks would have been less strong. Failure might have, for example, been due to flaws in the attack process. An analytical proof of the impossibility of loss of these properties, in a properly implemented instance, is a much more powerful result. In addition, the available resources for an audit trail experiment, on the ground and in the testbed, was not adequate for performing an at scale experiment. Network testbeds were not required for the analytical work. While working to design the experiments, we realized

[1] https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru

Co-funded by the Horizon 2020
Framework Programme of the European Union

that failure of these audit trail properties could be shown based on basic principles. We therefore successfully pursued that approach rather than using physical experiments.

b. System operations accountability

The experience was also used to conduct an evidence-based monitoring and evaluation of measurable key indicators with regards to system accountability. Our quantifiable set of values was sourced from key performance indicators integrated into user surveys through analysis of data. We reached **our target value of 70%** for measurable KPIs.

- **Front-end operations functioning indicator:** 76% of the users consider that P2PR2P works well. Only 15% of the users find the platform unsatisfactory.
- **Efficiency indicator:** 82% of the users find the application easy to use.
- **Indicator of met needs:** 80% of the users consider that P2PR2P meets their needs.
- **Back-end operations functioning indicator**: 82% of the users community successfully synchronized the collected information with the victims to the database.

This experimental analysis was based on data collected in the field and not from testbed results.

C. Experiment 3: Establish the quality of distributed governance strategies designed to maximize user trust within the system.

A system that records all tasks associated with collective action enhances the perception by admin and users of the security and privacy of the system which in turn **augments the system's perceived trustworthiness.** We reached **our target value of 70%.**

- 74% of users say the combined score of collective action was very/helpful.

- 83% of participants surveyed perceived our system to be secure.
- Only 26% don't wish to see more performance indicators of collective action in the next version of the application.

This experimental analysis was based on data collected in the field and not from testbed results.

4.1 Discussion and Analysis on Results

1. Verify the security and privacy of our network connections

Co-funded by the Horizon 2020
Framework Programme of the European Union

We accessed FABRIC for network experimentation. All of these activities assume that we are able to keep user communications private. Unfortunately, this assumption is quite difficult to assure in practice. One of the main problems with proving the privacy of communications, in practice, is the fact that the problem is largely asymmetric.

We see FABRIC as a tool that can provide network researchers access to network traffic that is comparable to the access provided by a national firewall. This year was spent defining experiments that can use FABRIC to test the ability of existing anonymization approaches to hide Internet use in practice. We tested the existing anonymization approaches including the Onion Router (Tor) – especially Tor hidden services. In Tor, each connection is encrypted 3 times and takes multiple hops through a large network of volunteers. In hidden services, the connection is made to a port that is kept open somewhere in the middle of the volunteer network;

In particular, the current EU/NGI Danaides project is building a tool for UN-funded human rights defenders providing legal assistance to women victims of gender based violence in remote areas of Chad. This tool is a secure platform for volunteer paralegals to collect information from these victims and allow for their headquarters to provide legal advice. It is imperative to protect the identities of the paralegals as well as the testimonies of these women. Our current implementation uses Android mobile devices interacting with a Tor hidden service.

We have done previous work to analyze the anonymity of Tor hidden services. We accept as given that the cryptography used in Tor is sound, since Tor uses open source implementations of standardized peer-reviewed cryptography algorithms. These tools are the current gold-standard for network security. Tor leverages NIST approved standardized ciphers and protocols. NSA experts augment existing NIST expertise in certifying the cryptographic approaches used. Our previous work found potential timing side-channels in Tor. We could associate the circuit source and destination in a private Tor network in our laboratory, but found that this passive attack was not practical on the global Tor network.

We routed traffic from the Danaides mobile devices through FABRIC into a hidden service. Traffic has been sampled leaving the Android devices and going to the hidden service. We have used FABRIC's P4 networking stack implementation to create a type of man-in-the-middle attack that lets us tamper with traffic and observe the results. This sort of intervention is common in nation-state firewalls. Side-channels we explore in Tor include:

- Inserting inter-packet delay patterns to see if they propagate through the network session so that delays introduced as traffic enters Tor can be used to reliably find Tor exit locations;
- Creating bit flip errors in selected network packets. These packets will be rejected causing retransmission events to occur. The hypothesis is that these stream interruptions will be detectable throughout the entire communications circuit; and
- Application of the machine learning tools in FABRIC in order to discover subtle identifying characteristics of these streams that we had not anticipated.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Work to date included:

- Implementation of network traffic generation process for Danaides;
- Network experiment planning;
- Learning P4 programming using the Rutgers testbed, with assistance provided from Ivan Seskar of NGIatlantic.eu;
- On-boarding onto the FABRIC platform;
- Implementation of experiment

Network Security Work. Our application design has the Android handsets store transactions in JSON files locally. When they reach a location with secure Wi-Fi, they synchronize with our Tor hidden service. This consists of uploading new transactions and downloading changes to their open requests. Since our users are in at-risk regions, which are often under the control of hostile groups, we do not want our users to be identified.

To avoid exposing our users, and provide extra security, our server is configured to work as a Tor hidden service. Tor is like a VPN, except that all connections are encrypted 3 separate times and take random hops through a cloud of volunteer nodes spread across the globe. Normally a client connection enters the Tor cloud and a randomly chosen exit node works as a proxy for the client. There are some potential issues with this approach:

- Tor does not hide the fact that you are using Tor. Since this has caused problems for Tor users in many countries, notably Iran and China block Tor use, many projects have been funded to develop pluggable transports to hide Tor use.[2]
- Correlation attacks are possible, where traffic from the client can be mapped to traffic leaving the Tor exit node by correlating the packet sizes and timing patterns with packets leaving a Tor exit node.

The second problem has been largely ignored, since it requires global visibility of the Internet. Exit nodes are distributed over the whole world. It was felt that few opponents would have the global surveillance infrastructure needed to execute these attacks. It was revealed in August 2021[3] that this is not a reasonable assumption. ISPs are willing to sell this information.

To establish whether or not our traffic is vulnerable to this type of attack, Danaides used the new FABRIC testbed to run a series of experiments[4]. FABRIC was chosen since its design gives a degree of network access/control that was previously impossible. Experimenters can access/modify/control the network at all possible levels. This is done by putting FPGAs in the network paths. (Field Programmable Gate Arrays are a type of reprogrammable hardware. They have performance similar to custom design silicon chips, but can be rewritten (almost) as easily as software. For FABRIC, these FPGAs are designed to already have a full TCP/IP network implementation.) The actual network can be easily modified without appreciably

[2] Notably, our Clemson partners have had a number of projects of this type and are implementing a system to encode Tor browser traffic into Minecraft video game sessions.

[3] https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru

[4] https://fabric-testbed.net/

degrading performance. This gives the experimenter basically capabilities comparable to China's great firewall, but without the sizable financial investment.

FABRIC[5] is, however, a brand new facility, with nodes just coming online. Therefore, to access FABRIC, we were designated to be alpha testers of their environment via this EU-US NGIatlantic.eu project opportunity, which made it possible for us to become the first people to use their system, which required extra effort. We became the first people to use their system, which requires extra effort. FABRIC deployment was slowed, in part, due to the inability of vendors to provide FPGAs because of the ongoing supply chain bottlenecks cuased by a lack of computer chips This slowed our access to the system. We ended up using P4 software for performing our attacks without the FPGA hardware support. For many FABRIC tests, which are geared towards network throughput, this would have been a severe hindrance. Since our work was looking at network flow patterns, the change from hardware to software based traffic tampering was not a major problem. The reprogrammable hardware has the same programming language as the software version. The hardware is capable of providing greater throughput, but our goal was not getting impressive throughput, It was tampering with the network flows, which the software interface was adequate for doing.

Much of our work could have been done using other testbeds, notably GENI, which we have experience using and we often considered changing our plans. In the end we did not use GENI, since FABRIC satisfied our needs and using GENI would have caused us to duplicate our effort. FABRIC's allowing us to work within the network stack was cleaner than the GENI configuration we had considered. With GENI we would have routed our traffic through intermediate nodes performing what is essentially a standard man-in-the-middle attack. When proposing the work, we knew we could fulfil our obligations using GENI based on our previous experience wit the testbed. We were enthused about the new possibilities provided by FABRIC, but FABRIC was still in the design phase so we could not know iwhether or not it would satisfy all of our needs. In the end, FABRIC's new functionality was able to satisfy our requirements and did not require the duplication of effort that would have been needed to use both testbeds.

However, we ended up using the FABRIC environment with software emulations of the programmable hardware.. This ultimate decision benefited our experiments, which enabled the team to to set up connections from our P2PR2P app to our hidden service, passing through FABRIC. We would then observe the network traffic at both ends. We would then perturb traffic going into the Tor cloud, which an informed attacker would do, in order to detect the disturbance patterns on traffic leaving the Tor cloud. Fabric's capabilities enabled this by:

- Giving us invasive access to observe the software flows as they entered the Tor network and left Tor to access our hidden service;
- Using the P4 network stack implementation to insert network traffic tampering logic; and
- Mixing our experimental traffic with normal Tor traffic as our network sessions left FABRIC temporarily to use Tor's anonymity service.

[5] https://fabric-testbed.net/

Co-funded by the Horizon 2020
Framework Programme of the European Union

Our hypothesis was that this type of attack could negate the anonymity provided by Tor. Attackers with money could purchase netflow data from various networks and then identify if individual users were in fact using P2PR2P. This would be done by identifying timing disturbances in the nodes traffic stream from their mobile device to our hidden server.

Our experiments determined that this hypothesis is not true. The first surprise is that the hidden service does not maintain one Tor circuit per user within the Tor cloud. We must note here, that a hidden service is technically embedded entirely within the Tor cloud. All of the server's incoming traffic is bundled into a single encrypted data stream while passing over the network. Once received at the server, this traffic is decrypted and separated into a number of independent data streams sent to the loopback (127.0.0.1) IP address. At that level we could detect the traffic, but for that to work the attacker would need direct access to the server. In which case, the attacker could read our databases directly.

In the past, we have managed to identify specific data streams from within bundled encrypted connections.[6] We note that this ability is not widely shared. Our ability to successfully do these attacks on smart grid systems relied heavily on two aspects of that traffic:

1. Different devices would produce packets of different uniform sizes. Tor cuts all packets into uniform packet sizes, which removes this side-channel; or
2. The smart grid devices produced data streams that sent each packet after a uniform time period. Our traffic is driven by machines sending/receiving files. Our traffic will be sent in small bursts of activity.

Both of these side-channels do not exist in this case. . Recent revelations show that netflow data can be purchased.[7] This fact makes the Tor anonymity network's security model less ironclad. Tor assumes that no one has a global view of the Internet, so that flows going into and out of Tor can not be correlated. In the past, this global view could reasonably have been limited to a small number of actors. With the purchase of netflow data being a reality, the Tor assumption should not be accepted out of hand. To match a data flow from one of our users to our hidden server, one would have to:

- ○ Find all of our user sessions;
- ○ Sum the volume of their traffic;
- ○ And correlate that incoming sum to the traffic from our server to the next hop on its Tor session.

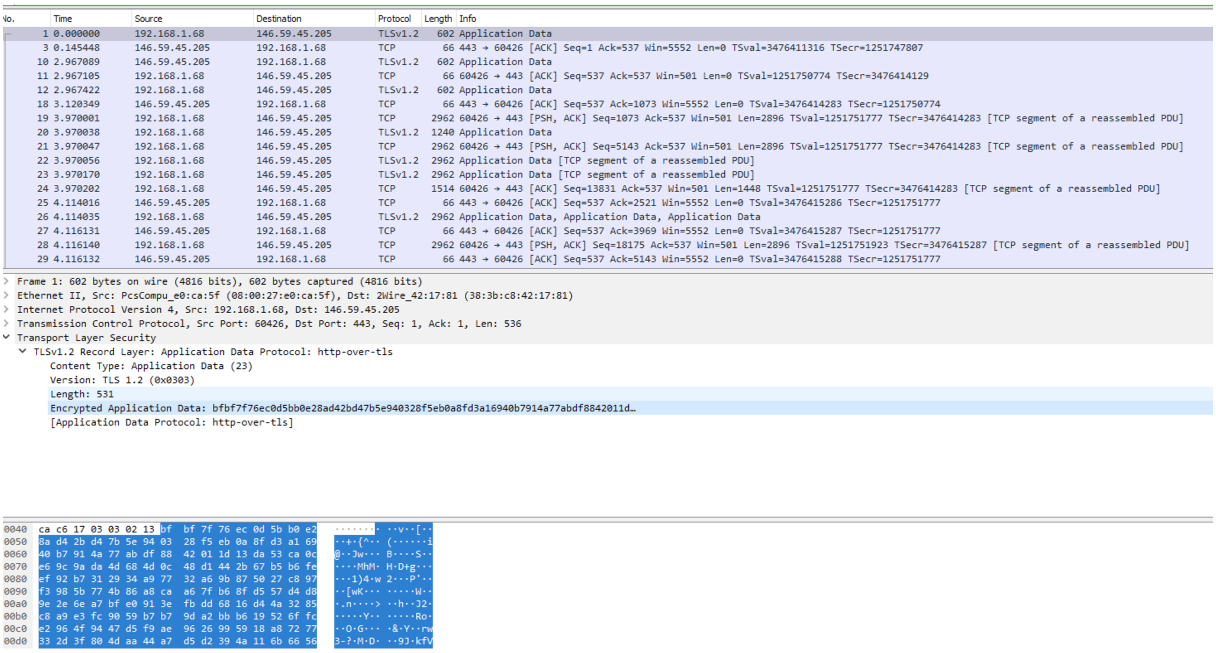
While this process may not technically be impossible, it would require a global view of all of our user traffic and assume that there are no other combinations of traffic that would correlate well with our server traffic Since our traffic volume is not large and amounts to

[6] X. Zhong, I. Jayawardene, G. K. Venayagamoorthy, and R. R. Brooks, "Denial of Service Attack on Tie-Line Bias Control in a Power System with PV Plant" IEEE Transactions on Emerging Topics in Computational Intelligence, 1(5), 375-390 (2018).

[7] https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru

Co-funded by the Horizon 2020
Framework Programme of the European Union

periodic transfers of small to medium sized files, one can assume that multiple network sessions will have profiles not terribly different from our users. Similarly, the number of network sessions going into and out of Tor is large. Many connections are heavily obfuscated using pluggable transports to hide the use of Tor. It is likely that many sessions not using our app could be combined to match the traffic to/from our hidden server quite well. Computing sums of reasonable traffic flows to find a possible match would suffer from a substantial combinatorial explosion. While it would be theoretically feasible that the sum of traffic flows from Danaides apps would be the best fit to the traffic flow entering/leaving our hidden service, collecting and evaluating the data to find this match would be prohibitively expensive. It is unlikely that this attack would be performed in practice. We expect that the cost of the resources required to perform this attribution would be orders of magnitude higher than the gains that could be expected by the attacker.



```
No.   Time        Source          Destination     Protocol Length Info
    1 0.000000    192.168.1.68    146.59.45.205   TLSv1.2   602 Application Data
    3 0.145448    146.59.45.205   192.168.1.68    TCP        66 443 → 60426 [ACK] Seq=1 Ack=537 Win=5552 Len=0 TSval=3476411316 TSecr=1251747807
   10 2.967089    146.59.45.205   192.168.1.68    TLSv1.2   602 Application Data
   11 2.967105    192.168.1.68    146.59.45.205   TCP        66 60426 → 443 [ACK] Seq=537 Ack=537 Win=501 Len=0 TSval=1251750774 TSecr=3476414129
   12 2.967422    192.168.1.68    146.59.45.205   TLSv1.2   602 Application Data
   18 3.120349    146.59.45.205   192.168.1.68    TCP        66 443 → 60426 [ACK] Seq=537 Ack=1073 Win=5552 Len=0 TSval=3476414283 TSecr=1251750774
   19 3.970001    192.168.1.68    146.59.45.205   TCP      2962 60426 → 443 [PSH, ACK] Seq=1073 Ack=537 Win=501 Len=2896 TSval=1251751777 TSecr=3476414283 [TCP segment of a reassembled PDU]
   20 3.970038    192.168.1.68    146.59.45.205   TLSv1.2  1240 Application Data
   21 3.970047    192.168.1.68    146.59.45.205   TCP      2962 60426 → 443 [PSH, ACK] Seq=5143 Ack=537 Win=501 Len=2896 TSval=1251751777 TSecr=3476414283 [TCP segment of a reassembled PDU]
   22 3.970056    192.168.1.68    146.59.45.205   TLSv1.2  2962 Application Data [TCP segment of a reassembled PDU]
   23 3.970170    192.168.1.68    146.59.45.205   TLSv1.2  2962 Application Data [TCP segment of a reassembled PDU]
   24 3.970202    192.168.1.68    146.59.45.205   TCP      1514 60426 → 443 [ACK] Seq=13831 Ack=537 Win=501 Len=1448 TSval=1251751777 TSecr=3476414283 [TCP segment of a reassembled PDU]
   25 4.114016    146.59.45.205   192.168.1.68    TCP        66 443 → 60426 [ACK] Seq=537 Ack=2521 Win=5552 Len=0 TSval=3476415286 TSecr=1251751777
   26 4.114035    192.168.1.68    146.59.45.205   TLSv1.2  2962 Application Data, Application Data, Application Data
   27 4.116131    146.59.45.205   192.168.1.68    TCP        66 443 → 60426 [ACK] Seq=537 Ack=3969 Win=5552 Len=0 TSval=3476415287 TSecr=1251751777
   28 4.116140    192.168.1.68    146.59.45.205   TCP      2962 60426 → 443 [PSH, ACK] Seq=18175 Ack=537 Win=501 Len=2896 TSval=1251751923 TSecr=3476415287 [TCP segment of a reassembled PDU]
   29 4.116132    146.59.45.205   192.168.1.68    TCP        66 443 → 60426 [ACK] Seq=537 Ack=5143 Win=5552 Len=0 TSval=3476415288 TSecr=1251751777

> Frame 1: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits)
> Ethernet II, Src: PcsCompu_e0:ca:5f (08:00:27:e0:ca:5f), Dst: 2Wire_42:17:81 (38:3b:c8:42:17:81)
> Internet Protocol Version 4, Src: 192.168.1.68, Dst: 146.59.45.205
> Transmission Control Protocol, Src Port: 60426, Dst Port: 443, Seq: 1, Ack: 1, Len: 536
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 531
      Encrypted Application Data: bfbf7f76ec0d5bb0e28ad42bd47b5e940328f5eb0a8fd3a16940b7914a77abdf8842011d…
      [Application Data Protocol: http-over-tls]

0040  ca c6 17 03 03 02 13 bf  bf 7f 76 ec 0d 5b b0 e2   ········ ··v··[··
0050  8a d4 2b d4 7b 5e 94 03  28 f5 eb 0a 8f d3 a1 69   ··+·{^·· (······i
0060  40 b7 91 4a 77 ab df 88  42 01 1d 13 da 53 ca 0c   @··Jw··· B····S··
0070  e6 9c 9a da 4d 68 4d 0c  48 d1 44 2b 67 b5 b6 fe   ····MhM· H·D+g···
0080  ef 92 b7 31 29 34 a9 77  32 a6 9b 87 50 27 c8 97   ···1)4·w 2···P'··
0090  f3 98 5b 77 4b 86 a8 ca  a6 7f b6 8f d5 57 d4 d8   ··[wK··· ·····W··
00a0  9e 2e 6e a7 bf e0 91 3e  fb dd 68 16 d4 4a 32 85   ·.n····> ··h··J2·
00b0  c8 a9 e3 fc 90 59 b7 b7  9d a2 bb b6 19 52 6f fc   ·····Y·· ·····Ro·
00c0  e2 96 4f 94 47 d5 f9 ae  96 26 99 59 18 a8 72 77   ··O·G··· ·&·Y··rw
00d0  33 2d 3f 80 4d aa 44 a7  d5 d2 39 4a 11 6b 66 56   3-?·M·D· ··9J·kfV
```

Figure 1. Tor traffic trace collected on FABRIC.

Our initial hypothesis was that the anonymity provided by Tor could, at best, be 1/*n* where our service has *n* users. This was based on an attacker's ability to sniff traffic from both our (hidden) service and our set of *n* clients. This gives the attacker many advantages that they may not have in practice, since finding our hidden service is non-trivial[8], but not impossible. We wanted to verify the attacker's ability to determine specific clients out of the set of *n* clients using our hidden service. Surprisingly, while the traffic that can be observed on the hidden service's side is not individual sessions, but rather the aggregate traffic of a set of sessions, this means that the attacker does not have to consider only our set of *n* users. This

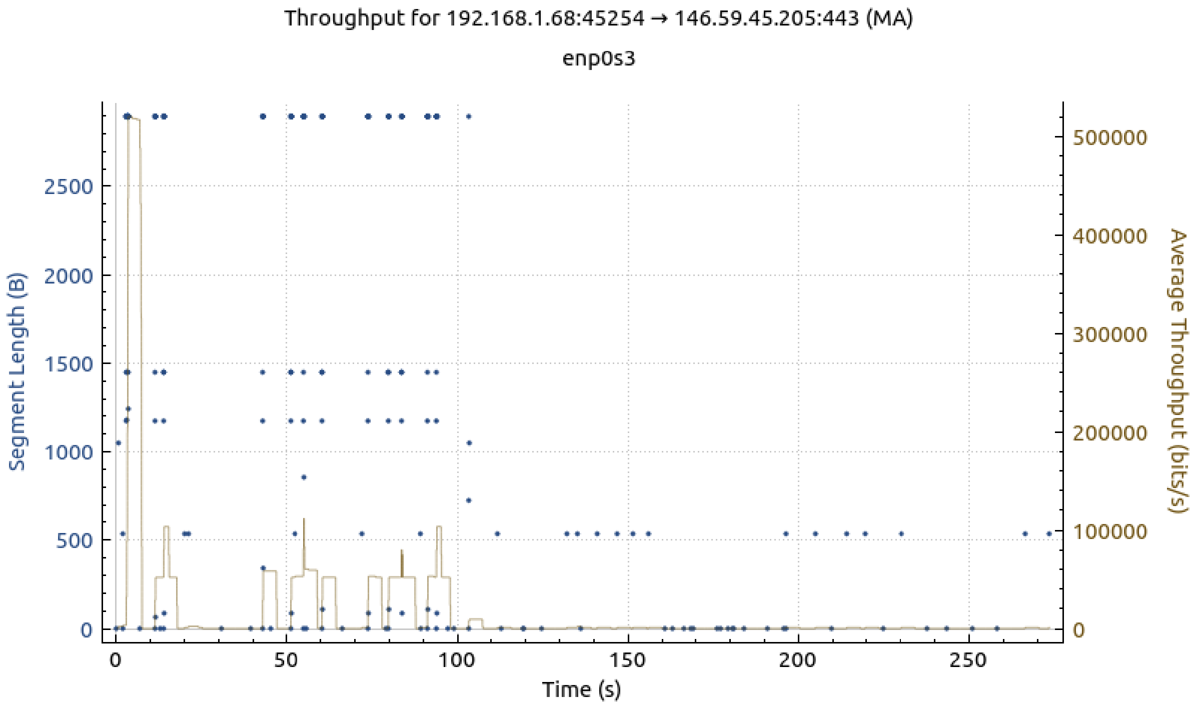
[8] Some work has been done on identifying servers using Tor, which have some limited success using timing side-channels to infer lIP address https://dl.acm.org/doi/abs/10.1145/2810103.2813667?casa_token=-7U4cEgvXGEAAAAA:cY6q49ncNfThdGM9NcymKgh9m_03roQm9doBgbbJMCaUXukr5YZJdOxXuh78b-oVa9U76lDDzpCO or physical location https://dl.acm.org/doi/abs/10.1145/1180405.1180410?casa_token=eOfVoA1JINIAAAAA:CglH1TsXloTncQ1SkjRQG4MivKjc4naEYsLMSSHZXbpvqoBAoTg9sd_OrguG5pCqUw11AfX8PaMV

Co-funded by the Horizon 2020
Framework Programme of the European Union

means that the attacker has to consider partitions[9] of the set of all *NT* users of Tor. This partition will have the cardinality defined by the Bell number $B_{NT,}$ where:

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

At which point, they need to maintain a list of all subsets where the aggregate traffic volume of the clients are on the order of the traffic volume observed at our hidden server's location. From the set of subsets retained, they then need to consider those nodes who have traffic volumes on the order of magnitude of our client. Since our clients send and receive files of rather modest size, it is most likely that this set of nodes will be of much greater cardinality than the set of our users. Finding the best set of users to match the observed traffic becomes a combinatorial optimization problem. While we are not providing a formal complexity proof, it is well accepted that combinatorial optimization problems are typically intractable since they are NP-complete. It is also almost certain that all of our clients will be present in multiple partitions. It is unlikely that our user community would be exposed by tor network traffic observation. If the number of Tor users is small in a specific country, or if Tor is blocked, users could be compromised. In which case, we will need to hide Tor use. This type of traffic obfuscation is done by using "pluggable transports" (PTs). Many PTS are being developed, and Clemson is actively involved in that effort. The other mode of compromise, which is most common, is for the attacker to either blackmail members of the network or insert confidential informers into our client user base. The second mode of attack is not one that technology is well suited to solving.



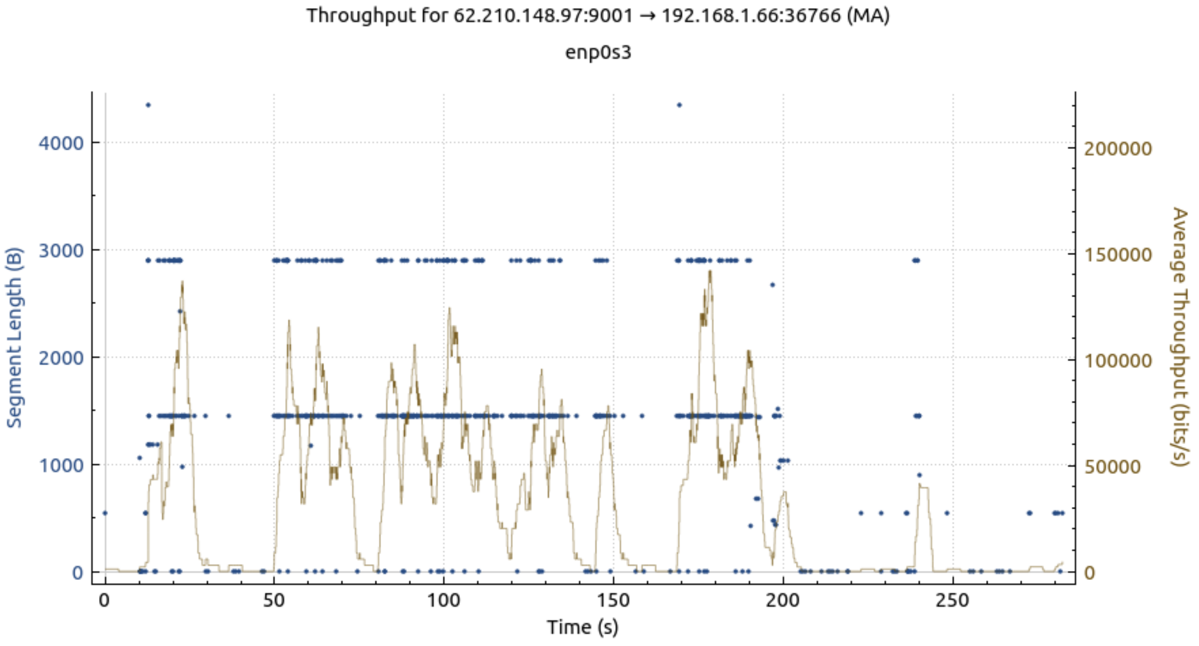
(a) Client Throughput - 512kB File

[9] In set theory, a partition is the set of non-null subsets of a set.

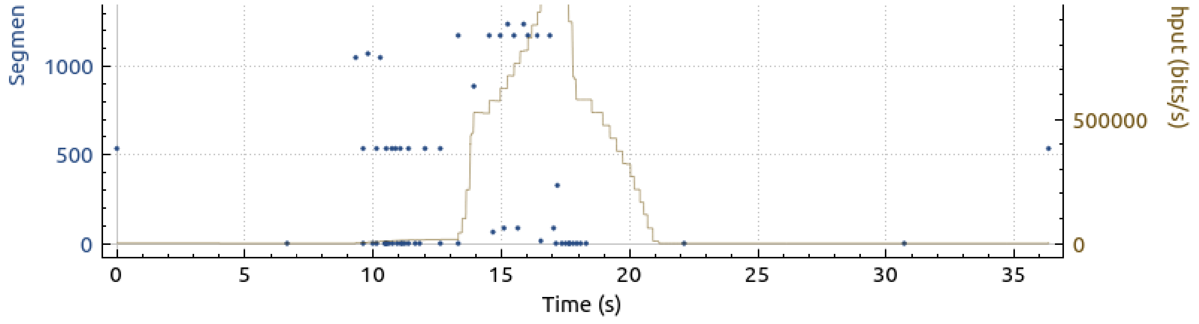
Co-funded by the Horizon 2020
Framework Programme of the European Union

This establishes that the privacy provided by using Tor hidden services is greater than anticipated. Our target goal of 1/*n* was wildly conservative.

The next test was to insert traffic disturbances at the server end and see if that resulted in detectable changes on the client's end. We inserted a process that corrupted up to 50% of the network traffic without finding a detectable change on the client's end.

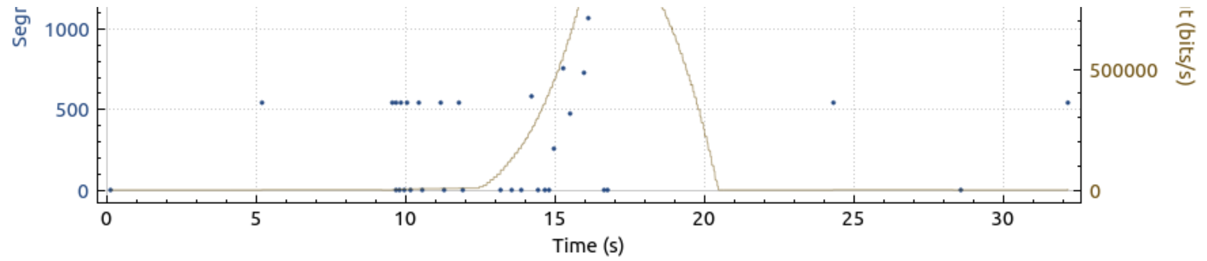


(b) Server Throughput - 50% Drop Rate



(c) Client Control Group - 512kB File

Co-funded by the Horizon 2020 Framework Programme of the European Union



(d) Server Control Group - 0% Drop Rate

Figures a-d show how disturbing traffic on the server side, by dropping up to 50% of the packets, did not result in any appreciable ability to differentiate between clients.

Our conclusions are:

- Tor hidden services provide much greater anonymity than normal Tor use;
- Our users are provided reliable anonymity by our current design and that Tor's countermeasures against side-channels are adequate for our application; however,
- The possible purchase of netflow data by third parties could be used to deanonymize normal Tor use.

We will do more research to determine if other classes of network disturbances could be used to trace Tor connections. We will also use FABRIC to analyze alternative anonymization architectures, especially I2P and Loki to see how their anonymization ability compares to Tor. This further work is the dissertation topic of the PhD student who participated in this work. He is currently designing experiments for testing these hypotheses. During this project, the students successfully defended his qualifier examination. A successful dissertation defence will require a few years of experimentation. Our hope is to publish a series of experimental analyses comparing existing privacy enhancing technologies. This work is ongoing. The analysis done in this project is useful for the censorship circumvention technology community that we belong to.

2. Audit trail verification and evaluation metrics to measure system operations accountability

2.1 Audit trail verification

Establishing the desirable characteristics of our on-chain audit trails could have been done either empirically or analytically. Empirical establishment of security problems tends to be unsatisfying, since software security is in large part established through either pains-taking reviews of software source code, or tedious penetration testing of the binary code. In either instance the result is a point solution that attests, at best, to the inability of the investigator to identify the specific errors that they searched for. Empirical work can never really establish the security of a piece of software, since one can not really prove a negative.

We worked analytically to prove that the design we are using is efficient and has all the security properties desired. This work extends our recent publications on our DLT design:

- Altarawneh, A., Sun, F., Brooks, R. R., Hambolu, O., Yu, L., & Skjellum, A. (2021). “Availability analysis of a permissioned blockchain with a lightweight consensus protocol.” *Computers & Security*, Elsevier, 102, 102098. Which did a queuing theory analysis of our approach and showed that malicious nodes can only slow the entry of data into the DLT.
- Oakley, J., Altarawneh, A., Obeid, J., Sun, F., Brooks, R. R., Yu, L., & Skjellum, A. (2021) "Scrybe: A Secure Audit Trail for Clinical Trial Data Fusion," *Digital Threats: Research and Practice*, ACM, In press. Provides a full security evaluation for the audit trail system for use in clinical trails for pharmaceuticals at the Medical University of South Carolina.

Our extensions to this work created formal proofs of security properties for our consensus protocol that has less impact on the environment. In January, we submitted a paper for review to the ACM’s new DLT journal. The paper is currently under peer review.The security properties that we prove are:

- Immutability,
- Data integrity,
- Non-repudiation, and
- Consensus.

The major existing consensus protocols (and their drawbacks) are:

- Proof of work – requires a large number of unnecessary computations,
- Proof of stake – to participate in mining nodes have to contribute a large amount of their monetary assets. One can invest more currency in order to have more influence. It is unclear as to why one would invest funds if one were not interested in abusing access and the approach seems destined to create an oligopoly.
- Proof of elapsed time – use of Intel SGX hardware allows the execution of programs within a trusted environment where a randomized timer is placed. The first node whose timer expires controls block production. The first problem is that this approach was proposed by Intel who produces those chips. This requires investing all trust into one financial player. The second issue is that numerous side-channel attacks (including plundervolt) have been disclosed that allow this class of hardware security to be compromised. Having one compromised node allows compromise of the entire system.

Our light-weight mining (LWM) approach can be summarized (leaving out details) as:

- Gather hash values for other nodes (2 iterations of steps 4 and 5):
    1. Each participating node *i* out of *n* nodes generates a random number *(R_i)* and calculates a hash value *$H(R_i)$*.
    2. Each node *i* broadcasts *$H(R_{i.})$*
    3. Each node waits for *n/3* *H(R)* values.
    4. Each node creates a vector of the *n/3* values form step 3 and broadcasts the vector.

Co-funded by the Horizon 2020
Framework Programme of the European Union

5. Each node waits for *n/2*+1 vectors

- Gather random number values for other nodes (2 iterations of steps 3 and 4)):
  1. Each node *i* broadcasts R_i
  2. Each node waits for *n/3 R* values.
  3. Each node creates a vector of the *n/3* values form step 3 and broadcasts the vector.
  4. Each node waits for *n/2*+1 vectors
- Determine who is the miner.
  1. Add R_i values modulo *n.* Resulting *i* value chooses node n_i to be miner.

In the paper we prove:

- As long as at least 1 node is non-malicious the choice of miner can not be manipulated. No one can influence miner choice;
- As long as fewer than *n/3* nodes are malicious, then (with probability of 1) all nodes have the same vectors of *H(R)* and *R* values, which means that all nodes agree on the miner choice;
- This protocol has complexity O(*N*), which is the most efficient complexity possible; and
- Immutability and non-repudiation are consequences of the hashing and cryptographic signing used, which the consensus does not change.

We therefore established the efficiency and security of our DLT approach. The proofs in that paper are very innovative in that they apply Erdos and Bollabas's random graph results to DLT analysis by considering DLT participants as a random overlay network within the Internet.

2.2 Implement monitoring and evaluation metrics to measure system operations accountability

The experience was also used to conduct an evidence-based monitoring and evaluation of measurable key indicators with regards to system operations accountability. Our quantifiable set of values was sourced from key indicators integrated into user surveys through analysis of data. Our target value for measurable key indicators is 70%, with a minimal target of 30 % for each key indicator.

We conducted a user survey with 17 paralegals in Chad in October, the 14th. The results obtained through this survey are very satisfying.

- **Front-end operations functioning indicator:** 76% of the users consider that P2PR2P works well. Only 15% of the users find the platform unsatisfactory.
- **Efficiency indicator:** 82% of the users find the application easy to use.
- **Indicator of met needs:** 80% of the users consider that P2PR2P meets their needs.
- **Back-end operations functioning indicator**: 82% of the users community successfully synchronized the collected information with the victims to the database.

In conclusion, thanks to evidence-based monitoring, we are able to evaluate front-end and back-end operations accountability. In a representative environment, users adopt the P2PR2P technology.

Co-funded by the Horizon 2020
Framework Programme of the European Union

3. Establish the quality of distributed governance strategies designed to maximize user trust within the system.

Each P2PR2P deployment starts by identifying a local informal network working on a collective action. We first identified the Association des femmes pour le développement et la culture de la paix au Tchad (AFDCPT) as a potential semi-informal network of users. However, due to an unforeseen coup d'état in Chad, the NGOs key person was forced to temporarily flee the country. We then identified the Public Interest Law Center (PILC) as a potential test network. We later included the AFDCPT, as well as another PILC partner organisation, Patriots of Chad, as participants in a final session held on the 14th of October 2021 in order to create a space for collegial polycentric (multi-organisational) governance of the system.

The collective action of the PILC aims to support women victims of gender based violence seeking justice. To achieve this the PILC trains paralegal volunteers who operate in remote areas of Chad so that they reach victims and produce information resources (questionnaires) on victims' circumstances. These resources are used for further action by PILC admins and their partners to initiate penal and/or civil actions, which in turn justifies fundraising for the collective action. Paralegals also contribute to the PILC's collective action by building resilience to violence at a community level by organising outreach events in their geographic zones.

To evaluate user trust within the system we identified the parameters with PILC admins that participate in creating 1) trust by PILC admins in the paralegal user's production, as well as 2) the paralegal user community's trust in P2PR2P.

3.1. Creating trust in paralegal's output.

The questionnaires produced by paralegals reflect a victim's testimony and are only actionnable by PILC admins if the information is complete. PILC has a fairly formal and pyramidal hierarchy where the contribution of paralegals towards the collective action is controlled, evaluated and enhanced by regional supervisors (points focaux, animateurs). This means paralegals don't have full control over their production and only reap part of the social benefits of their contributions to the PILC collective action. Questionnaires are completed and then transferred by the supervisors in a paper version by bus or, since mid 2021, digitally through another open source application (Kobo). The documents (paper version or Kobo questionnaire) are then centralised in the headquarters of the organisation based in N'djamena. The user groups of the Kobo application are at a supervisory level, not paralegals. The assumption being that paralegals need supervision in order to produce actionable information resources which indicates limited trust in the quality of their production which in turn renders their work invisible within the analog and Kobo systems.

P2PR2P aims to measure the contribution made by paralegals and therefore create trust in the quantity and quality of paralegal's production. We used Elinor Ostrom's common pool-resource institutional framework to establish common governance rules of the informational resources produced by their paralegals with the PILC. A central tenant of Ostrom's theory is that actors should create their own institutions in order to foster

Co-funded by the Horizon 2020
Framework Programme of the European Union

"institution robustness". P2PR2P deployment includes interface co-creation with local civil society initiatives and establishing rules according to their context. Payoff for rule compliance is incentivised according to community rules, which can include leveling up (accessing more functionalities). We integrated Ostrom's rules adapted by the PILC into the system and created a bespoke UX to record the production of paralegals (questionnaires). In addition to the questionnaire resource of P2PR2P we expected to deliver the P2PR2P app with the possibility for paralegals to record the work produced by their community outreach sessions. However, the design phase of the UX was marked by covid related delays on our US partner side. Unfortunately we were not able to travel either to Chad nor the US to workshop the outreach feature IRL. Therefore, only the questionnaire feature was tested on zone during an initial training session in N'djamena on the 14th of october 2021. The questions were elaborated by PILC admins, and collectively enhanced during this training session by participants from the AFDCPT and Patriots of Chad organisations as well as paralegals from the PILC. During this session both AFDCPT and Patriots of Chad suggested changes as well as further categories of actions that could enhance the collective action of all organisations.

During the October session we were able to measure the quality of the paralegal's production. 100% of the synchronised questionnaires was deemed exploitable by the PILC admins for further action in defense of women victims of abuse. 18% of users were unable to synchronise during the given time. This was due to connectivity issues (some synchronised at a later time in the day), as well as age factor. According to an interview carried out on the 25th of October with PILC admin staff, less young members of the user group might need additional time to adopt the technology.

This result confirms that P2PR2P, once finalised, will allow for the transfer of control of paralegals' production to them and therefore fluidify the flow of information by eliminating the bottleneck that is the control of the paralegal's production by regional supervisors.

3.2. Creating user's trust in the P2PR2P system

Our current trust model is based on the notion of integrity-by-design where integrity is "trustworthiness of data and resources" at both user and systems level. It informs user actions with integrity certifications for a) user/network compliance and b) data privacy and security. Together with resource level/values, a) and b) inform the network's sustainability equation that defines the sustainability of the commons. Integrity attestations certify the user trust score (UTS) and the pool's sustainability (OS). Users' choice of action[10] affects their personal UTS as well as OS.

- UTS is linked to reputation (competency/quality of information) and reciprocity (number and type of transactions/volume and diversity)
- OS is also linked to the perception of privacy and accountability
- User trust in P2PR2P is linked to the volume of resources as well as trust in other user's and overall security and privacy.

[10] Somasse, Gbetonmasse & Smith, Alexander & Chapman, Zachary. (2018). Characterizing Actions in a Dynamic Common Pool Resource Game. Games. 9. 101.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- The sustainability of the common pool (OS) is therefore an overall measure of trustworthiness of the system. It is a product of a) and b).

During the session in October, 83% of participants surveyed perceived P2PR2P to be secure. Only 9% said they had too little knowledge of the technology to be able to say if it was secure. This tends to show that P2PR2P is trusted by users, even though privacy testing on FABRIC had not yet been completed. During an interview with PILC admin staff it was explained that the co-creation phase of the P2PR2P UX participated in enhancing trust in the technology. This hypothesis is supported by the fact that the 9% were mainly participants from AFDCPT and Patriots of Chad organisations who were less involved in the co-creation process.

Due to delays in development we could not synchronise the UTS and OS scores on the interface but we did display a static OS score that we told the participants reflects the performance of collective action. We asked paralegals during the training session whether this combined score of collective action was helpful to them. 74% thought this was very/helpful. Asked why, they stated that currently they have little real time information on the collective performance of the PILC and this gave them more insight and sense of shared purpose. We also asked participants of the session if they wished to see more performance indicators of collective action in the next version of the application. Only 26% answered no. This tends to reflect that paralegals are interested in information that evaluates group performance of collective action and that they trust that P2PR2P could deliver these indicators.

Conclusion :

- Ostrom's rules governing common-pool informational resources can be applied to the human rights/humanitarian space.
- Collegially designing a bespoke UX that records all tasks associated with collective action enhances the perception by admin and users of the security and privacy of the system which in turn augments the system's perceived trustworthiness.
- Recording the production of the paralegals empowers this user group and contributes to enhancing the overall collective action in the human rights space.

5 Present and Foreseen TRL

Thanks to the NGI Atlantic program, we have now reached TRL 6 (System Adequacy Validated in Simulated Environment). We have managed to validate the security of our system on FABRIC, but also its operation in a representative environment (namely during a testbed workshop with Chadian organizations promoting human rights).

We are now heading to reach TRL 7, and produce a system prototype for demonstration in an operational environment (with the same Chadian organizations).

Co-funded by the Horizon 2020
Framework Programme of the European Union

6 Exploitation, Dissemination and Communication Status

- ❑ **March-April 2021**:
  - ❑ 20’ Interview with Ruben Tognetti (NGI Atlantic Team)
  - ❑ Interview by Pr. Richard Brooks in the US TV media Fox Carolina
  - ❑ Presentation of the project in the Paris Peace Forum Newsletter
- ❑ **June 20-30 /July 1st :** Participation to the Tetra summer bootcamp
- ❑ **October 20:** Richard Brooks presenting our project at the “Next Generation Internet” session at the 2021 Digital Around the World
- ❑ **October 20, 2021**: Releasing of a video promoting the P2PR2P project *with support from the NGI initiative* https://vimeo.com/635138513 Password : danaidesEN
- ❑ **November 2, 2021**: Releasing of our press release in French and English to 500 hundred journalists, containing a presentation of our P2PR2P project funded by the NGI Atlantic and our main results

After the end of the project, our **exploitation plan** is the following:

- Winter 2021 : a paper for review of the ACM’s new DLT journal.
- Winter2021: a paper of review of the International Journal of the Commons

7 Impacts

Impact 1: Enhanced EU – US cooperation in Next Generation Internet, including policy cooperation.
The French NGO Danaides and Clemson University (SC, USA) are collaboratively developing and testing the P2PR2P (Peer-to-Peer Responsibility to Protect) system. Testing will establish the P2PR2P system’s security, privacy, and ability to promote trust among system participants. Testing involves both use of the FABRIC testbed being jointly developed by RENCI computing, University of Illinois Urbana-Champaign, and Clemson University. The security and privacy testing of P2PR2P builds on a separate NSF funded project that Dr.s Brooks and Wang of Clemson have to use FABRIC to test the viability of existing privacy enhancement and

Co-funded by the Horizon 2020 Framework Programme of the European Union

censorship circumvention tools. The P2PR2P and NSF projects have a clear synergy that shows the joint interest of the EU and USA in increasing the security of the Internet and support the use of the Internet as a tool for enhancing civil society and democratic movements within the developing world. Dr. Brooks has worked to support civil society within Western Africa within the US Department of State's Internet Freedom initiative since 2011. This work has included collaboration with French partners from the very beginning. Danaides is part of consortium that will be funded in a two-years project by the European Commission to develop digital tools to ensure digital security of journalist networks preventing conflits in West Africa.

Specific points of EU- US collaboration that are enhanced by this project include:

- ❑ Development of new approaches for testing and evaluating computer network security,
- ❑ Creation and documentation of an experimental framework for quantifying the amount of privacy a system provides. (We note that enhancing user privacy is a cornerstone of censorship circumvention and countering the information control regimes in Iran, China, Myanmar, Russia, and numerous other non-Democratic states is one of the major points of foreign policy agreement between the EU and USA.)
- ❑ P2PR2P's deployment in Sub-saharan Africa helps protect the rights of women across the Sahel conflict region. Both the EU and USA are actively supporting women's rights and have military involvement in stabilizing the Sahel. Use of the Internet in this work is critical.
- ❑ Assuring network security and privacy within Africa will help limit China's ability to dominate Sub-Saharan Africa.
- ❑ In designing future Internet solutions, the developed countries tend to ignore the fact that there are already more Internet users in both Asia and Africa than either North America or Europe. In addition, Internet penetration rates in Africa and Asia are much lower than in the mature markets of Europe and North America. This means that the future of the Internet, including commercial opportunities, will be dominated by a region that is being largely ignored by most Internet researchers.

Thanks to our collaboration, we have submitted another EU project (1,2 millions euros) with Lawyers Without Borders and three African CSOs. The project builds on our current P2PR2P project with the University of Clemson. We will provide the consortium with our system which guarantee privacy, accountability and trust within a user community.

Impact 2: Reinforced collaboration and increased synergies between the Next Generation

This project includes collaboration between the French University Sciences Po Toulouse and the US Clemson University. Clemson is already engaged in implementing and using the NSF funded FABRIC testbed both as a central development hub and as part of their Fabric Across Borders project. The NGI funding allows Sciences Po Toulouse the ability to integrate this capability into its research and teaching agenda. This is particularly interesting, since it establishes a joint research venture that integrates computer engineering and political science. Creating network tools that support civil society by utilizing the Internet's emerging capabilities provides a new

Co-funded by the Horizon 2020
Framework Programme of the European Union

dimension to the collaboration between both ventures, including comparative research on new modes of governing transnational collective action.

We feel that our work as alpha testers of the FABRIC system was in accordance the EU/NGI goals and the extra effort taken was well spent. It helped advance the North Atlantic community's ability to field advanced Internet infrastructure and showed the necessity of EU/North American collaboration.

Impact 3: Developing interoperable solutions and joint demonstrators, contributions to standards.

While this project concentrates on the P2PR2P system, it is an enabling step in Dr. Brooks and Mr. Shao's larger research into enhancing system privacy and trust enhancement. Notably:

- ❏ We are testing multiple privacy enhancement tools on the FABRIC testbed. Since FABRIC supports reprogramming the network core, we can include machine learning and active traffic interference in our tests. This puts university researchers on an equal footing with nation state firewalls used to enforce censorship. It will make it possible to better establish the true abilities and limitations of these systems.

- ❏ We will test the privacy of numerous Tor pluggable transports (PTs). PTs are the current state of the art tools for avoiding censorship in China, Iran, Kazakhstan, Myanmar, and other authoritarian regimes.

- ❏ We use distributed ledger technologies to maintain our trust records. Dr. Brooks is the recording secretary of the IEEE standards society P2418.3 - Blockchain in Agriculture working group and a member of the IEEE standards society P2145 blockchain governance working group.

- ❏ Dr. Brooks is collaborating with Clemson's Dr.s Gao and Yu developing graduate level courses in Blockchain systems and Distributed ledgers and privacy.

- ❏ Danaides and Clemson are working with an economist from the Federal reserve to develop models of distributed trust that can be integrated into our system experiments. These models will be useful in multiple domains.

DLT technologies work occurred at many levels. Dr. Brooks continued his participation in the IEEE P2145 Blockchain Governance and 2418.3 Blockchain for Agriculture committees. This work simultaneously informed his Danaides work and partially fulfilled the EU/NGI goal of helping to nurture emerging standards. In this case, the IEEE Blockchain governance standards committee looks solely at how communities should best be able to maintain DLT systems, where as the Danaides work looks at realizing DLT systems in ways that enhance the internal governance of civil society groups. The Blockchain for Agriculture committee is more directly in that it considers alternative architectures for ledgers that indelibly document the provenance of objects. These insights will be integrated into our audit trail chain. Dr. Brooks is an editor of the ACM Distributed Ledger Technologies journal and a participant in the IEEE TEMS working group countering money laundering and human trafficking.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Impact 4: An EU - US ecosystem of top researchers, hi-tech start-ups / SMEs and Internet-related communities collaborating on the evolution of the Internet

Dr. Brooks collaborates actively with Dr. Wang who is co-PI of the FABRIC testbed project. Clemson has been a key participant in NSF's GENI testbed program. He is currently part of Clemson's VIPR program which is developing technologies to support the development of distributed ground vehicle prototypes for the US Army GVSC. He is also actively collaborating with French and Senegalese NGOs working to use the Internet to support civil society. This positions Danaides in the middle of multiple large multi-disciplinary efforts for developing new Internet capabilities, which concentrates on finding socially responsible, secure, and privacy enhancing applications.

Operational deployments will be the basis of deeper and stronger ties between the political science faculty of Sciences Po Toulouse Laboratory of Social Sciences of Polity with Clemson's Electrical and Computer Engineering department. Dr. Félix Blanc, M.A. Adeline Demoncy, M.A. Stephanie Lamy and M.A. Candice Duprix are currently teaching M.A. classes at Sciences Po Toulouse on civil societies and international organizations with Pr. Benjamin Gourisse, who is in charge of the Sciences Po Toulouse's Laboratoire des Sciences Sociales du Politique (LaSSP) research program on transnational circulation and global governance. Dr.s Blanc and Brooks foresee increased collaborations between these departments as strategic goals that broaden student perspectives on both sides of the Atlantic. They also foresee comparative research programs on new technologies and their influence on international relations and global governance, including funding for Ph. D. combining field research and multi-disciplinary analysis (law, sociology, economics, computer science, cybernetics, applied ethics and political theory). They are currently working on an interdisciplinary postdoctoral project with the Artificial and Natural Intelligence Toulouse Institute.

8 Conclusion and Future Work

During this 9 months project, we have developed strong ties between the political science faculty of Sciences Po Toulouse Laboratory of Social Sciences of Polity with Clemson's Electrical and Computer Engineering department. We have combined the methodology of computer and social sciences to measure security, accountability and trust within our system.

Danaides used the new FABRIC testbed to run a series of experiments. FABRIC was chosen since its design gives a degree of network access/control that was previously impossible. Experimenters can access/modify/control the network at all possible levels.

We also used an experimental testbed in a representative environment in Chad. We organized a workshop with organizations of women's rights defenders in need of secured, accountable and trustworthy tools to collect, store and share sensitive information.

1. Our conclusions are that **our Tor hidden services provide much greater anonymity than normal Tor use.** In future work, we will do more research to determine if other

Co-funded by the Horizon 2020
Framework Programme of the European Union

classes of network disturbances could be used to trace Tor connections. We will also use FABRIC to analyze alternative anonymization architectures, especially I2P and Loki to see how their anonymization ability compares to Tor

2. We also worked analytically to prove that **the DLT design we are using is efficient and has all the security properties desired.** In future work, Danaïdes, in partnership with Clemson University, will develop blockchain extending Linux's Hyperledger Fabric components and including chaincode smart contracts that use privacy preserving zero-knowledge proofs to give caseworkers fine grained control over data visibility.

   The experience was also used to conduct **an evidence-based monitoring and evaluation of measurable key performance indicators** with regards to system accountability. Our quantifiable set of values was sourced from key performance indicators integrated into user surveys through analysis of data. We reached our target value of 70% for measurable KPIs. Further research will include forthcoming functionalities (messaging, InformaCam).

3. Last, we also demonstrated that **recording all tasks associated with collective action according to institution building rules (Ostrom)** enhances the perception by admin and users of the security and privacy of the system which in turn **augments the system's perceived trustworthiness**. More research is required to evaluate if individual performance indicators could be useful in enhancing participation in collective action.

9 References

1. Dingledine, Roger, and Nick Mathewson. "Design of a blocking-resistant anonymity system" (2006).

2.Hoang, Nguyen Phong, et al. "An empirical study of the i2p anonymity network and its censorship resistance." Proceedings of the Internet Measurement Conference, 2018

3.Loesing, Karsten, Steven J. Murdoch, and Roger Dingledine. "A case study on measuring statistical data in the Tor anonymity network." International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2010.

4.Diaz, Claudia, et al. "Towards measuring anonymity." International Workshop on Privacy Enhancing Technologies, Springer, Berlin, Heidelberg, 2002.

5. Wiley, Brandon, "Circumventing Network Filtering with Polymorphic Protocol Shapeshifting," PhD Dissertation, University of Texas at Austin, 2016

Co-funded by the Horizon 2020 Framework Programme of the European Union

6. Baumeister, Todd "Fundamental Design Issues in anonymous peer-to-peer distributed hash table protocols," PhD Dissertation, University of Hawaii, Manoa, 2019.

7. Paul J. Gertler, Sebastian Martinez, Patrick Premand, Laura B. Rawlings, Christel M. J. Vermeersch, "Impact evaluation in practice", 2nd edition, World Bank, IDB, 2016

8. Evaluation de l'AFD, "Comment contribuer au renforcement des droits de l'homme ? Exemples d'ONG soutenues par les pouvoirs publics français (2008-2012)", Expost n°63, 2016.

9. Evaluation de l'AFD, "Impact du forfait obstétrical en Mauritanie Étude statistique à partir des données sociosanitaires de 2001 à 2011", Expost n°66, 2017.

10. Pamies-Sumner, Stéphanie, "Les évaluations d'impact dans le domaine du développement, état des lieux et nouveaux enjeux", A Savoir n°27, AFD, 2014.

11. Abdesselem Beghriche, Azeddine Bilami, « Modélisation et Gestion de la Confiance dans les Réseaux Mobiles Ad hoc », Département d'informatique, Université de Batna–Algérie. 2009

12. Kaisa Granqvist, "Monitoring and evaluation of P2P initiatives", Policy Paper, Centre for Social Innovation, Era Portal, Austria, 2016.

13. Cyril Ray, Gouenou Coatrieux, Benjamin Coste, "Modèle et mesures de confiance pour la sécurité des systèmes d'information", Revue des Sciences et Technologies de l'Information - Série ISI: Ingénierie des Systèmes d'Information, 2017, 22 (1), pp.19 - 41.

14. Maxime Malafosse, Serge Amabile, Amandine Pascal, "Crypto-technologies & blockchain, artefacts distribués au service de la gouvernance des communs", AIM Nantes, 2019.

15. Gibson, Clark & Andersson, Krister & Ostrom, Elinor & Shivakumar, Sujai, The Samaritan's Dilemma: The Political Economy of Development Aid, 2005

16. The Danish Red Cross and Mercy Corps report. The Next Generation Humanitarian Distributed Platform, 2020

17. Aldrich, Daniel P., Kolade, Oluwaseun, McMahon, Kate, et al. Social Capital's Role in Humanitarian Crises. Journal of Refugee Studies, 2020.

18. Mulder, Femke. Governing the humanitarian knowledge commons. Politics and Governance, 2020, vol. 8, no 4, p. 407-420.

19. Rozas Domingo, David, Tenorio Fornés, Antonio, Díaz Molina, Silvia, et al. "When ostrom meets blockchain: exploring the potentials of blockchain for commons governance", SSRN, 2018.

Co-funded by the Horizon 2020
Framework Programme of the European Union

20. Poux, Philémon, De Philippi, Primavera, et Ramos, Simona. “Blockchains for the Governance of Common Goods” In: Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good. 2020. p. 7-12.

21. Cila, Nazli, Ferri, Gabriele, De Waal, Martijn, et al. “The blockchain and the commons: dilemmas in the design of local platforms”, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020. p. 1-14.

22. Somasse, Gbetonmasse B., Alexander Smith, and Zachary Chapman. "Characterizing actions in a dynamic common pool resource game", Games 9.4 (2018): 101.

23. Schweik, Charles M., and Meelis Kitsing. "Applying Elinor Ostrom's rule classification framework to the analysis of open source software commons", Transnational Corporations Review 2.1 (2010): 13-26.

24. Henry, Adam Douglas, and Thomas Dietz, “Information, Networks, and the Complexity of Trust in Commons Governance”, International Journal of the Commons, 2011, vol. 5, no. 2, pp. 188–212.

25. Z. Liu et al, “A Survey on Blockchain: A Game Theoretical Perspective”, IEEE Access, 2019, vol. 7, pp. 47615-47643

26. Janssen, Marco A., “The Role of Information in Governing the Commons: Experimental Results”, Ecology and Society, 2013, vol. 18, no. 4.

27. Somasse, Gbetonmasse B.; Smith, Alexander; Chapman, Zachary, “Characterizing Actions in a Dynamic Common Pool Resource Game”, Games 9, 2018, no. 4: 101.

28. Seyedsayamdost, Elham and Vanderwal, Peter, “From good governance to governance for good: blockchain for social impact”, Journal of International Development, 2020, vol. 32, no 6, p. 943-960.

29. Baharmand, Hossein and Comes, Tina, “Leveraging partnerships with logistics service providers in humanitarian supply chains by blockchain-based smart contracts”, IFAC-PapersOnLine, 2019, vol. 52, no 13, p. 12-17.

30. Altarawneh, A., Sun, F., Brooks, R. R., Hambolu, O., Yu, L., & Skjellum, A. (2021). “Availability analysis of a permissioned blockchain with a lightweight consensus protocol.” *Computers & Security*, Elsevier, 102, 102098. Which did a queuing theory analysis of our approach and showed that malicious nodes can only slow the entry of data into the DLT.

31. Oakley, J., Altarawneh, A., Obeid, J., Sun, F., Brooks, R. R., Yu, L., & Skjellum, A. (2021) "Scrybe: A Secure Audit Trail for Clinical Trial Data Fusion," *Digital Threats: Research and Practice*, ACM, In press. Provides a full security evaluation fo the audit trail system for use in clinical trails for pharmaceuticals at the Medical University of South Carolina.

Co-funded by the Horizon 2020
Framework Programme of the European Union

32. X. Zhong, I. Jayawardene, G. K. Venayagamoorthy, and R. R. Brooks, "Denial of Service Attack on Tie-Line Bias Control in a Power System with PV Plant" IEEE Transactions on Emerging Topics in Computational Intelligence, 1(5), 375-390 (2018).

10 Glossary

Counterfactual	What the outcome would have been for program participants if they had not participated in the program. By definition, the counterfactual cannot be observed. Therefore, it must be estimated using a comparison group (or control group).
Evaluation	A periodic, objective assessment of a planned, ongoing, or completed project, program, or policy. Evaluations are used to answer specific questions, often related to design, implementation, or results.
P2P	Peer-to-peer service is a decentralized platform whereby individuals interact directly with each other, without intermediation by a third party.
R2P	Responsibility to protect is a political commitment adopted during the United Nations General Assembly in 2005 that normalises the idea that State sovereignty is linked to a State's responsibility to protect the humans on its territory. It is intended to reconcile what duties the international community has in the face of grave human rights abuses. Its theoretical and practical application is governed by the Secretary-General on the Responsibility to Protect, United Nations Office on Genocide Prevention.
CPR	A common pool resource is a resource that benefits a group of people, but which provides diminished benefits to everyone if each individual pursues his or her own self-interest.
Humanitarian	Concerned with human security during natural or man-made emergencies.
Human Rights	Civil, political, economic, social and cultural rights that apply to all humans equally, whichever geographical location, state, race or culture they belong to.
Collective action	Action taken together by a group of people whose goal is to enhance their condition and achieve a common objective.
DLT	Distributed ledger technology that replicates, shares, and synchronises digital data across peer-to-peer networks and where

Co-funded by the Horizon 2020
Framework Programme of the European Union

	consensus algorithms ensure replication across nodes.
Forensics-grade metadata	Content meta-data admissible in courts.
Commons approach	Governance of shared resources by a community organised from the ground up and shaped to cultural norms
Conflict/complex environments	A place affected by extreme poverty and/or climate change, and/or where State and non-State actors exert various forms of coercion on civilian populations.
Human security	Emerging paradigm in national and international security that gives primacy to human beings and their complex social and economic interactions.
Common rules	Rule classification method that was developed by Ostrom and Crawford (2005) as part of the Institutional Analysis and Development framework (Ostrom 2010).

Co-funded by the Horizon 2020
Framework Programme of the European Union