

REPORT DOCUMENTATION PAGE				Form Approved OMB NO. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 19-09-2022		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 30-Sep-2018 - 29-Sep-2022	
4. TITLE AND SUBTITLE Final Report: New Reputation-Based Mining Paradigm: Incentivizing Blockchain Miners to Avoid Dishonest Mining Strategies				5a. CONTRACT NUMBER W911NF-18-1-0483	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER 106012	
6. AUTHORS				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Florida Atlantic University 777 Glades Road PO Box 3091 Boca Raton, FL 33431 -0991				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211				10. SPONSOR/MONITOR'S ACRONYM(S) ARO	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) 72498-RT-REP.13	
12. DISTRIBUTION AVAILABILITY STATEMENT 2 Approved for public release; distribution is unlimited					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Mehrddad Nojournian
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 618-305-4348

RPPR
as of 27-Feb-2023

Agency Code:

Proposal Number:

Agreement Number:

Organization:

Address: , ,

Country:

DUNS Number:

EIN:

Date Received:

Report Date:

for Period Beginning and Ending

Title:

Begin Performance Period:

End Performance Period:

Report Term: -

Submitted By:

Email:

Phone:

Distribution Statement: -

STEM Degrees:

STEM Participants:

Major Goals:

Accomplishments:

Training Opportunities:

Results Dissemination:

Plans Next Period:

Honors and Awards:

Protocol Activity Status:

Technology Transfer:

I certify that the information in the report is complete and accurate:

Signature:

Signature Date:

Contract Number: W911NF1810483 - **Dates Covered:** Sep, 30 2018 to Sep, 29 2022

All texts, figures, charts, formulas, etc are included in the links below

Mehrdad Nojournian, Florida Atlantic University

Abstract: Verification of transactions in digital currencies is very resource intensive, therefore, miners form mining pools to verify each block of transactions in return for a reward where only the first mining pool that accomplishes the process will be rewarded. This leads to intense competitions among miners, and consequently, dishonest mining strategies, e.g., block withholding attack, selfish mining, to name a few. As such, it is necessary to regulate the mining process to make the miners accountable for dishonest behaviors. We therefore designed a new reputation-based mining paradigm in which the miners not only were incentivized to conduct honest mining but also disincentivized to commit any malicious activities against other mining pools.

Objectives: We therefore aimed at several primary objectives during the course of this project. Our first objective was to conduct research on adversarial activities and dishonest mining strategies that may happen during the mining process. Our next goal was to construct resistant trust models and reputation systems for the proposed mining paradigm. Our subsequent purpose was to implement and simulate the new reputation-based mining paradigm similar to an actual setting. Our final objective was to analyze the new mining scheme through experimental and theoretical analyses and define novel applications for this new model.

Findings: We accomplished four goals that we defined in the project. We created a new model for the validation of transactions on the Bitcoin or similar platforms, named reputation-based mining, by considering adversarial activities and dishonest mining strategies. We also proposed a couple of new trust models for this scheme including rational trust modeling as well as privacy-preserving trust management schemes. We simulated our proposed model and then validated this model by real data. Finally, we defined new applications for this new model in other domains for information sharing.

Journal Papers:

<https://doi.org/10.1016/j.bcr.2022.100065> (Elsevier BCRA)

<https://doi.org/10.3390/cryptography6020023> (MDPI Cryptography)

Refereed Conference Papers:

<https://doi.org/10.1109/ICNP52444.2021.9651979> (ICNP'21)

<https://doi.org/10.1109/BRAINS52497.2021.9569825> (BRAINS'21)

https://doi.org/10.1007/978-3-030-89912-7_13 (FTC'21)

https://doi.org/10.1007/978-3-030-31511-5_8 (STM'19)

https://doi.org/10.1007/978-3-030-01554-1_24 (GameSec'18)

https://doi.org/10.1007/978-3-030-01177-2_81 (SAI'18)

PhD Dissertation and MSc Thesis:

https://faculty.eng.fau.edu/nojournian/Files/StDissertation/Dissertation_Linir.pdf

https://faculty.eng.fau.edu/nojournian/Files/StThesis/MSc_Thesis_Pouya.pdf

Software Codes/Simulation:

<https://faculty.eng.fau.edu/nojournian/PRsimulation.zip>

Note: Dr. Linir Zamir was supported for 34 months, but the max value for the “Person Month” was 15 in the system. This must be corrected manually.