Research Statement

I stopped my academic career on 4/2012 for personal reasons; however I've been studying and trying for the last 5 years to re-qualify myself again and improve my skills, especially in Blockchains.

-I failed twice in 2 rejected papers about Bitcoin stateless clients. Both papers are available in GitHub, and a copy of reviewers' comments is available here (https://m.facebook.com/story.php/?id=100010333725264&story_fbid=1566310467056729) which are most about the significance of the presented contribution; ie, not fetal errors or misconceptions in the research & development cycle. I also followed by some analysis on dust UTXOs and reasons behind them (https://shymaaarafat.wordpress.com/2022/02/12/bitcoin-dust-utxos-are-way-too-much-and-increasing-while-total-utxos-are-decreasing/, https://bitcointalk.org/index.php?topic=5385559.msg59237463#msg59237463)

-I finally managed to achieve an acceptance for a different paper about NFTs in BlockTEA 2022 which is an EAI conference and proceedings is published in Sprenger Verlag (https://youtu.be/mT7qSMvV7FQ, https://link.springer.com/chapter/10.1007/978, manuscript available on GitHub). They ranked the paper with a research index of 17 (it seems the research index is per year because it has turned to 0 again because I haven't published in 2023).

-A while before that I took an 8/8 grade in the article of DeFi MOOC Berkeley online course 2021 (https://github.com/Shymaa-Arafat/lab2/blob/main/DeFi_MOOC_Article.md, submitted in 1/2022). I chose to write it on ***propagation delay*** because it was something new for me to learn although I had an earlier draft from 3/2021on sandwich attacks and Ethereum dark forest papers (https://m.facebook.com/story.php?story_fbid=pfbid0bCdTZB4xyk69LaVNpNsoU4vXu74aE12hCFTao8jfVH7MhF4hqj99dHYmaDAoxxutl&id=100010333725264). However, I didn't pursue more research on propagation delay and kept my original research interest on DeFi attacks; I lately revoked it in a series of medium articles that I finished 2 of them and plan to write more (https://medium.com/@shymaa.arafat), but those were not evaluated by the Berkeley DeFi MOOC staff. My first 2 medium articles (***Verkle Trees for Bitcoin*** Stateless nodes, and ***Fiat Shamir transformation*** and its security problems) are also internationally evaluated through the Berkeley ZKP MOOC 2023 course which I've earned the Trailblazer NFT Tier for them ().

My old research papers (uptill 2008) are available on the CV, some of which came through supervision of Master students (ex.s: http://193.227.0.100/eulc_v5/Libraries/Thesis/BrowseThesisPages.aspx?fn=PublicDrawThesis&BibID=11104058, http://193.227.0.100/eulc_v5/Libraries/Thesis/BrowseThesisPages.aspx?fn=PublicDrawThesis&BibID=9581512)

I also reviewed some papers for WSEAS back then; unfortunately, I don't have a proof for that. I think those twitter threads are real life samples of my thorough reading of papers for you to judge:

https://twitter.com/ArafatShymaa/status/1679380972737900544,
https://twitter.com/ArafatShymaa/status/1687536965871190016,
https://twitter.com/ArafatShymaa/status/1436289917794013327

(I know Of course this does not scale up to peer reviewing, but it gives an idea on how I read papers and how would I be as a reviewer)

I'm very much interested in ***Blockchain*** & ***DeFi*** research in general; I think MEV and different DeFi attacks is an endless research topic, and ***Ethereum L2*** evolved even more new interesting topics, like ***random leader selection*** for example. I'm currently waiting for the reviewers decision on my paper on ***Blockchain Consensus*** in SBC'25 and Cyber Security Journal; I believe I worked really hard on this paper.

In addition, I'm interested in ***CBDC*** research in general (https://medium.com/@shymaa.arafat/cbdcs-part1-1da3a944722c), and CBDC interoperability got me involved in a correlated much research area ***cross-chain bridges*** and ***interoperability*** in general; I've studied just a little about through the last lecture of the ZKP MOOC, then through some evolving steps I finished 2 medium articles about it (https://github.com/DrShymaa2022/articles_papers/blob/main/Understanding_CrossChain_Interoperability_Solutions-_part1.pdf, https://medium.com/@shymaa.arafat/what-happened-to-polynetwork-2021-then-2023-2e991e29655b).

Interoperability challenges are there for ***NFTs & Metaverses*** as well, although I haven't tackled much of this area; I've only finished part1 (available in GitHub & medium) and tried to organize a "Workshop call for papers" about as stated in medium but couldn't get feedback. I'm currently enrolled on an NFT & Metaverse in web3 online MOOC by Nicosia University. I have already took another two (DeFi, Introduction to digital currency) in 2023 as stated in my CV.

I think I can supervise master or PhD thesis about a variety of subtopics on that, or maybe participate in writing a complete set of Sprenger Verlag Book Chapters about *Blockchain Interoperability*. ***Ordering*** and resolving ***semantic*** conflicts between TXs crossing borders (or coming from different shards in L2 roll-ups in Ethereum for example) is also an interesting area that I only read in *Chimera Chains* but seems interesting to pursue later on.

I'm still interested in ***CBDCs***, I think I can get back with what I learned from different threats and exploits to find possible improvements in existing systems; different interdisciplinary areas between computer science/engineering & economy/finance there are very interesting (this one needs economy/finance researchers https://www.sciencedirect.com/science/article/pii/S027553192300096X, and this is a simple example of how possible DeFi threats and different attacks can interfere here https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies/)

Within Blockchains research, and correlated with auction mechanisms, there's also what Nicosia University lectures call "the boring stuff" of ***energy trading*** and/or ***water trading & management using Blockchains.*** The link (https://m.facebook.com/story.php/?id=100010333725264&story_fbid=1951166891904416) contains, alongs with other links inside it, what I've learned from a paper about that was in the same BlockTEA

conference my paper was in and then more material I gathered and comments I wrote about the subject. However, with time ***water management and trading using Blockchains*** interested me more, since I had earlier readings about the Game Theoretic model of the Ethiopian dam conflict (being an Egyptian). I tried to publish a paper that have passed the first level abstract filtration for CWW'24, but it failed along the way when reached the full paper journal publishing level (WWP2). The current version is available on researchgate; however, honestly, I'm not self-motivated to work on it anymore as I definitely am for e-voting papers.

E-voting with or without Blockchains also seems an interesting topic for ongoing research; there are hundreds of papers in 2023 alone, ranging from Zero Knowledge solutions for privacy, vulnerability to vote buying when using trusted hardware like Intel SGX, papers in economics conferences & journals, data science, political impact,...etc.

-Although my short WIP paper got rejected from evoting'24 workshop (accompanying Financial Cryptography'24), further reading made me add some little tweaks to the idea and "maybe" I will try again after wrapping it. I withdrew a planned SoK paper, since I realized what I aim to, or should, include is a complete Book Chapters material. I finished an overview of developing countries experiments, read about USA, Switzerland and France

-Currently I'm working on the Estonian i-voting paper and probably will complete this article into a paper to submit soon after integrating newly published material about modifications done before the European Parliament elections (those were not published in June 2024, only 23/12/2024) and whatever comes up.

Also, last year I tried to tackle the game equilibrium of ***deceased organ donation***; maybe as Egypt started to encourage people to sign an official approval statement about it, I recalled my earlier study of kidney exchange algorithms in ***Algorithmic Game Theory*** and searched for more general material (not just kidney). I gathered a lot of material, I read some including A E Roth work (https://youtu.be/ouVeoLg_h4A); although I stopped after a while, I got back to Blockchain research, I recently posted a "call for Book Chapters" about it (https://www.researchgate.net/post/Call_for_Book_Chapters_on_Deceased_Organ_Donations_as_an_interdisciplinary_science_information_Systems_Game_model_AI) hoping to get some interested researchers to break the ice and also cover all merits of the topic but haven't got any.

I had another earlier aborted research attempt when studied AGT, I tried to check what if the sub-additive property constraint was not applied in some auctions (although buying more pieces help achieving market clearance, people usually pay more to get 2 adjacent land pieces or apartments to merge them in a wider one), and there was an auction selling 2000 land pieces but I couldn't get the data to compare results since I was working alone (not backed by a university when trying to contact the office that made the auction) after years of retirement since 2012. I also tried to ***map some graph reduction rules into auction rules*** but never knew if they were useful (https://economics.stackexchange.com/questions/36049/reduction-rules-for-auction-conflicting-deals).

I also tried to suggest some of those ideas as students graduation projects aiming to make their project part of a post graduate student research, possibly their TA (https://m.facebook.com/story.php/?id=100010333725264&story_fbid=2021520151535756).

In short, I have a wide variety of research ideas; if I only finished step1 (or even the step 0 preface), it's because I'm not working right now and I'm doing everything solely. I believe if I'm working in a university and have a research group, the ideas will be distributed and pursued more according to the interests of participants.

Final note is that I originally came from an Algorithmic background, my PhD finished 7/2001 was about Hu-Tucker and Huffman Trees, and I guess it affects all my research orientation and the way I approach different areas. I still read some Algorithms papers in arXiv and would be interested in doing research in such topics.

Sincerely,

Shymaa M Arafat

On 8th April 2025