CURRICULUM VITAE

Siamak SOLAT

Blockchain Research Engineer

at

ENGIE - Laboratory for Computer Science and Artificial Intelligence

361 Avenue du President Wilson, France

==========

EDUCATION:

1. Diplôme de Recherche (Research Degree) in Computer Science (2018)
   - Research Topic: "A Timestamp-Free Prevention of Selfish Mining in Bitcoin And A New Decentralized Consensus For Blockchain"
   - Sorbonne University (Pierre and Marie Curie Campus)

   ---
2. Master in Computer Science - Computer Networks
   - Sorbonne University (Pierre and Marie Curie Campus)
   - A joint Master with École Nationale Supérieure des Télécommunications - TÉLÉCOM Paris-Tech
   - Master Graduation Internship: "Distributed Algorithms for Autonomous, Anonymous and Forgetful MobileRobotsNetworks" (6 months) under the supervision of Pr.Claude Chaudet (chaudet@webster.ch)

   ---
3. Bachelor's degree in Computer Engineering – Software Engineering (4 years)
   - Azad University, Tehran, Iran

==========

PUBLICATIONS:

Peer-Reviewed Conference Proceedings:

1. **Title:** "ZeroBlock: Timestamp-Free Prevention of Selfish Mining or Block-Withholding Attack in Bitcoin"

   - **Published in:** "SSS 2017: 19th Annual International Symposium on Stabilization, Safety, and Security of Distributed Systems"

   - **Abstract:** We introduced a new timestamp-free solution to prevent block-withholding or selfish mining in Bitcoin network. This attack relies on block concealing and revealing only at an opportunistic time selected by selfish miners such that selfish miners can earn revenues superior to a fair situation. The key idea of our solution, ZeroBlock, is that each block must be generated and received by the network within a maximum acceptable time for receiving a new block interval (called *mat*) that is possible to calculate locally by each miner. Within this time interval, an honest miner must receive or discover a new block. Otherwise, it generates a dummy Zeroblock that does not need any proof-of-work computation. The computation of each *mat*time interval is done locally by each miner based on the following Bitcoin parameters: the expected

delay for a block mining (calculated based on the Poisson nature of proof-of-work) and the information propagation time in Bitcoin network. We proved that ZeroBlock algorithm is resilient to block-withholding or selfish mining attack without using forgeable timestamps. That is, we demonstrated that if selfish miners intend to keep their blocks private more than the duration of a *mat*time interval, then the selfish block will be rejected by honest miners. Moreover, we proved that selfish miners are not incentivized to ignore Zeroblock or to generate too many of them. Furthermore, we demonstrated that our solution is compliant to nodes churn. Proof-of-work is a Poisson process and causes blocks to be discovered randomly and independently. ZeroBlock uses Poisson property of proof-of-work and thus does not cause any additional latency for block generation in the network. Generation of Zeroblock does not need to solve proof-of-work. Although, one of the reasons for using PoW is preventing DoS attack (Denial of Service) but since Zeroblock is not broadcast and generated locally, so ZeroBlock algorithm is not vulnerable against DoS attacks.

---

2. **Title:**"RDV: An Alternative To Proof-of-Work And A Real Decentralized Consensus For Blockchain"

   - **Published in:** "ACM Workshop on Blockchain-enabled Networked Sensor Systems (BlockSys 2018) as a part of the 16th ACM Conference on Embedded Networked Sensor Systems (SenSys 2018)"

   - **Abstract:** A blockchain is a decentralized ledger where all transactions are recorded. To achieve immutability of transactions history, we need a real decentralized consensus and permission-less blockchain since in a permissioned blockchain, although we can accelerate transactions validation throughput; however contrary to permission-less blockchains that are open to everybody for participating in transactions validation process, in a permissioned blockchain the fate of transactions is determined by a limited number of permissioned validators and this fact can impair decentralization of the system. Bitcoin as a permission-less blockchain uses proof-of-work. PoW powered blockchains currently account for more than 90% of the total market capitalization of existing digital currencies. PoW is a cryptographic puzzle that is difficult to solve but easy to verify. Significant latency of proof-of-work for transactions confirmation has negative effects on blockchain security such that longer delays may increase the number of forks and the possibilities for mounting double-spending attacks. On the other hand, PoW consumes a significant amount of energy that by growing the network, it becomes a major problematic of this consensus mechanism. We introduce an alternative to PoW because of all its major problems and security issues that may lead to collapsing decentralization of the blockchain, whereas a full decentralized system is one of the main purposes of designing blockchain technology. The approach we introduce is based on a distributed voting process and called "RDV: Register, Deposit, Vote" in which all participants by proceeding a registration procedure can participate in voting process in a permission-less blockchain. Since in RDV algorithm, there is no mining process, so it may be more appropriate for low-level energy devices and Internet of Things (IoT). This paper was the first phase of our consensus. In the next phase, as further works, we extend this algorithm by designing a mixed lottery-based and voting-based consensus and combining both interior cost (such as coins) and exterior cost (such as memory) to achieve more enhanced security level.

==========

Works in Progress:

1. **Title:**"Anonymity in Blockchain Systems: A Review"

   - **Abstract:** Anonymity is one of the features has affected the success of Bitcoin deployment. Since on a blockchain, the identity of a user is concealed behind a cryptographic public key, so linking public addresses to individual users is particularly difficult to achieve. This raises questions about how blockchain can be regarded as truly transparent. The transparency of a blockchain originates in the fact that transactions of each public address are open to viewing. Using an explorer it is feasible to see the transactions that users have carried out. This level of transparency has not existed within financial systems before Bitcoin. In the past, large financial institutions were able to use their customers funds as they saw fit, without anyone's knowledge, and not always in the most effective or honest matter. However, this level of transparency can be problematic since everybody can see every historic transaction in the clear in an explorer site. On the other hand, recent efforts in cryptography and decentralized blockchains enable people to protect better their data and identity from entities that we interact with. In this paper, we evaluate the most important techniques for enhancing anonymity of the blockchain-based transactions. We also evaluate de-anonymization approaches as countermeasures for revealing the transactors and the owners of the addresses.

---

2. **Title:**"Towards More Decentralized Payment Routing in Lightning Network"

   - **Abstract:** The Lightning Network is a decentralized system for instant micropayments, aiming to generate an overlay network on the Bitcoin protocol allowing arbitrary parties to route payments to each other without writing to the blockchain.Bitcoin includes an advanced scripting system allowing users to program instructions for funds. There are, however, some drawbacks, such that transactions confirmations take up to around one hour, before they are irreversible, as payments are widely regarded as secure on Bitcoin after confirmation of 6 blocks that takesaround one hour. The fees also make micropaymentsnot affordable. Lightning Network is one of the first implementations of a multi-party contract using Bitcoin's built-in scripting.Since establishing a channel needs for locking up on-chain funds and users have a finite resource, so it is not feasible to expect a channel between any two participants who want to transact to each other via the Lightning Network.The routing process is therefore required to decrease the amount of on-chain transactions and also to have higher liquidity per channel available.The LN white paper only in one paragraph is addressing the payment routing in LN network and does not explain any step-by-step payment routing process since the routingin LN is a client side decision making and the intermediary hopes just forward the packets as requested.The current structure of payments on the Lightning Network is a hub-and-spoke model. Although, the hub-and-spoke model basically needs for fewer routes; however, it can threaten decentralization of the system by relying heavily on the hubs as powerful intermediaries. This could also potentially threaten privacy and give rise to possible censorship. The target is therefore to design a more decentralized mechanism for the payment routing in the Lightning Network.

---

3. **Title:**"Common Imprecise Beliefs And Misunderstandings About Blockchain"

   - **Abstract:** The term of blockchain was introduced for the first time in the original paper of Bitcoin. The blockchain as a new innovation brings us many opportunities as a crucial element of the Bitcoin by getting us rid of a central authority, leading to improve the security of the

system by removing a single point of failure; however,it possesses several significant drawbacks such as latency in the performance, scalability etc, which we need to consider them at the time of using blockchain in a platform.If we actually search about the advantages of the blockchain in the Internet, we can see that usually all the features of the Bitcoin is attributed to the blockchain, whereas, the blockchain is just a part of the Bitcoin protocol and other elements such as consensus, cryptography etc all together bring us the advantages of the Bitcoin. Unfortunately, a belief has been spread that if the blockchain, as a data structure, is added to a platform, the system then possesses all the features of the Bitcoin such as immutability of the stored data in the blockchain. In this paper, wementionthe most common misconceptions and imprecise beliefs about the blockchain in many research papers.

==========

INVITATION as KEYNOTE SPEAKER on Blockchain:

- Invited as Keynote Speaker on Blockchain Technology at International Conference on Intelligent and Innovative Computing Applications
- All travel and accommodation costs covered by the conference organizers

==========

SKILLS:

1. BlockchainConception, Distributed Ledger Technology (DLT)
2. Blockchain Platforms : Bitcoin , Ethereum, Hyperledger, ZCash, EOSIO, etc
3. Blockchain Consensuses: PoW, PoS, DPoS, PBFT, Tendermint, Ripple, PoET, Raft, PoA, etc
4. Byzantine Fault Tolerance
5. Blockchain Programming, Smart Contracts, Solidity, Remix, Web3.js, EthereumJS
6. Ethereum Test-nets: Ropsten, Kovan, Rinkeby
7. Meta Mask, TestRPC
8. Payment Channels and State Channels in Blockchain
9. DAG-based DLTs (Directed Acyclic Graph): SPECTRE, Graphchain, IOTA
10. Blockchain platforms for more anonymization: Enigma, Hawk, zkLedger, etc
11. Zero-Knowledge Proofs : zk-SNARKs, zk-STARKs, Bulletproofs
12. Cryptographic Algorithms: Elliptic Curve Cryptography, ECDSA, ECAES, RSA, DES
13. Public Key Infrastructure (PKI)
14. Game Theory
15. Programming Languages : C / C++, Solidity, Java, .Net Framework, JavaScript
16. Distributed Algorithms
17. Distributed Networks

==========

PROFESSIONAL EXPERIENCE:

1. ENGIE, Laboratory for Computer Science and Artificial Intelligence (France)

   - (05/03/2018 – Currently)
   - Blockchain Research Engineer
   - (Blockchain Consultant - CDI)
   - Duties:
     - Research and development on the blockchain and distributed ledger technology,

- Investigating current challenges on the blockchain and discovering and proposing solutions,
- Analyzing, implementing, and testing current blockchain solutions and platforms,
- Developing Ethereum-based smart contracts in Solidity and DApps,
- Proof-of-concepts (PoC) for using blockchain in energy sector,

---

2. FIME (France)

- (01/05/2015 – 21/09/2015) (4 months)
- Mastercard CPV Engineer

---

3. École Nationale Supérieure des Télécommunications - TÉLÉCOM Paris-Tech

- (01/04/2013 – 30/09/2013) (6 months)
- Master Graduation Internship: "Distributed Algorithms for Autonomous, Anonymous and Forgetful MobileRobots Networks", under the supervision of Pr.Claude Chaudet (chaudet@webster.ch)

---

4. SAMAN Bank - Electronic Payment Service (provider of electronic payment solutions) (Tehran, Iran)

- (01/05/2010 – 01/11/2011) (1.5 years)
- Expert in software production in the field of security in C#, Java, C++ for the payment solutions

---

5. Infotech-International (provider of electronic payment solutions and partner of Gemalto and Ingenico) (Tehran, Iran)

- (01/11/2008 – 01/05/2010) (1.5 years)
- Expert in software production in the field of security in C#, Java, C++ for the payment solutions

---

6. Eniac-Tech (provider of electronic payment solutions) (Tehran, Iran)

- (01/11/2007 – 01/11/2008) (1 year)
- Expert in software production in the field of security in C#, Java, C++ for the payment solutions

---