Ministry of Science and ICT

IITP Institute of Information & Communications Technology Planning & Evaluation

APPLICATION FORM
(JOINT RESEARCH)
HIGH POTENTIAL INDIVIDUALS GLOBAL TRAINING PROGRAM)

AGREEMENT

As stated above, I submit this application form to IITP that conducts "High Potential Individuals Global Training Program" supported by Ministry of Science, ICT in South Korea. IITP may disclose the information below to the public for the purpose of providing information and matching a research partnership between your institute and a Korean university.

* IITP : Institute for Information & communications Technology Planning & Evaluation

Printed Name of Chief of Research	Vojislav B. MIŠIĆ	Date(mm-dd-yyyy)	01-27-2020
Signature of Chief of Research			

☞ ***(Note)*** *This application is to identify the willingness to participate in this research and to find a research partnership for research institutes in Korea. Therefore, in its sole discretion, it is acceptable to contain only minimal information. (max. 3 pages)*

1. Research Title	*Efficient data propagation and ledger updates in the Bitcoin network*						
2. Research Area	**A.I.**	**Big Data**	**Cloud Computing**	**Block Chain**	**AR/ VR**	**ICT/SW Convergence**	**Other ICT /SW**
				X			
3. Chief of research	Title	*Professor*		Contact	E-mail : jmisic@ryerson.ca		
	Name	*Jelena MIŠIĆ*			Tel: +1-416-979-5000 ext. 7404		
4. Affiliation	Name	*Ryerson University Toronto, Canada*		Classification	(X) University ( ) Research Institute ( ) Industry ( ) ETC.		
5. Capacity for students (5 or less)	*3*		**Support for students** ***(all necessary)***		(X) Visa support (X) Research Mentoring (X) Research Space (X) Accessibility to Research equipment		

6. Research Objective	The objectives of the proposed research are: • to propose new and/or augment existing data propagation protocols for the blockchain network in order to optimize its operation and reduce the impact of finite and random message propagation times on system performance; • to develop effective metrics for the performance of permissionless blockchain-based systems that will guide the design of the underlying communication network; and • to devise protocols for secure information exchange and ensure privacy protection for user data as well as for the distributed ledger using blockchain technology.
7. Research Summary	The proposed research aims to improve of network performance to minimize the potential for ledger inconsistency and as a by-product minimize the attack surface created by this inconsistency. This will reduce forking which is due to finite propagation time of blocks in the Bitcoin [1] network and the inability to determine whether the current main tip of the blockchain should be replaced by the newly arrived block that builds upon the same previous block as the current main tip. Both topics are applicable to other public blockchain platforms (e.g., Ethereum [2]), provided they use some form of distributed consensus. We also plan to investigate consensus protocols with the goal of adapting them to the requirements of the application in question. Reducing data propagation times may be accomplished by improved network infrastructure and by proper design of the protocols; for obvious reasons we will focus on the latter approach. To this end, we will begin by defining novel metrics for characterization of network performance, and we will extend the compact block relaying approach [3] to transactions and eliminate some of the messages in the regular INV-GETDATA-TX procedure. A promising solution is to develop additional messages to package several transactions instead of just one. This will lead to the following benefits: first, we decrease latency as the data exchange takes 0.5RTT instead of 1.5RTT as in the original approach. Second, we will decrease the volume of transaction traffic and improve bandwidth utilization. Finally, we can improve security by judicious choice of peers to which the new messages are directed, as this will make harder for eavesdroppers to launch deanonymization attacks that infer the node IP addresses from transaction messages [4]. We will use approaches based on set reconciliation [5][6] as benchmarks to compare the performance of proposed techniques. Improved decision making at forking events would be simple if only we could know the exact time a block has been mined but this is impossible because of possible clock skews between different nodes. Instead, we will use measurements of Round-Trip Times (RTTs) to infer the transmission delays between different nodes. Note that such measurements can be made at the transport protocol level and, thus, require no modification to the Bitcoin messaging protocols.

	We will then use machine learning techniques or, alternatively, non-parametric estimation techniques such as kernel-based estimation [7][8], to estimate the block mining times that will help us make the necessary decisions. As the decisions are made locally by each node, the potential for security vulnerabilities or collusion between nodes is minimal. Furthermore, we will develop new metrics for ledger inconsistency, taking into account both the time until fork resolution and the size of network partition (measured as the number of nodes) that has adopted the incorrect chain tip, and investigate the ways in which these metrics could be minimized. **References** [1] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. [2] V. Buterin. Ethereum: A next-generation smart contract and decentralized application platform, 2017. Available online at http://ethereum.org/ethereum.html. [3] M. Corallo. BIP 152: compact block relay. https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki, 2016. [4] G. Fanti *et al*. Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees. *ACM SIGMETRICS '18*, 2018. [5] A. P. Ozisik *et al*. Graphene: A new protocol for block propagation using set reconciliation. *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pp. 420-428, Oslo, Norway, 2017. [6] G. Naumenko *et al*. Bandwidth-efficient transaction relay for bitcoin. CoRR, abs/1905.10518, 2019. [7] M. Wand and M. Jones. *Kernel smoothing.* Chapman & Hall, Inc., 1995. [8] Racine JS. Nonparametric econometrics: a primer. *Foundations and Trends in Econometrics* **3**(1): 1–88, 2008
8. Need for funding from Korean government	*Funds are needed to support internship of Korean students at Ryerson University in Toronto, ON, Canada for the duration of 9 to 12 months.*
9. Request for Korean Universities	*The selection of students studying abroad should be conducted after mutual consultation, and please cooperate as much as possible to prepare for necessary travel documents.*