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: Taeho Jung   Date(mm-dd-yyyy): 01-30-2019

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	Transformative Consensus Mechanisms for Blockchain Systems						
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	Assistant Professor	Contact	E-mail : tjung@nd.edu			
	Name	Taeho Jung		Tel : +1-574-631-8322			
4. Affiliation	Name	University of Notre Dame	Classification	(X) University ( ) Research Institute ( ) Industry ( ) ETC.			
5. Capacity for students (5 or less)	2	**Support for students *(all necessary)***	(X) Visa support (X) Research Mentoring (X) Research Space (X) Accessibility to Research equipment				

6. Research Objective	Substantially improve the efficiency permissionless blockchains and security of permissioned blockchains via transformative consensus mechanisms.
7. Research Summary	For permissionless blockchains, Proof-of-Useful-Work (PoUW) mechanisms will be investigated, where fully decentralized PoUW mechanisms (i.e., without central entities evaluating the usefulness of the work) will be designed. For permissioned blockchains, Trusted Execution Environment (TEE) and cryptographic Secure Computation primitives will be leveraged to develop consensus mechanisms that only need one honest node and constant number of message exchanges. For more details, please see the attached 1-page description (next page).
8. Need for funding from Korean government	The PI will devote 20% of his time in this project, and funds are requested to support two months of his summer salary. Also, an existing Ph.D. student of the PI's research group will assist the project with his expertise in Trusted Executed Environment and Secure Multiparty Computation. Funds are requested to support his research activity.
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 VISA.

Transformative Consensus Mechanisms for Blockchain Systems

Taeho Jung, Ph.D., Assistant Professor
Department of Computer Science and Engineering, University of Notre Dame, USA

Background and Motivation

Blockchains can be categorized into many types, and this project focuses on the two: permissionless and permissioned blockchains. A permissionless blockchain relies on any participating nodes who are not authenticated or vetted to reach consensus among the nodes. Because the nodes are not vetted, the consensus is derived by relying on decentralized mechanisms (e.g., Proof-of-Work or PoW, Proof-of-Stake or PoS). A permissioned blockchain reaches consensus relies on the nodes who are authenticated and authorized. Because the nodes are known authorized entities, the consensus can be derived by existing Byzantine Fault-Tolerant (BFT) protocols which are usually much more efficient and provably secure, but requires that certain percentage of the nodes must be honest. Both types of blockchain have different advantages and different application scenarios. A permissionless blockchain does not rely on trust assumptions because (in theory) the security holds as long as there is one honest node, and it is suitable for applications that require complete decentralization (e.g., cryptocurrency). A permissioned blockchain has certain degree of control over the distributed ledger (in that only the authorized nodes can write into the ledger), and it has certain degree of decentralization as well because nodes behave on their own without needing to trust others. It is suitable for applications that require collaboration among nontrustful organizations (e.g., international bank networks, medical data sharing among hospitals, auditing of multi-organization transactions, cross-platform communication).

Research Goal and Rationale

Existing permissionless blockchains have various resource efficiency issues (e.g., Bitcoin network emits more CO_2 gas a year than 1 million transatlantic flights, and it consumes more electricity than Switzerland) or lack of provable security (e.g., attackers have no penalties in PoS-based blockchain, and there are "nothing-at-stake" or "fake-stake" problems). On the other hand, a permissioned blockchain does not guarantee the security that is on a par with that of permissionless blockchains because certain percentage of the nodes need to be trusted in order to guarantee consensus among all nodes. **The research goal of this project is to develop the following two transformative consensus mechanisms** that have potentials to substantially change the way people operate with blockchain systems and thus achieve substantially improved efficiency and/or security.

- For permissionless blockchains: Fully decentralized consensus mechanisms who do not have existing issues in PoW or PoS mechanisms but have the security guarantees that are identical or comparable to those of PoW mechanisms.
- For permissioned blockchains: Decentralized consensus mechanisms (among the authorized nodes) which guarantee consensus with only one honest node (on contrary to certain percentage of the total nodes) and/or with constant number of message exchanges (on contrary to $\Omega(n)$ message exchanges with n users).

Expected Research Activity and Contributions/Impacts

Continued from the past achievements, the PI will investigate the Proof-of-Useful-Work (PoUW) mechanisms for permissionless blockchains. Miner nodes in such mechanisms perform useful work instead of meaningless hash calculation, however all existing mechanisms involve centralized entities who distribute and evaluate the usefulness of the miners' work outcome. The PI will explore and introduce decentralized protocols for such entities, which will lead to **permissionless blockchains with strong consensus robustness but without efficiency issues**.

For the permissioned blockchains, the PI will explore and leverage Trusted Execution Environment (TEE) and secure computation primitives (e.g., Secure Multiparty Computation and Homomorphic Encryption) to allow authorized nodes to reach consensus by exchanging only constant number of messages. This will be done based on the PI's past achievements in these domains, which will lead to **permissioned blockchains whose consensus is ensured with only one node behaving honestly**.

Both studies will impact the blockchain industry as well as the academic community. The studies will lead to theories and discoveries (e.g., protocols, algorithms, analysis) that can be utilized to develop permissionless or permissioned blockchain systems with substantially improved efficiency and/or security. The theories and discoveries will advance the studies in the blockchain community.

Anticipated Student Qualification

Students are expected to have knowledge of the C programming language, and they are expected to be able to write technical articles in English. The PI, Dr. Jung, will provide mentoring and training to let students gain skills necessary to ensure scientific rigor, ethical conduct of research, and oral and written communication for presentation.