# Federated Contract Market for Decentralized Applications

Shashi Raj Pandey, Sabah Suhail, Yan Kyaw Tun, Madyan Alsenwi, Choong Seon Hong*
Department of Computer Engineering,
Kyung Hee University,
Yongin, 17104 Korea
Email: {shashiraj, sabah, ykyawtun7, malsenwi, cshong}@khu.ac.kr

**Abstract**

As an emerging platform for decentralized applications, blockchain has gained popularity in recent years. With its ability to quickly establish a self-organized data management platform for various decentralized applications, permissionless blockchain creates a framework to support seamless data trading for various mobile crowdsensing tasks by using executable smart contracts. In this regards, the task of solving resource extensive cryptographic puzzle for a new block of transactions in the blockchain network, known as "mining", can be offloaded to the edge infrastructure by the contract providers, referred as virtual miners. In this work, we design a flexible infrastructure for the resource constraint users to trade data autonomously, in an affordable and secure manner by exploiting economic interaction between virtual miners and the blockchain network. The users can interact with the smart contract provider, who can independently design smart contracts and build decentralized applications, namely DApps, by themselves without the trusted intermediaries. We facilitate the user requirements with the smart contract providers, and formulate a utility maximization problem to adapt the computational resource sharing policy between the competing smart contract providers in the blockchain network to construct DApp infrastructure. Simulation results characterize the optimal trading point that maximizes the overall network utility.

***Keywords –*** *blockchain, smart contract, resource trading, utility maximization*

## I. Introduction

Blockchain network is an overlay peer-to-peer network (P2P) that provides a distributed and decentralized network architecture, and was introduced by Nakamoto as a bitcoin's public ledger in 2009 [1]. The basic component in the blockchain network is called a *block*. The transactions in the P2P network are hash-linked to form *blocks*, which are sequentially chained in a chronological order together, and confirmed amongst all the nodes (*miners*) in the network to form the blockchain. The underlying Nakamoto consensus protocol governs the computational extensive *Proof-of-Work (PoW)* process [1], namely *mining*. Using PoW the network characterizes the wining member node who is legitimate to embed the newly formed block of transactions in the existing chain of blocks. Note that, the newly added block is broadcast in the network, and further undergoes validation and comparison for approval to the block chain. Once the process is successful, the miner will receive a mining reward (an possibly a bonus depending upon the transactions).

Recent years have observed growth in the integration of permissionless blockchain technology for various decentralized autonomous applications such as access control, electricity trading and data sharing [2], [3]. With its ability to quickly establish a self-organized data management platform for various decentralized applications (DApps), permissionless blockchain creates a framework to support seamless data trading for various mobile crowdsensing tasks by using executable smart contracts [4]– [6]. In this regards, the challenge is to facilitate resource constrained nodes such as mobile devices (*possible DApp users*) to use decentralized autonomous services without burdening them by the requirement for building resource extensive blockchain infrastructure [7].

To address this issue, we at first introduce the smart contract providers (SCSs) who independently design smart contracts and build decentralized applications. Together, SCSs create a contract pool, namely smart contract (SC) market with variety of smart contracts to sell to the resource constrained users for adopting DApps services. The users can use DApp platform to interact with the SC market. In the proposed framework, the SCSs will compete with each other to buy corresponding computing resourcing in the mining network to build the infrastructure for DApp devices with the set of smart contracts. Here, it is intuitive that having more number of participating SCSs interested in purchasing the computational resources will make the DApps platform more secure, however the criticality of resource selling for the competing SCSs in the blockchain network still exists i.e., the paradox of more buyers with less resource selling point, and less buyers with higher resource selling point in network. Thus, we model the network carefully to adjust the normalize resource selling point to the candidate virtual miners in the SC market in order to maximize its total utility. Here, the network utility is defined in terms of trustworthy measure increase for DApps.

The paper is organized as follows. Section II discusses the system model and Section III explains about the problem formulation and proposed solution approach. Section IV shows

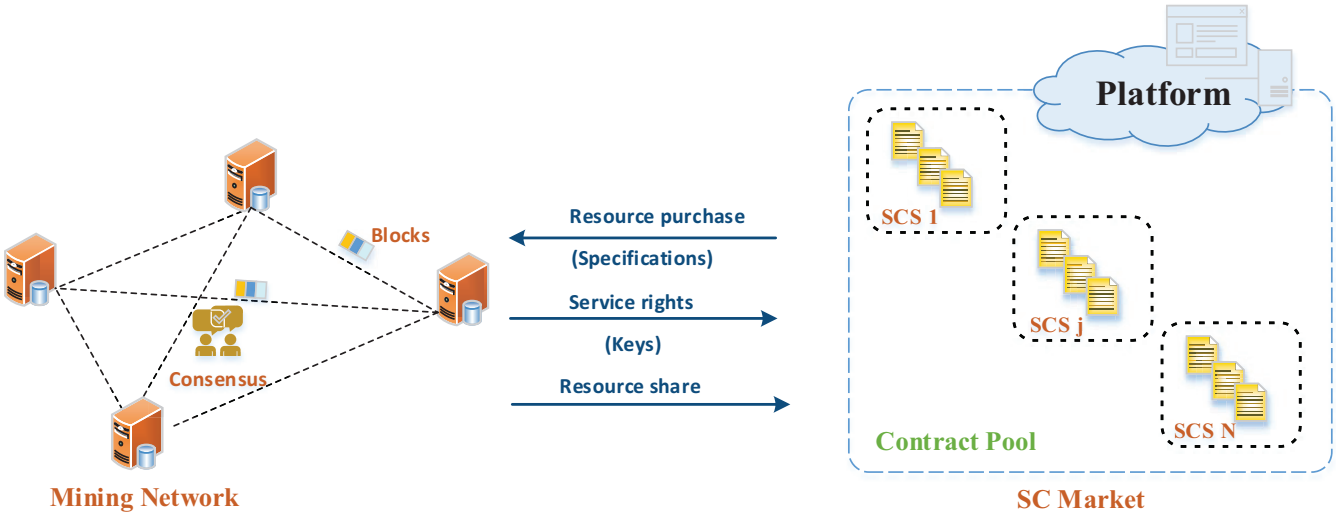


Fig. 1. System Model

simulation results. Finally, Section V concludes the paper with future work.

## II. System Model

We define a pool of smart contract provider, namely SCS as a set $\mathcal{N} = \{1, 2, \ldots, j, \ldots, N\}$ together forming a Smart Contract (SC) market as in Fig. 1. Basically, SCS sell smart contracts as per the DApp users requirements, and correspondingly compete to mine the block of transactions related with the applications to evoke smart contract privileges and earn mining bonus from the blockchain network. This way, on the one hand, the proposed framework facilitates the resource constrained DApp users to use the permissionless blockchain infrastructure for various applications, and on the other, it abandons the need of resource extensive mining process to build infrastructure for DApps. Consequently, the competing virtual miners or SCS will trade the resources of mining network for different smart contract configuration. The mining network will estimate the resource requirement for interacting SCSs, and set the optimal resource selling point to the SCSs for maximizing its utility. In the following section, we will formulate our problem for this framework.

## III. Problem Formulation

We consider that per SCS normalized resource request $\mathbf{x}$ is an i.i.d and uniformly distributed random variable over the range $[x_{min}, x_{max}]$. Then, we can define the PDF of the possible requests as $f_{\mathbf{x}}(x) = \frac{1}{x_{max} - x_{min}}$. Let us consider a sequence of discrete time slots $t \in \{1, 2, \ldots\}$, where the DApp developer adjust the difficulty level of the mining network.

At time slot $t$, the number of SCSs competing in the mining network is $|\mathcal{N}(t)|$, or simply $N$. To effectively plan the normalized resource selling point for per SCS, the network will restrict SCSs with $\mathbf{x}(t) \geq x_{max}$. Therefore, the total number of selected SCSs $N(t)$ by the mining network for selling the computing resource is $N(t) = N \cdot F_{\mathbf{x}(t)}(x) = N \cdot P[\mathbf{x}(t) \leq x]$. We have $N(t) = N \cdot \left[\frac{x(t) - x_{min}}{x_{max} - x_{min}}\right]$. During each time of adjusting the mining difficulty, the network sets a per SCS resource selling point $\mathbf{x}(t)$, which is a fair value in the competitive and bias market, that maximizes the sum of the network's utility $\mathcal{U}(\cdot) + (1 - x) \cdot N(t)$ over the constraint of per SCS resource purchase.

The function $\mathcal{U}(\cdot)$ is non-decreasing and concave to $x$ that characterizes the trustworthy measure increase for DApps services. In this work, we define the function $\mathcal{U}(.)$ as

$$\mathcal{U}(\cdot) \equiv \gamma \left(1 - 10^{-(a(1-x)+b)}\right), \tag{1}$$

where $0 < \gamma \leq 1$ is a coefficient, and $a \geq 0, b \leq 0$ are defined parameters that characterizes the mining network's response upon resource trading. Therefore, for the set of competing SCS, the mining network maximizes its utility as follows:

$$\begin{aligned} \max_{x(t)} \quad & \gamma \left(1 - 10^{-(a(1-x(t))+b)}\right) + (1 - x(t)) \cdot N(t) \\ \text{s.t.} \quad & x(t) \in [x_{min}, x_{max}]. \end{aligned} \tag{2}$$

We define the Lagrangian of (2) as

$$\begin{aligned} \mathcal{L}(x(t), \lambda, \mu) = \gamma \left(1 - 10^{-(a(1-x(t))+b)}\right) + (1 - x(t)) \cdot \\ \left[\frac{x(t) - x_{min}}{x_{max} - x_{min}}\right] + \lambda(x(t) - x_{min}) \\ + \mu(x_{max} - x(t)), \end{aligned} \tag{3}$$

where $\lambda \geq 0$ and $\mu \geq 0$ are dual variables. Thus, we can characterize the primal and dual variables of the convex problem (2) using the Karush-Khun-Tucker (KKT) conditions [8].

Following the KKT condition (*details omitted for brevity*), the optimal per SCS resource selling point $x^*(t)$ satisfies the following relation

$$N = \frac{\ln(10) \cdot (\gamma a) \cdot 10^{-(a(1-x^*(t))+b)} \cdot (x_{min} - x_{max})}{1 - 2x^*(t) + x_{min}}. \tag{4}$$

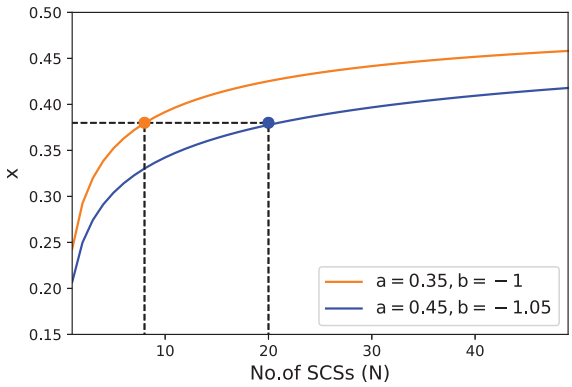


Fig. 2. Resource Trading Point for Competing SCSs.

We can rearrange (4) as $f(x^*(t)) = 0$, and obtain the value of $x^*(t)$ with *Netwon-Raphson method* [9]. We choose an appropriate initial guess that guarantees the quadratic convergence of the optimal solution. We use an initial guess $x_0^*(t) = E(\mathbf{x}(t)) = \frac{x_{max}+x_{min}}{2}$ to obtain $x^*(t)$ that follows the PDF $f_{\mathbf{x}(t)}(x) \sim U[x_{min}, x_{max}]$. Thus, an iterative method to obtain the solution is as follows:

$$x_{i+1}^*(t) = x_i^*(t) - \frac{f(x_i^*(t))}{\gamma a^2 \cdot \ln^2(10) \cdot 10^{-(a(1-x_i^*(t))+b)}}. \quad (5)$$

## IV. Numerical Results

We setup the SC market and increase the number of SCS up to 50. We use the coefficient $\gamma = 1$, and run the iterative algorithm for two different parametric configurations of $a$ and $b$. In Fig. 2, we observe that the value of resource trading point $x$ increases with the increase in the number of SCSs in the market up to a certain number. This is intuitive as the increase in SCSs directly corresponds to the growth of SC market with potential increase in number of transaction requests for various DApps services. Thus, the corresponding increase in frequency of mining is observed which requires a proper resource trading point for the mining network as characterized in the Fig. 2. However, the trend saturates as more SCS will not contribute much to the mining network's utility. Furthermore, larger values of parameter $a$ will introduce stringent resource selling point for the number of SCSs, to maximize the network's utility and trading benefits.

## V. Conclusion

In this work, we proposed a smart contract (SC) market, with the number of smart contract providers, namely SCS who can independently sell smart contracts to the requester(s) (DApps users) for various decentralized services. They act as a virtual miner and trade computing resourcing with the mining network for building the infrastructure for DApps. We model the network's utility considering the criticality of resource selling for the competing SCSs for building DApp infrastructure in the blockchain network. Further, the solution of the formulated optimization problem is characterized with the KKT solutions, and following iterative solution approach the optimal per SCSs resource selling point is obtained. Numerical results derives the optimal resource trading point for competing SCSs to maximize the utility of the mining network.

## Acknowledgment

This work was partially supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2015-0-00557, Resilient/Fault-Tolerant Autonomic Networking Based on Physicality, Relationship and Service Semantic of IoT Devices), and by MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2018-2015-0-00742) supervised by the IITP(Institute for Information & communications Technology Promotion). *Dr. CS Hong is the corresponding author.

## References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009.
[2] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plugin hybrid electric vehicles using consortium blockchains," IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 3154–3164, 2017.
[3] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in Proceedings of the 2017 on Cloud Computing Security Workshop, pp. 45–50, ACM, 2017.
[4] Ferrag, Mohamed Amine, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, and Helge Janicke. "Blockchain technologies for the internet of things: Research issues and challenges." IEEE Internet of Things Journal (2018).
[5] Wang, Jingzhong, Mengru Li, Yunhua He, Hong Li, Ke Xiao, and Chao Wang. "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications." IEEE Access 6 (2018): 17545-17556.
[6] Pandey, Shashi Raj, and Choong Seon Hong. "Response driven efficient task load assignment in mobile crowdsourcing." In 2018 International Conference on Information Networking (ICOIN), pp. 442-446. IEEE, 2018.
[7] Pandey, Shashi Raj, Sabah Suhail, Yan Kyaw Tun, and Choong Seon Hong., "Hierarchical Model for Consuming Proof-of-Work Complexity in Blockchain Networks." Proc. of the KIISE Korea Computer Congress 2018, pp. 373-375, 2018.
[8] S. Boyd and L. Vandenberghe, Convex optimization. Cambridge university press, 2004.
[9] S. D. Conte and C. De Boor, Elementary numerical analysis: an algorithmic approach. SIAM, Dec 2017, vol. 78.