Blockchain Technology Enabled Pay Per Use Licensing Approach for Hardware IPs

Krishnendu Guha[1], Debasri Saha[2], Amlan Chakrabarti[3]
A. K. Choudhury School of Information Technology
University of Calcutta
Kolkata, India
kgchem_rs@caluniv.ac.in[1], sahadebasri@gmail.com[2], acakcs@caluniv.ac.in[3]

***Abstract*—The present era is witnessing a reuse of hardware IPs to reduce cost. As trustworthiness is an essential factor, designers prefer to use hardware IPs which performed effectively in the past, but at the same time, are still active and did not age. In such scenarios, pay per use licensing schemes suit best for both producers and users. Existing pay per use licensing mechanisms consider a centralized third party, which may not be trustworthy. Hence, we seek refuge to blockchain technology to eradicate such third parties and facilitate a transparent and automated pay per use licensing mechanism. A blockchain is a distributed public ledger whose records are added based on peer review and majority consensus of its participants, that cannot be tampered or modified later. Smart contracts are deployed to facilitate the mechanism. Even dynamic pricing of the hardware IPs based on the factors of trustworthiness and aging have been focused in this work, which are not associated in existing literature. Security analysis of the proposed mechanism has been provided. Performance evaluation is carried based on the gas usage of Ethereum Solidity test environment, along with cost analysis based on lifetime and related user ratings.**

***Index Terms*—Blockchain, Hardware IP, Licensing**

I. Introduction

The present embedded era has witnessed a surge in the demand of hardware intellectual properties (IPs) or integrated circuits (ICs). It has been estimated by the International Technology Roadmap for Semiconductors (ITRS) that a ten times increase in design productivity will be required by 2020 [1]. Due to deficit in design productivity, system designers are adopting a modular design approach, where plug and play environment is facilitated. Hardware IPs are procured from different sources and integrated to form a complete system [2]. Such a technique not only aids in the reduction of design cost, but also ensures meeting of stringent marketing deadlines.

In such scenarios, authentication of hardware IPs is very important. As in case of malfunction, if source of vulnerability can be traced during post mortem analysis, then legal action can be taken with associated vendor who supplied the malicious IP. Even eminent researchers have termed authentication of procured resources as the first line of defense [5].

A blockchain is a growing list of records called blocks, that are connected to each other by cryptographic hash functions [4]. Details of blockchain is discussed in Section II. Recent works on hardware IP tracing have sought refuge to blockchain technology [5], [6]. But these neither focus on pay per use licensing of the hardware IPs, nor does they determine the dynamic pricing of the hardware IPs based on factors like aging and trustworthiness. Trustworthy IPs which provide the best performance are generally deployed in critical regions of the system, while less trustworthy IPs or aged IPs are generally deployed for functioning in lesser critical and non-critical regions of the system.

Hence, an IP producer may initially charge low for a newly produced IP. After a certain number of uses, when it reaches a trustworthy level, the producer may price it high. Again with time, when performance of the IP will degrade due to aging, the producer may lower its price accordingly, till its expiry. Thus, a pay per use licensing scheme suits best for modern day hardware IPs, which will benefit both producers and users.

Existing pay per use licensing or hardware metering techniques [7], [8] are associated with a centralized third party, which is assumed to be trusted and do not adhere to a blockchain based technology. Even dynamic pricing is not focused in these mechanisms.

In this work, we propose a pay per use licensing mechanism for hardware IPs, powered by blockchain technology. Centralized third parties (associated with control for the pay per use licensing mechanism deployed by previous techniques) are eradicated, which enhances the trust factor of the system. Smart contracts (discussed in Section II) are deployed for facilitating the pay per use licensing scheme. The smart contracts perform functions like registering new IPs, providing information of the IPs to the users and managing payment and license delivery mechanism. In addition to this, it keeps a record on the ratings of the IPs received as feedback from the users, which determines its trustworthiness. The mechanism also facilitates automated dynamic pricing of the IPs based on prior protocols defined in the smart contracts, according to factors like trustworthiness and age of the hardware IPs. Security analysis of the protocol is discussed. Performance evaluation of the proposed mechanism is based on the amount of gas limit utilized when implemented in Ethereum Solidity test environment. Cost analysis is presented graphically with respect to factors like lifetime and user ratings of an IP.

Our main contributions are summarized as follows:

(i) Analyzing limitations of the existing pay per use licensing mechanisms (where blockchain technology is not utilized).

(ii) Proposing a blockchain enabled pay per use licensing strategy for hardware IPs.

(iii) Smart contract enabled dynamic cost pricing of the hardware IPs based on factors like age and trustworthiness.

This work is supported by 'Department of Science and Technology, Government of India, INSPIRE Fellowship Number IF150916', 'Intel India Final Year Research Fellowship Award 2019' and 'TEQIP III, Univ, of Calcutta'

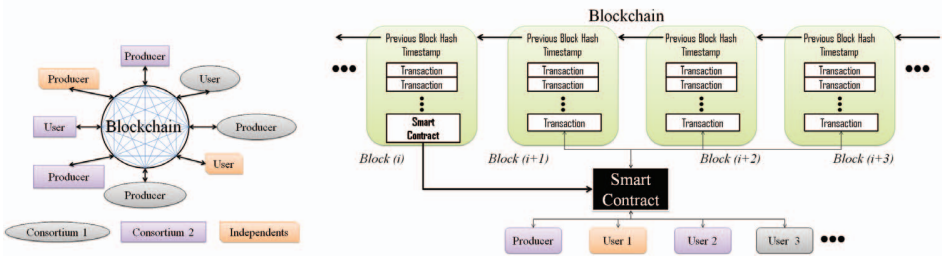

Fig. 1: *Diagrammatic Illustration of a Blockchain System*

This paper is organized as follows. In Section II, basics are discussed. Existing works and limitations are exhibited in Section III. The proposed mechanism is presented in Section IV. Security analysis of the proposed technique is discussed in Section V. Section VI deals with implementation and analysis. The paper concludes in Section VII.

II. Background

A. Blockchain

Blockchain is a distributed public ledger which stores information in a continuously growing list of connected blocks [4]. Each block comprises a set of transactions, with a time stamp and a link to the previous block, via a cryptographic hash, as shown in Fig. 1. A transaction may represent any type of information, which in the present case are IP details or payment and licensing details. Each new block is reviewed by the participants and only after receiving majority consensus, is added to the blockchain. Data once recorded, cannot be modified. If wrong data is added, then correctional measures have to be recorded via transactions in new blocks. Blockchains can be public or private and we consider a private one.

B. Smart Contract

A Smart Contracts (SC) is a computer program that executes autonomously in a blockchain [4]. Protocols and conditions are defined in prior for these SCs, based on which it operates, like the verification or negotiation strategy of a contract.

C. Identification of Blockchain Participants

Each blockchain participant (χ) has a public key ($K_{pub}[\chi]$) and a private key ($K_{pri}[\chi]$). Information sent to a participant is encrypted by ($K_{pub}[\chi]$), which can be decrypted by ($K_{pri}[\chi]$). Similarly, χ can digitally sign an information, by encrypting it with ($K_{pri}[\chi]$), which others can decrypt with ($K_{pub}[\chi]$).

D. Verification Mechanism of Hardware IPs by PUFs

Side channel parameters like delay depend on the intrinsic property of the base semiconductor material of ICs or hardware IPs, which are introduced during their fabrication. This disorderness is classified as a function and a set of challenge response pairs (CRPs) are generated for its unique classification [3]. CRPs are provided by producers to users. Users apply challenges and matches the obtained responses to those provided, to confirm the genuineness of hardware IP.

III. Existing Works and Limitations

A. Hardware Metering/ Pay Per Use Licensing Mechanisms

Gaining post fabrication control of hardware IPs via hardware metering was proposed in [10], [11]. A pay per use licensing for IPs of reconfigurable hardware platform was proposed in [7]. A PUF-FSM binding scheme for pay per use licensing and protection of IPs was proposed in [8].

Limitations

1. These consider a centralized third party for controlling the operations, which cannot be trusted.

2. These do not focus on dynamic pricing of the IPs based on factors like trustworthiness and aging.

B. Blockchain based IC Authentication

For authentication of IoT devices, PUFs were used for generating their identification details, which were stored in blockchains for verification by the users [9]. Logging supply chain information in blockchain for tracing of hardware IPs was proposed in [6]. With use of SCs, registering and transferring ownership of hardware IPs was made feasible [5].

Limitation: These do not focus on pay per use licensing.

IV. Blockchain Technology Enabled Pay Per Use Licensing Approach for Hardware IPs

A. Creation of Hardware IP

An IP producer creates a new hardware IP. A PUF is used for its identification, whose CRPs are recorded.

A set of one time passwords (OTPs) are used to activate the functionality of the hardware IP for each use, which is facilitated with the aid of a finite state machine (FSM), as described in Fig. 2. After an OTP activates the functionality of the IP, the path of that FSM is deactivated to prevent its future use. Simultaneously, the next OTP is activated. The set of OTPs and their order is also recorded by the IP producer.

B. Registration of the Hardware IP in the Blockchain

Rules of the SC in the blockchain are pre-decided and majority agreed. It performs functions like *register, enquire, cost_determination, receive_payment, manage_OTP, send_payment and receive_feedback*. Via these functions, SC co-ordinates the pay per use licensing mechanism.

For registration of the hardware IP in the blockchain, the IP producer sends information comprising the ID of Hardware IP, its CRPs, Initial Cost, Lifetime and its Public Key as a transaction. This information is signed by its private key.

If a majority of the participants of the blockchain provide consent to the transaction, then the $register$ functionality of the smart contract is triggered and the associated details are recorded in the blockchain.

C. Enquiry about Hardware IP by an User

An user may procure a hardware IP directly from the IP producer or from other users. Before its use, the user needs to know its authenticity. For this, it sends an enquire message to the blockchain, which comprises the ID of the hardware IP.

The $enquire$ functionality of the SC is triggered, which provides details of the hardware IP like the public key of the owner, its CRPs, lifetime, number of times used. It also

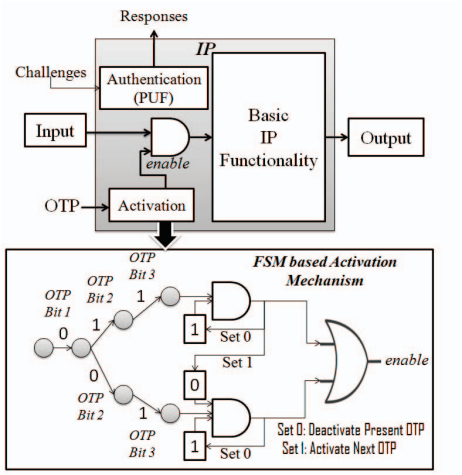

Fig. 2: *Structure of IP and FSM Based Activation Mechanism*

executes the $cost\_determination$ functionality to provide the license fees for associated usage.

We consider a dynamic pricing model based on the number of times it is used and related ratings or feedback provided by the users as follows: Let lifetime of an IP be divided into five phases. Then tentative cost (C_1) in its five phases will be *IC, 2*IC, 1.5*IC, IC and 0.5*IC*, where IC is the initial cost provided by the producer during registration. If a 3 scale rating ($R1, R2, R3$) is considered, then the final cost will be based on the weighted average rating, $R = (3 * R1 + 2 * R2 + R3)/(R1 + R2 + R3)$, which is $0.5 * C_1$ if $R = 1$, $0.7 * C_1$ if R is between 1 and 2, C_1 if R is between 2 and 2.5 and $1.5 * C_1$ if R is between 2.5 and 3.

Any type of pricing model can be developed, which needs to be agreed by majority of the participants of the blockchain and duly recorded in the SC.

D. Physical Authentication of the Hardware IP

The user applies the challenges to the hardware IP and matches the obtained responses, with the responses provided. A match in responses indicate genuineness of the IP.

E. Payment and OTP Management

This comprises three phases:

Phase 1: If the user is satisfied with the genuineness of the hardware IP, its cost and average rating, then it moves on to payment. The payment can be made via standard blockchain based transaction schemes. This information is again signed by the user with its private key and sent as a transaction. On majority consensus, this is recorded in the blockchain. $receive\_payment$ function of the smart contract is actuated. If the sent value matches the cost value, then notification is sent to the owner, else payment is declined.

Phase 2: The producer encrypts the OTP first with the public key of the user and then signs it or encrypts it with its private key. This information is sent as a transaction to the blockchain. On majority consensus, this is recorded in the blockchain and the OTP is sent to the user, who can decrypt it first with the public key of the owner and then with its own private key. This is the $manage\_OTP$ function.

Phase 3: The currencies received from the user are sent to the producer, denoted by $send\_payment$ function. $Usage$ variable related to the hardware IP is incremented by 1.

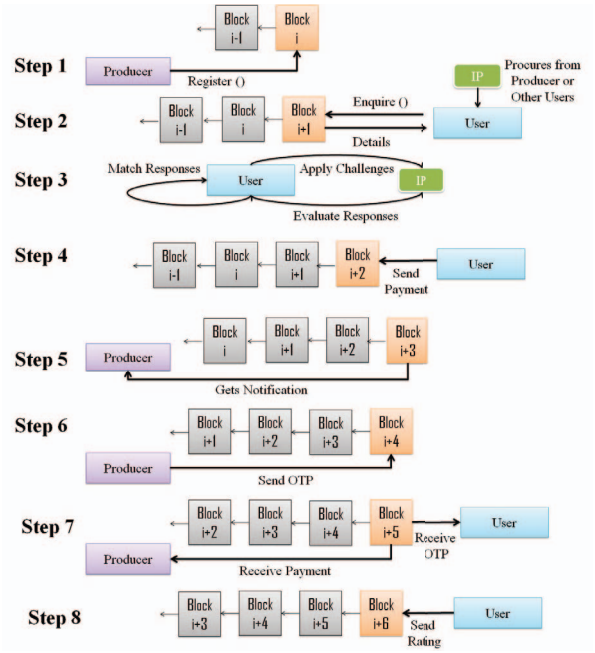

Fig. 3: *Diagrammatic Representation of Blockchain Enabled Pay Per Use Licensing Mechanism for Hardware IPs*

F. Feedback from User

The user can send a rating, $R1\ or R2\ or R3$, related to the hardware IP as a transaction, signed by its private key. On majority consensus, this is recorded in the blockchain. For this, $receive\_feedback$ functionality of the SC executes, which increments the related rating by 1.

The proposed blockchain enabled pay per use licensing mechanism is presented in Fig. 3.

V. Security Analysis of the Proposed Approach

In this section, we discuss problem scenarios and effectiveness of our proposed mechanism to handle these:

1) Registration of Fake IPs: Previously, nexus among a producer and the central third party controller could facilitate registration of fake IPs. However, in the automated blockchain mechanism, only members can register their IPs. Even majority consensus among all members is needed before registering an IP. Moreover, as details of each IP is signed by the producer, hence, the producer is liable for any type of malfunction. Thus, possibility of fake IP registration is highly negligible.

2) Problem of Double Spending: Not applicable as the hardware IP is a physical entity and only a single user can access it at a time. As two users can never simultaneously possess the same hardware IP, hence, two users will never send license fees at the same time, which is sent only after ascertaining its authenticity via CRPs in the actual IP.

3) Arbitrary Pricing: Previously, if a nexus was present among the central third party and the producer, then they could charge arbitrary license fees from the users. Presently, as pricing mechanism is pre-determined as per rules of the SC, the users are safeguarded from arbitrary pricing.

4) Non-repudiation: A case may arise if the producer sends a wrong OTP. However, as the OTP is signed by the producer, the producer has to bear its liability if it does not work. The user can get his license fees back or take legal actions.

TABLE I: Operational Cost for Functions

Operation	Gas Units	Gas Cost (Ether)
register()	452593	0.00492873
enquire()	91756	0.000999222
cost_determination()	359686	0.00391698
receive_payment()	65896	0.000717607
receive_OTP()	63512	0.000691645
send_payment()	67853	0.000738919
receive_feedback()	49561	0.000539719

5) Hijacking IPs by the User: An unethical user may try to hijack and sell a hardware IP, posing as its producer. However, as the registration details are stored in a blockchain, hence, any potential buyer can easily verify the ownership.

6) Duplication of IP Design via Side Channel Analysis: An user may try to get acquainted with intricate details of an IP via side channel analysis and try to duplicate it. For this, several operations are required. As pay per use licensing is followed, the producer will understand this based on licensing records stored in blockchain and take appropriate actions.

7) Overuse of Hardware IP: After a legal use via a valid OTP, an unethical user may try to overuse it by applying all possible sets of OTPs. This illegal action will come to notice of the producer when the next legal OTP will be generated, as OTP next in order as per the producer record will not match the OTP for unlocking the overused IP. Via blockchain records, the producer will be able to identify the unethical user.

8) Incorrect Payment from User: Previously, if a nexus was present among the central party and an user, the user may pay less. Presently, this is not possible as the mechanism is automated and follows pre-decided rules of the SC, where user payment is made via a signed transaction, that is recorded in the blockchain after peer review by members.

9) Non-sending of OTP by Producer: Previously, if a nexus was present among the centralized third party and the producer, then an user can be cheated by stopping the sending of OTP, after payment. Presently, the payment is only transferred to the producer after the producer has sent the OTP, else refunded back to the user.

VI. Implementation and Analysis

A. Implementation Strategy

Ethereum's test environment tool, $testrpc$, provides an execution environment for performance analysis [12]. SCs are scripted in Solidity [13] and evaluated based on gas usage.

Hardware IPs of standard benchmarks like ISCAS 85, ISCAS 89, ITC 99 and HLS 1992 are considered for analysis. During their HDL synthesis, in their Verilog codes, associated PUF and FSM based activation mechanisms are incorporated. Lifetime of the IPs is varied in each case for experimentation. Even additional delay inducing circuitry is added, which degrades their performance after a certain number of usage.

B. Performance Analysis

Performance analysis is determined based on the total gas amount exhausted for executing the functions in the SC. Ethereum's test environment tool [12] has the capability to automatically count the gas amount. 1 Gas = $10.89 * 10^9$ ETH (10.89 Gwei). Based on this, operational costs for our proposed functions is analyzed in Table I. As these are quite nominal, hence, our methodology suits practical applications.

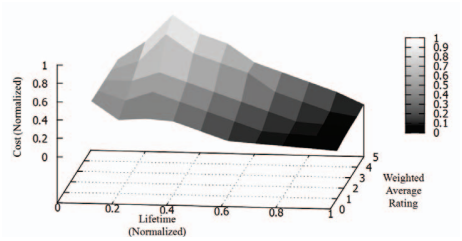

Fig. 4: *Analysis of Cost (Normalized) based on Number of Uses or Lifetime (Normalized) and Weighted Average Rating*

C. Cost Analysis

Cost analysis is performed via simulation based experiments over lifetime and average weighted rating for several dynamic pricing models, with ratings on a scale from 1-5. The analysis is provided graphically in Fig. 4. As evident, cost is nominal during initial stages, then increases in middle stages and eventually decreases with lifetime. However, the factor of rating impacts the normal behavior, as when an IP is rated low due to non-performance, its cost decreases accordingly.

VII. Conclusion

A blockchain enabled pay per use licensing scheme, where no centralized third party is involved, is proposed in the current paper. A dynamic pricing scheme based on the factors of aging and trustworthiness is also presented. Security analysis for the proposed mechanism is discussed. Performance evaluation is carried based on gas usage in Ethereum Solidity, along with cost analysis based on lifetime and weighted average ratings. Nominal gas usage depicts effectiveness of the mechanism.

References

[1] International Technology Roadmap for Semiconductors, 2013, *Available : www.itrs.net/reports.html*

[2] J. V. Rajendran, O. Sinanoglu, R. Karri, "Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach," *IEEE Transactions on VLSI Systems*, vol. 24, no. 9, pp. 2946-2959, 2016.

[3] R.Pappu, B.Recht, J.Taylor, and N.Gershenfeld, Physical one-way functions, *Science*, vol.297, no.5589, pp.2026-2030,2002.

[4] V. Buterin, 2015, "On public and private blockchains," *Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/*

[5] Md N. Islam, S. Kundu, "Enabling IC Traceability via Blockchain Pegged to Embedded PUF," *ACM Transactions on Design Automation of Electronic Systems*, vol. 24, no. 3, pp. 36:1-36:23, 2019.

[6] Md N. Islam, V. C. Patii, S. Kundu, "On IC traceability via blockchain," *In Proceedings of the International Symposium on VLSI Design, Automation and Test (VLSI-DAT18)*, 2018, pp. 14.

[7] R. Maes, D. Schellekens, I. Verbauwhede "A Pay-per-Use Licensing Scheme for Hardware IP Cores in Recent SRAM based FPGAs," *IEEE Trans. on Information Forensics and Sec*, vol.7, no.1, pp.98-108, 2012

[8] J. Zhang, Y. Lin, Y. Lyu and G. Qu, "A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing," *IEEE Trans. on Information Forensics and Sec*, vol. 10, no. 6, pp. 1137-1150, 2015.

[9] U. Guin, P. Cui and A. Skjellum, "Ensuring Proof-of-Authenticity of IoT Edge Devices Using Blockchain Technology," *IEEE International Conference on Blockchain*, 2018, pp. 1042-1049.

[10] F. Koushanfar, G. Qu, "Hardware metering," *in Proc. 38th Annu. Design Autom. Conf. (DAC)*, 2001, pp. 490-493.

[11] F. Koushanfar, "Provably secure active IC metering techniques for piracy avoidance and digital rights management," *IEEE Trans. Inf. Forensics Security,* vol. 7, no. 1, pp. 51-63, 2012.

[12] TestRPC, *[Available:] nethereum.readthedocs.io/en/latest/ethereum-and-clients/test-rpc/*

[13] Solidity, *[Available:] http://solidity.readthedocs.io/en/latest*