BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS

Title	BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS
Publication Type	Conference Paper
Year of Publication	2018
Authors	Bose, S., Raikwar, M., Mukhopadhyay, D., Chattopadhyay, A., Lam, K.
Conference Name	2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)
Date Published	jul
Keywords	active IC transactions, advanced technologies, BLIC protocol, blockchain, blockchain protocol, blockchain technology, composability, composite consensus protocol, Computer crime, cryptocurrencies, cryptography, data privacy, deleterious design modification, distributed ledger, electronic engineering computing, Hardware, huge paradigm shift, IC supply chains, ICs, integrated circuit design, integrated circuits, IP piracy, Manufacturing, passive IC transactions, Peer-to-peer computing, policy-based governance, Protocols, pubcrawl, Resiliency, smart contracts, split manufacturing, supply chain management, Supply chains, Watermarking

Abstract
Blockchain technology has brought a huge paradigm shift in multiple industries, by integrating distributed ledger, smart contracts and consensus protocol under the same roof. Notable applications of blockchain include cryptocurrencies and large-scale multi-party transaction management systems. The latter fits very well into the domain of manufacturing and supply chain management for Integrated Circuits (IC), which, despite several advanced technologies, is vulnerable to malicious practices, such as overproduction, IP piracy and deleterious design modification to gain unfair advantages. To combat these threats, researchers have proposed several ideas like hardware metering, design obfuscation, split manufacturing and watermarking. In this paper, we show, how these issues can be complementarily dealt with using blockchain technology coupled with identity-based encryption and physical unclonable functions, for improved resilience against certain adversarial motives. As part of our proposed blockchain protocol, titled `BLIC', we propose an authentication mechanism to secure both active and passive IC transactions, and a composite consensus protocol designed for IC supply chains. We also present studies on the security, scalability, privacy and anonymity of the BLIC protocol.

Cryptography data privacy Hardware Protocols Resiliency pubcrawl composability policy-based governance Peer-to-peer computing blockchain Computer crime supply chain management supply chains manufacturing cryptocurrencies smart contracts integrated circuits blockchain technology distributed ledger ICs integrated circuit design Watermarking electronic engineering computing blockchain protocol IP piracy split manufacturing active IC transactions advanced technologies BLIC protocol composite consensus protocol deleterious design modification huge paradigm shift IC supply chains passive IC transactions