Editorial: Distributed Public Ledgers and Block Chains—What Good Are They for Embedded Systems?

I have been ranting and raving a lot about the security of embedded systems, embedded systems for security, Internet of Things (IoT), and Cloud Security, Insider threats, and so on, for more than a year now on this editorial column. I have been trying to find scalable solutions to the of IoT authentication problem that is resilient to insider attacks, digital governance free of privileged user exploitation, and in general transactional record keeping with resilient authentication and nonrepudiation properties. Recently, with the breaking stories of bitcoins being stolen from a bitcoin exchange, I started peering into the literature on block chains. On further digging, I found the technology that underlies these crypto-currencies, such as bitcoin and ethereum, and it is fascinating. According to some articles, a technology revolution might be imminent on top of this distributed public ledger technologies. The reason I say “might be” is because a lot of the issues are still unsettled, especially the power hungry nature of this technology, the possibility of collusion among the independent parties involved in verifying public ledgers, authentication, statistical attacks on privacy, and so on. Notwithstanding all that, the technology seems to have tickled the imagination of many—including governments. Estonia government has already started experimenting with this technology—in particular, Keyless Signature Infrastructure (KSI), which allows citizens to cryptographically verify that all records about themselves are as they expect them to be. Since this is distributed public ledger based and verifiable by any citizen computationally, it is extraordinarily hard for a corrupt official to compromise its integrity. This technology gives its citizens confidence in the security and accuracy of this information, and thus the government can use this digital governance. In welfare states, this could be a revolutionary technology, where government schemes for providing aids to its financially weak citizens are often in the hands of corrupt officials who manipulate the data and the amounts, and there is no nonrepudiation or ways for the citizens to check the veracity. The government of India has launched the Aadhaar Scheme for collecting biometric and other information for every resident almost 6 years ago, but the security and integrity of that information has been questioned by crypto-experts, cyber-security experts, political scientists, and economists. The trust in that data and, even worse, in the security and accuracy of that data has been questioned seriously—but the government has been trying to use this database for “direct-money-transfer” and other schemes to aid the needy, bypassing the middlemen. The possibilities of corruption have been hanging like a dark shadow on these schemes. If the experiment being carried out by the Estonian government can be scaled to the size of Indian population—it might usher a new era of digital governance in India and reduce corruption drastically.

At our academic institutes, we are often confronted with the question of authenticity of transactions, for example, with student grade databases. The faculty enters the grades that are usually persisted into a relational database. Normally, the faculty and the administrators use username/password combinations to access this system and get authenticated and authorized to enter or change grades. This system even with two-factor authentication is prone to possible cyber breaches, as a password can be stolen or guessed, and the SMS-based second factor could also be compromised, as has

been found recently prompting the NIST to advise against using SMS-based two-factor authentication. Also, a grade change done by someone else on our behalf could not be easily attributed to the exact identity with these kinds of methods. A permissioned block chain (where only faculty and administrators have the permission to verify the transactions) might be the solution to this problem provided the trust base is wide enough.

Even in critical infrastructure security, there is buzz about using this technology to secure the last known trustworthy version of all firmware and software installed on IT equipment, and whenever any action that tampers any of these essential components of the system are taken, the integrity has to be verified on the block chain. The authentication in IoT autonomically, without involving a public key infrastructure requiring certification authorities, is being dreamed up at the moment as well. Recently, the British government's Office of Science published a report on this topic that is worth reading.¹ There are tens of startups working on bringing technology platforms to the market for solving various problems using block chain-type technologies.

The reason I am writing about this is because I would like to solicit proposals on how this technology would affect the IoT, embedded systems, and in general cyber physical systems, for example, for guaranteeing data integrity, providing scalable authentication platforms, or for resilient online services. This is an area that needs to be explored, and I suspect that a lot of our colleagues are deeply involved in such efforts. We would like to see papers on some interesting use of this technology in the embedded space (which includes IoT, Cyber-Physical Infrastructure, etc.) published in this journal soon.

Now, coming to the current issue of the journal, we are now entering Volume 16, and this is the first issue of Volume 16. We have two special issue papers published in this issue. The first one is "Emerging Technologies in Embedded Software and Systems," guest edited by Dakai Zhu, Meikang Qiu, and Samarjit Chakraborty. The idea of this special issue came from the 12th IEEE International Conference on Embedded Software and Systems, but the scope was sharpened to focus on emerging techniques and technologies, and an open call for papers was issued. The response was quite overwhelming, and after several rounds of reviews, 10 papers were selected to be included in the special issue. The other special issue is also based on the VIPES Workshop from 2015, which is a relatively young workshop on virtual prototyping of parallel and embedded systems. This issue was guest edited by Jeronimo Castrillon, and Cristina Silvano. For today's complex, multicore, heterogeneous embedded systems, virtual prototyping is an enabling technique, and VIPES has a history of attracting high-quality papers on this topic. I thank the guest editors of both these special issues for their conceptualization to smooth execution of the responsibilities of guest editors. We need more special issue proposals on various topics other than the one I mentioned earlier. We also have four regular papers in this issue on a potpourri of topics such as data quality in medical imaging, scratchpad memory management, battery-free mixed criticality systems, and Network on Chip.

Please keep the submissions pouring in and keep proposing exciting special issues.

Sandeep K. Shukla
Indian Institute of Technology Kanpur
September 22, 2016
Editor-in-Chief

¹The UK Government Chief Scientific Advisor. 2016. Distributed Ledger Technology beyond Block Chain. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.