Chapter 1
Metrics, Platforms, Emulators, and TestNets for Ethereum

Iamia Chaari Fourati

Higher Institute of Computer Science and Multimedia of Sfax, Tunisia

Taher Layeb

Higher Institute of Computer Science and Multimedia of Sfax, Tunisia

Achraf Haddaji

ENET'COM, Tunisia

Samiha Ayed

University of Technology of Troyes, France

Wiem Bekri

ENET'COM, Tunisia

ABSTRACT

Blockchain technology is considered the most relevant technology after the internet that revolutionizes many application domains. The first generation of BC technology, BC 1.0, is used for cryptocurrency purposes; the second generation, BC 2.0, as represented by Ethereum, is an open and decentralized platform empowering the running of decentralized applications (DApps) on top of BC as a new computing paradigm. Ethereum as a BC 2.0 leader has a large development community. Its open-source feature leads to the development of several emulation tools, simulators, TestNets, and security verification tools dedicated to Ethereum-based system performance analysis. Making an adequate decision regarding the choice of the most appropriate Ethereum tool responding to the requirement of a specific system or application still requires more investigation from researchers. In this regard, this chapter presents the characteristics of the most-used Ethereum simulators, emulators, and TestNets and provides comparative studies between Ethereum simulators, TestNets, and security verification tools.

INTRODUCTION

Before Ethereum (Wood, G., 2014), BC applications designed to do limited things. The crypto-currencies were designed to operate as peer-to-peer digital currencies, nothing more, which caused a problem for developers. To fill this gap, the developer of Ethereum, Vitalik Buterin, came up with an Ethereum Virtual Machine (EVM) as an inventive approach. EVM is a Turing-complete software executed on the Ethereum network. EVM allows anybody to execute whatever program he or she wants independent from the programming language. The EVM simplifies the creation of BC-based applications and enables the build of thousands of different apps on one single platform. Furthermore, Ethereum has its crypto-currency named Ether and a currency to pay for computations and transactions fees called Gas. Ethereum is principally for developers to build and deploy their decentralized applications, taking into consideration all the different industries. Besides, Ethereum can be used to build DAOs (Decentralized Autonomous Organizations) that are fully autonomous without any leader. DAOs run purely by Ethereum programming code and smart contracts.

Since all these decentralized applications will run on the Ethereum platform, they will all benefit from the BC properties. These proprieties are:

- **Immutability:** changes cannot be made to any data by a third party.
- **Tamper-proof and corruption-free**: the apps built are based on the principle of consensus and this makes censorship virtually impossible
- **Secure**: all applications and transactions secured with cryptography, giving them strong protection against fraud and hacking.
- **Anonymity**: based on the asymmetric cryptography and hashing of BC data (digital cryptographic keys, transactions...).

Although, the advantages of using Ethereum platform to run Dapp, the performance analysis of Ethereum- based solution require the use of simulators, emulators and Testnets. In this context, several tools are developed and this chapter presents these tools. Indeed, the manifolds of this chapter could be summarized into three points:

- Providing a comprehensive comparative study of current and various Ethereum emulation tools dedicated to analyzing the performance of Ethereum-based systems, which is useful for the
- researchers to better comprehend Ethereum aspects and to select the s
- uitable tools that fit their needs and their applications.
- Discussing Ethereum Testnets tools and their usage.
- Analyzing the potentialities of Ethereum security verification tools.

The rest of this chapter organized as follows: The second section pinpoints the Ethereum architecture. The third section discusses intensively BC evaluation strategies and metrics. The fourth section highlights the popular simulators and emulators tools developed for Ethereum-based BC. This book chapter provides a particular focus on Ethereum security verification tools. The fifth section describes and compares the most known Ethereum Testnets. The sixth section assesses open issues and future research direction regarding the possible enhancement of BC platforms. The last section concludes this chapter and pinpoints the lesson learned through this chapter.

Related Content

Understanding Blockchain: Case Studies in Different Domains
Hemraj Saini, Geetanjali Ratheeand Dinesh Kumar Saini (2021). *Large-Scale Data Streaming, Processing, and Blockchain Security (pp. 181-202).*
www.irma-international.org/chapter/understanding-blockchain/259471

IEEE802.21 Assisted Fast Re-Authentication Scheme over GSABA
Qazi Bouland Mussabbirand Thomas Owens (2012). *Situational Awareness in Computer Network Defense: Principles, Methods and Applications (pp. 221-243).*
www.irma-international.org/chapter/ieee802-assisted-fast-authentication-scheme/62384

A Cross Segment Analysis of Performance Variables of General Insurance Players in India
T. Joji Rao (2019). *International Journal of Risk and Contingency Management (pp. 18-30).*
www.irma-international.org/article/a-cross-segment-analysis-of-performance-variables-of-general-insurance-players-in-india/227020

Socio-Economic and Environmental Impacts of Poor Paper Management at Higher Education Institutions in Ethiopia: Evidence From Hawassa University
Akalewold Fedilu Mohammed, Abdurahman Hamza Ibrahimand Degwale Gebeyehu Belay (2018). *International Journal of Risk and Contingency Management (pp. 24-41).*
www.irma-international.org/article/socio-economic-and-environmental-impacts-of-poor-paper-management-at-higher-education-institutions-in-ethiopia/201073

Privacy and Banking in Australia
Supriya Singh (2009). *Handbook of Research on Social and Organizational Liabilities in Information Security (pp. 161-174).*
www.irma-international.org/chapter/privacy-banking-australia/21340