Slovenská Technická Univerzita

Fakulta Informatiky a Informačných Technológií

# Bitcoin a Ethereum: Porovnanie bezpečnosti

Semestrálna práca

2020 Norbert Matuška

Slovenská Technická Univerzita

Fakulta Informatiky a Informačných Technológií

# Bitcoin a Ethereum: Porovnanie bezpečnosti

Semestrálna práca

Študijný program: B – INFO 4

Študijný odbor: informatika

Konzultant: Ing. Bystrík Bindas

2020

Norbert Matuška

# Čestné vyhlásenie

Prehlasujem, že som semestrálnu prácu vypracoval samostatne s využitím získaných teoretických poznatkov a s použitím uvedenej literatúry.

Sebechleby, December 2020 Norbert Matuška

**Abstrakt**

MATUŠKA, Norbert: Bitcoin a ethereum: Porovnanie bezpečnosti
Slovenská technická univerzita v Bratislave, Fakulta informatiky a informačných technológií
Bakalárska práca, 7 strán

Bitcoin a Ethereum, spoločne dve najväčšie kryptomeny na trhu, majú veľa podobností a spoločných prvkov: každá z nich je digitálna mena obchodovaná pomocou on-line výmien a následne uložená do rôznych typov peňaženiek kryptokurencie. Oba tieto tokeny sú decentralizované, čo znamená, že nie sú nijak regulované bankami alebo inými autoritami. Prirodzene, keďže nie sú regulované, môže to prilákať nechcených používateľov, ktorých zámeri by mohli byť škodlivé pre ostatných používateľov. V tejto práci, rozličné metódy poradenia si s týmito uživateľmi budú uvedené a prezentované. Či už použitím strojového učenia, honeypots alebo správanie vplyvných článkov, táto práca preskúma ako môžu tieto metódy pomôcť odhaliť a/alebo opísať podozrivé správanie a tým pádom predísť takému správaniu.

Kľúčové slová: bitcoin, ethereum, blockchain, bezpečnosť, články, honeypot

**Abstract**

MATUŠKA, Norbert: Bitcoin a ethereum: Security comparison
Slovak University of Technology in Bratislava, Faculty of information and information technology
Bachelor/Diploma work, 7 pages

Bitcoin and Ethereum, together the two biggest cryptocurrencies on the market, are similar in many ways: each is a digital currency traded via online exchanges and stored in various types of cryptocurrency wallets. Both of these tokens are decentralized, meaning that they are not issued or regulated by a central bank or other authority. Naturally, since it is not regulated, it can attract some unwanted users, whose intentions could be harmful to other users. In this paper, different methods on coping with these malicious users will be overviewed and presented. Using either machine learning, honeypots or behaviour of influental nodes, the paper will explore how these methods can help detect and/or profile suspicious behaviour and thus prevent such behaviour.

Keywords: bitcoin, ethereum, blockchain, security, nodes, honeypot

# Obsah

# 1 Úvod

Práca sa primárne venuje riešeniam bezpečnostných problémov pri kryptomenách Bitcoin a Ethereum pomocou škále rozličných spôsobov. Pomocou vysvetlenia viacerých techník vyhľadávania podozrivého správania a profilovania škodlivých uživateľov sa práca snaží priblížiť tieto témy a následne aj ukázať riešenie. Taktiež stručne vysvetlí a porovná tieto dve kryptomeny.

# 2 Comparison

The 21 st century is all about modernization and accepting new technologies. The Blockchain Technology is a prominent and reliable technology that is getting into almost every industry today. After it was first initiated in 2008, it has tremendously gained traction. Within a short span of 10 years, it is commendable that it has grown massively and has been easily accepted worldwide. Though the first application of this technology is cryptocurrency, blockchain technology has transcended to support more applications as well. Developers have been smart enough to study the underlying protocol and customize it according to their own requirements. Today, blockchain offers multiple functionalities like decentralization, security, transparency and democracy.Two such giants which are most popular in the blockchain world are - Bitcoin and Ethereum. The elemental difference between these two platforms of the blockchain technology is the purpose for which they have been created. In this paper, the underlying differences between these two blockchain platforms will be overviewed. Both these applications are cryptocurrencies, but the focus in this paper would be on the comparison of the the underlying concepts and their protocols. The objective of both platforms, the differences in their architectures and the consensus or agreement mechanism used between the participants would be summarized along with the scalability factors and limitations. This paper will provide a brief overview of both these platforms and a clear idea about their use in the industry today. [1]

# 3 Bitcoin Concepts, Threats, and Machine Learning Security Solutions

The concept of Bitcoin was first introduced by an unknown individual (or a group of people) named Satoshi Nakamoto before it was released as open-source software in 2009. Bitcoin is a peer-to-peer cryptocurrency and a decentralized worldwide payment system for digital currency where transactions take place among users without any intermediary. Bitcoin transactions are performed and verified by network nodes and then registered in a public ledger called blockchain, which is maintained by network entities running Bitcoin software. To date, this cryptocurrency is worth close to U.S.$150 billion[1] and widely traded across the world. However, as Bitcoin's popularity grows, many security concerns are coming to the forefront. Overall, Bitcoin security inevitably depends upon the distributed protocols-based stimulant-compatible proof-of-work that is being run by network entities called miners, who are anticipated to primarily maintain the blockchain (ledger). As a result, many researchers are exploring new threats to the entire system, introducing new countermeasures, and therefore anticipating new security trends. In this survey paper, we conduct an intensive study that explores key security concerns. We first start by presenting a global overview of the Bitcoin protocol as well as its major components. Next, we detail the existing threats and weaknesses of the Bitcoin system and its main technologies including the blockchain protocol. Last, we discuss current existing security studies

[1] United States Dollar

and solutions and summarize open research challenges and trends for future research in Bitcoin security. [2]

# 4 Profiling of Malicious Users Using Simple Honeypots on the Ethereum Blockchain Network

Blockchain is a service operated by a peer-to-peer type distributed network, and protocol control such as JSON-RPC[2] is implemented as the interface for flexibility and operability. However, attacks that use protocol control against vulnerable and unmanaged interfaces have been reported. One of the methods to track cyber attacks on such a malicious user's network service is a honeypot that imitates the service and acquires attacker's behavior information. In this research, focusing on the Ethereum network, the behavior of malicious users is clarified using malicious communication history sent to simple honeypots installed in nine countries, Ethereum network information and darknet arrival packets. By analyzing these, the behavior of attackers and the tendency of requests were elucidated, and primary safety measures were established. [3]

# 5 Analysis of Ethereum Network Properties

Ethereum is arguably the second most popular cryptocurrency-based network after Bitcoin, both make use of the distributed ledger technology known as blockchain. The blockchain-based networks are considered to be secure, but the level of provided security is proportional to the number of connected nodes, the number of influential nodes and the supported amount of hash power. Thus, the knowledge of the network properties and nodes behavior is useful to protect the network from the possible attacks such as double spending attacks, DDoS[3] attacks, 51% attacks, and Sybil attacks. In this paper, we propose nodes discovery mechanism, which performs a P2P[4] links discovery on Ethereum main-network. For that, we developed the Search-node, a modified version of Ethereum Client that search for all participating nodes in the network, store the nodes identification in the Bucket, and then process the peer discovery method. We analyze the collected data to discover the relationship between nodes, heavily-connected nodes, nodes geo-distribution and provide network snapshots, as well as some data related to security issues and possible attacks over the influential nodes. Our results show that approximately 300,000 nodes are connected over Ethereum network, and among these roughly 139 nodes show a high-degree. [4]

[2] Remote Procedure Call
[3] distributed denial of service
[4] peer-to-peer

# Literatúra

[1] B. P. Rankhambe and H. Kaur Khanuja. A comparative analysis of blockchain platforms – bitcoin and ethereum. In *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, pages 1–7, 2019.

[2] M. Rahouti, K. Xiong, and N. Ghani. Bitcoin concepts, threats, and machine-learning security solutions. *IEEE Access*, 6:67189–67205, 2018.

[3] K. Hara, T. Sato, M. Imamura, and K. Omote. Profiling of malicious users using simple honeypots on the ethereum blockchain network. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–3, 2020.

[4] S. H. Maeng, M. Essaid, and H. T. Ju. Analysis of ethereum network properties and behavior of influential nodes. In *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pages 203–207, 2020.