IEEE

((("Full Text Only":Blockchain) AND "Full Text Only":anti money laundering) NOT "Full Text Only":regulations)

A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures

Abstract:
The rapid improvement in the global connectivity standards has escalated the level of trade taking place among different parties. Advanced communication standards are allowing the trade of all types of commodities and services. Furthermore, the goods and services developed in a particular region are transcending boundaries to enter into foreign markets. Supply chains play an essential role in the trade of these goods. To be able to realize a connected world with no boundary restrictions in terms of goods and services, it is imperative to keep the associated supply chains transparent, secure, and trustworthy. Therefore, some fundamental changes in the current supply chain architecture are essential to achieve a secure trade environment. This paper discusses the supply chain's security-critical application areas and presents a detailed survey of the security issues in the existing supply chain architecture. Various emerging technologies such as blockchain, machine learning (ML), and physically unclonable functions (PUFs) as solutions to the vulnerabilities in the existing infrastructure of the supply chain have also been discussed. Recent studies reviewed in this work reveal a growing sentiment in the industry towards new and emerging technologies such as IoT, blockchain, and machine learning. While many organizations have already adopted IoT applications and AI systems in their businesses, widespread adoption of blockchain remains distant. It has also been found that over the past decade, PUF-based authentication systems have gained much ground. However, a proper reference model for their implementation in complex supply chains is still missing.
Published in: IEEE Internet of Things Journal (Early Access)
Page(s): 1 - 1
Date of Publication: 22 September 2020
DOI: 10.1109/JIOT.2020.3025775
Publisher: IEEE
V. Hassija, V. Chamola, V. Gupta, S. Jain and N. Guizani, "A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures," in *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2020.3025775.

Blockchain Application for Central Banks: A Systematic Mapping Study

Abstract: Blockchain is a novel technology capturing the attention of Central Banks and a technology with significant disruptive potential. However, a gap in research effort between practitioners and academics seems to have emerged. This paper analyses and maps that gap by exploring trends in peer-reviewed research contributions through thematic categorisation of academic literature on Distributed Ledger Technology (DLT) use-cases for services, operations and functions performed by central banks. Furthermore, this paper provides summaries of opportunities and challenges for central banks arising from

blockchain adaptation to each of those use-cases. To achieve this goal, we utilise a Systematic Mapping Study approach. The paper presents an in-depth assessment of statistical and thematic analysis of research maturity and the types of researchers, with specific emphasis on types of central bank use-cases considered for blockchain adaptation. Our work contributes to an understanding of where the most or least attention is directed, allowing for identification of gaps and opportunities for both academics, practitioners and combinations of each. Results show that the research topic is a comparatively new domain. It confirms the gap between depth and volume of the research provision from industry and academia, with industry leading the trend. Our study also found that the most research-intensive use-cases are those for: 1) Central Bank issued Digital Currency (CBDC), 2) Regulatory Compliance and 3) Payment Clearing and Settlement Systems (PCS) operated by central banks; a comparatively low engagement was found in the areas of 4) Assets Transfer/Ownership and 5) Audit Trail.

Published in: IEEE Access (Volume: 8)
Page(s): 139918 - 139952
Date of Publication: 27 July 2020
Electronic ISSN: 2169-3536
INSPEC Accession Number: 19973904
DOI: 10.1109/ACCESS.2020.3012295
Publisher: IEEE
N. Dashkevich, S. Counsell and G. Destefanis, "Blockchain Application for Central Banks: A Systematic Mapping Study," in *IEEE Access*, vol. 8, pp. 139918-139952, 2020, doi: 10.1109/ACCESS.2020.3012295.

AI-Powered Blockchain - A Decentralized Secure Multiparty Computation Protocol for IoV

Abstract: The rapid advancements in autonomous technologies have paved way for vehicular networks. In particular, Vehicular Ad-hoc Network (VANET) forms the basis of the future of Intelligent Transportation System (ITS). ITS represents the communication among vehicles by acquiring and sharing the data. Though congestion control is enhanced by Internet of Vehicles (IoV), there are various security criteria where entire communication can lead to many security and privacy challenges. A blockchain can be deployed to provide the IoV devices with the necessary authentication and security feature for the transfer of data. Blockchain based IoV mechanism eliminates the single source of failure and remains secure at base despite having strong security, the higher level layers and applications are susceptible to attacks. Artificial Intelligence (AI) has the potential to overcome several vulnerabilities of current blockchain technology. In this paper, we propose an AI-Powered Blockchain which provides auto coding feature for the smart contracts making it an intelligent contract. Moreover, it speeds up the transaction verification and optimises energy consumption. The results show that intelligent contracts provide higher security compared to smart contracts considering range of different scenarios.

Published in: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)
Date of Conference: 6-9 July 2020

Date Added to IEEE *Xplore*: 10 August 2020
ISBN Information:
Electronic ISBN:978-1-7281-8695-5
Print on Demand(PoD) ISBN:978-1-7281-8696-2
INSPEC Accession Number: 19875795
DOI: 10.1109/INFOCOMWKSHPS50562.2020.9162866
Publisher: IEEE
Conference Location: Toronto, ON, Canada, Canada
G. Raja, Y. Manaswini, G. D. Vivekanandan, H. Sampath, K. Dev and A. K. Bashir, "AI-Powered Blockchain - A Decentralized Secure Multiparty Computation Protocol for IoV," *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, 2020, pp. 865-870, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162866.

PROQUEST

blockchain AND anti money laundering AND artificial intelligence NOT regulations

When Bitcoin encounters information in an online forum: Using text mining to analyse user opinions and predict value fluctuation

Young Bin Kim; Lee, Jurim; Park, Nuri; Choo, Jaegul; Jong-Hyun, Kim; et al.**PLoS One; San Francisco** Vol. 12, Iss. 5, (May 2017): e0177630. DOI:10.1371/journal.pone.0177630

Abstract

Bitcoin is an online currency that is used worldwide to make online payments. It has consequently become an investment vehicle in itself and is traded in a way similar to other open currencies. The ability to predict the price fluctuation of Bitcoin would therefore facilitate future investment and payment decisions. In order to predict the price fluctuation of Bitcoin, we analyse the comments posted in the Bitcoin online forum. Unlike most research on Bitcoin-related online forums, which is limited to simple sentiment analysis and does not pay sufficient attention to note-worthy user comments, our approach involved extracting keywords from Bitcoin-related user comments posted on the online forum with the aim of analytically predicting the price and extent of transaction fluctuation of the currency. The effectiveness of the proposed method is validated based on Bitcoin online forum data ranging over a period of 2.8 years from December 2013 to September 2016.

A Novel Electricity Transaction Mode of Microgrids Based on Blockchain and Continuous Double Auction

Wang, Jian; Wang, Qianggang; Zhou, Niancheng; Yuan, Chi.**Energies; Basel** Vol. 10, Iss. 12, (2017): 1971. DOI:10.3390/en10121971

Abstract: The installed capacity of distributed generation (DG) based on renewable energy sources has increased continuously in power systems, and its market-oriented transaction is imperative. However, traditional transaction management based on centralized organizations has many disadvantages, such as high operation cost, low transparency, and potential risk of transaction data modification. Therefore, a decentralized electricity transaction mode for microgrids is proposed in this study based on blockchain and continuous double auction (CDA) mechanism. A buyer and seller initially complete the transaction matching in the CDA market. In view of the frequent price fluctuation in the CDA market, an adaptive aggressiveness strategy is used to adjust the quotation timely according to market changes. DG and consumer exchange digital certificate of power and expenditure on the blockchain system and the interests of consumers are then guaranteed by multi-signature when DG cannot generate power due to

failure or other reasons. The digital certification of electricity assets is replaced by the sequence number with specific tags in the transaction script, and the size of digital certification can be adjusted according to transaction energy quantity. Finally, the feasibility of market mechanism through specific microgrid case and settlement process is also provided.

Keywords: microgrid market; electricity transaction; blockchain; continuous double auction; adaptive aggressiveness strategy

Development of Algorithms for Searching, Analyzing and Detecting Fraudulent Activities in the Financial Sphere

Khrestina, Marina Pavlovna; Dorofeev, Dmitry Ivanovich; Kachurina, Polina Andreevna; Usubaliev, Timur Rinatovich; Dobrotvorskiy, Aleksey Sergeevich.**European Research Studies; Anixis** Vol. 20, Iss. 4B, (2017): 484-498.

Abstract

According to Digital Evolution Index 2017, Russia is included to the category of so-called "Break Out" countries. The major problem to be encountered at transfer to the digital economy is adaptation of new technologies - such as Big Data, Blockchain, Internet of Things, Cryptocurrency, machine learning. No less important field is development offriendly informative environment facilitating international cooperation, cyber safety problems resolving, etc.

This example provides the data of the report prototype of a system to detect suspicious transactions. This system shall read and analyze the transaction database and, in accordance with search algorithms, it detects suspicious transactions within the entire data base.

The algorithm consists of several stages: development of a graph, selection of suspicious and trusted transactions, calculation of signs and machine learning. The methods of social connections analysis, parallel processing of graphs and mathematical apparatus of neural networks are used as the basis of this research.

Keywords: Digital economy, antifraud, AML-systems, digital transformation, machine learning, Big Data, financial control, parallel processing, neural networks.