A Survey Of Blockchain Security Issues And Challenges

Where To Download A Survey Of Blockchain Security Issues And Challenges

A Survey Of Blockchain Security Issues And Challenges | 8e283cf2a5d186f04fc79381bae66ebe

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2

Design and Analysis of Cryptographic Algorithms in Blockchain

Blockchain for Distributed Systems Security

AN ESSENTIAL GUIDE TO USING BLOCKCHAIN TO PROVIDE FLEXIBILITY, COST-SAVINGS, AND SECURITY TO DATA MANAGEMENT, DATA ANALYSIS, AND INFORMATION SHARING
Where To Download A Survey Of Blockchain Security Issues And Challenges

Distributed Systems Security contains a description of the properties that underpin the formal foundations of Blockchain technologies and explores the practical issues for deployment in cloud and Internet of Things (IoT) platforms. The authors—noted experts in the field—present security and privacy issues that must be addressed for Blockchain technologies to be adopted for civilian and military domains. The book covers a range of topics including data provenance in cloud storage, secure IoT models, auditing architecture, and empirical validation of permissioned Blockchain platforms. The book’s security and privacy analysis helps with an understanding of the basics of Blockchain and it explores the quantifying impact of the new attack surfaces introduced by Blockchain technologies and platforms. In addition, the book contains relevant and current updates on the topic. Blockchain for Distributed Systems Security contains the most recent information and academic research to provide an understanding of the application of Blockchain technology.

Blockchain Applications in IoT Security

This book seeks to generalize techniques and experiences in designing and analyzing cryptographic schemes for blockchain. It devotes three chapters to review the background and basic knowledge, four chapters to discuss specific types of cryptographic primitive design for blockchain, one chapter to discuss optimization tools and another chapter for blockchain regulation and economies. This book covers the systematic survey of research objects, as well as detailed reviews of cryptographic schemes, lectures and methodologies to practice cryptography. The main findings of this book are summarized as following, first, the practical design and analysis of cryptographic schemes for blockchain can address major problems in blockchain at algorithmic level. Then, some intrinsic deficiencies in some traditional cryptographic primitives, like centralized setup, impractical design, etc, prevent the successful application of these primitives in Blockchain. However, huge efforts are being made to make these primitives practical and applicable for researchers. Finally, the formal and rigorous design and analysis of public key cryptographic algorithms is vital to Blockchain. Design and Analysis of Cryptographic Algorithms in Blockchain is a useful textbook for graduate students and PhD students, or researchers who wish to connect cryptography with blockchain for research and developing projects.

Blockchain in the Industrial Internet of Things

The success of many companies through the assistance of bitcoin proves that technology continually dominates and transforms how economics operate. However, a deeper, more conceptual understanding of how these technologies work to identify innovation opportunities and how to successfully thrive in an increasingly competitive environment is needed for the entrepreneurs of tomorrow. Transforming Businesses With Bitcoin Mining and Blockchain Applications provides innovative insights into IT infrastructure and emerging trends in the realm of digital business technologies. This publication analyzes and extracts information from Bitcoin networks and provides the necessary steps to designing open blockchain. Highlighting topics that include financial markets, risk management, and smart technologies, the research contained within the title is ideal for entrepreneurs, business professionals, managers, executives, academicians, researchers, and business students.

Transforming Businesses With Bitcoin Mining and Blockchain Applications

The 2019 International Conference on System Science and Engineering (ICSSE) is an international conference that will take place in Dong Hoi City, Quang Binh province during July 20-21, 2019. This event will provide a great opportunity for scientists, engineers, and practitioners from all over the world to present the latest system design concepts, research results, developments and applications, as well as to facilitate interactions between scholars and practitioners. ICSSE 2019 will feature plenary speeches in emerging technology topics given by world renowned scholars.

Blockchain Security in Cloud Computing

Discusses how to choose and use cryptographic primitives, how to implement cryptographic algorithms and systems, how to protect each part of the system and why, and how to reduce system complexity and increase security.

2019 International Conference on System Science and Engineering (ICSSE)

Artificial intelligence (AI) is taking an increasingly important role in our society. From cars, smartphones, airplanes, consumer applications, and even medical equipment, the impact of AI is changing the world.
Security Issues And Challenges

Where To Download A Survey Of Blockchain

Blockchain technology applications in a variety of industries, and how this technology can further
a vital reference source that examines the latest scholarly material on trends, techniques, and uses of
the technology is key to the advancement of many industries.

The ability to perform such tasks as tracking fraud and securing the distribution of medical records, this
being applied in fields that include accounting and finance, supply chain management, and education. With
and security provided by blockchain technology is challenging innovation in a variety of businesses and is
using it for areas other than cryptocurrency has become increasingly popular as of late. The transparency
addition in several business domains ranging from healthcare, financial services, government, supply chain
and retail.

Cyber Security Practitioner's Guide

Blockchain is a technology that transcends cryptocurrencies. There are other services in different sectors
of the economy that can benefit from the trust and security that blockchains offer. For example, financial
institutions are using blockchains for international money transfer, and in logistics, it has been used for
supply chain management and tracking of goods. As more global companies and governments are
experimenting and deploying blockchain solutions, it is necessary to compile knowledge on the best
practices, strategies, and failures in order to create a better awareness of how blockchain could either
support or add value to other services. Cross-Industry Use of Blockchain Technology and Opportunities for
the Future provides emerging research highlighting the possibilities inherent in blockchain for different
sectors of the economy and the added value blockchain can provide for the future of these different sectors.

Blockchain for Information Security and Privacy

Blockchain is emerging as a powerful technology, which has attracted the wider attention of all businesses
across the globe. In addition to financial businesses, IT companies and business organizations are keenly
analyzing and adapting this technology for improving business processes. Security is the primary enterprise
application. There are other crucial applications that include creating decentralized applications and smart
contracts, which are being touted as the key differentiator of this pioneering technology. The power of any

Blockchain Technology and Applications illustrates how blockchain is being sustained through a host of
platforms, programming languages, and enabling tools. It examines: Data confidential, integrity, and
authentication Distributed consensus protocols and algorithms Blockchain systems design criteria and
systems interoperability and scalability Integration with other technologies including cloud and big data. It
details how blockchain is being blended with cloud computing, big data analytics and IoT across all
industry verticals. The book gives readers insight into how this path-breaking technology can be a value
addition in several business domains ranging from healthcare, financial services, government, supply chain
and retail.

Computational Intelligence in Pattern Recognition

The theme of the conference is Intelligent Computing for Smart World The aim and objective of the
conference is to bring together academicians, researchers, professionals, executives and practicing
engineers, from various industries, research institutes and educational bodies to share and exchange ideas
and information on the theme of the conference. The authors who wish to contribute to the conference are
solicited to submit their papers that illustrate research results, projects, surveying works and industrial
experiences addressing state of the art research and development in the areas related to computing,
communication, control and instrumentation. This conference will offer a real opportunity to discuss new
issues, tackle complex problems and find advanced enabling solutions which are able to shape new trends
in Engineering and Technology for the development of human mankind being as a whole

Security and Trust Issues in Internet of Things

Even though blockchain technology was originally created as a ledger system for bitcoin to operate on,
using it for areas other than cryptocurrency has become increasingly popular as of late. The transparency
and security provided by blockchain technology is challenging innovation in a variety of businesses and is
being applied in fields that include accounting and finance, supply chain management, and education. With
the ability to perform such tasks as tracking fraud and securing the distribution of medical records, this
technology is key to the advancement of many industries.

The Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government is
a vital reference source that examines the latest scholarly material on trends, techniques, and uses of
blockchain technology applications in a variety of industries, and how this technology can further
transparency and security. Highlighting a range of topics such as cryptography, smart contracts, and decentralized blockchain, this multi-volume book is ideally designed for academics, researchers, industry leaders, managers, healthcare professionals, IT consultants, engineers, programmers, practitioners, government officials, policymakers, and students.

**Blockchain Technology for Data Privacy Management**

This book highlights recent research on Soft Computing, Pattern Recognition, Information Assurance and Security. It presents 38 selected papers from the 10th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018) and the 14th International Conference on Information Assurance and Security (IAS 2018) held at Instituto Superior de Engenharia do Porto (ISEP), Portugal during December 13-15, 2018. SoCPaR - IAS 2018 is a premier conference and brings together researchers, engineers and practitioners whose work involves soft computing and information assurance and their applications in industry and the real world. Including contributions by authors from over 25 countries, the book offers a valuable reference guide for all researchers, students and practitioners in the fields of Computer Science and Engineering.

**Blockchains for Network Security**

This proceedings constitutes the refereed proceedings of the 15th EAI International Conference on Communications and Networking, ChinaCom 2020, held in November 2020 in Shanghai, China. Due to COVID-19 pandemic the conference was held virtually. The 54 papers presented were carefully selected from 143 submissions. The papers are organized in topical sections on Transmission Optimization in Edge Computing; Performance and Scheduling Optimization in Edge Computing; Mobile Edge Network System; Communication Routing and Control; Transmission and Load Balancing; Edge Computing and Distributed Machine Learning; Deep Learning.

**Convergence of Internet of Things and Blockchain Technologies**

Blockchain technology is a powerful, cost-effective method for network security. Essentially, it is a decentralized ledger for storing all committed transactions in trustless environments by integrating several core technologies such as cryptographic hash, digital signature and distributed consensus mechanisms.

**Blockchain**

**Blockchain For Dummies**

BIG DATA ANALYTICS FOR INTERNET OF THINGS Discover the latest developments in IoT Big Data with a new resource from established and emerging leaders in the field. Big Data Analytics for Internet of Things delivers a comprehensive overview of all aspects of big data analytics in Internet of Things (IoT) systems. The book includes discussions of the enabling technologies of IoT data analytics, types of IoT data analytics, challenges in IoT data analytics, demand for IoT data analytics, computing platforms, analytical tools, privacy, and security. The distinguished editors have included resources that address key techniques in the analysis of IoT data. The book demonstrates how to select the appropriate techniques to unearth valuable insights from IoT data and offers novel designs for IoT systems. With an abiding focus on practical strategies with concrete applications for data analysis and IoT professionals, Big Data Analytics for Internet of Things also offers readers: A thorough introduction to the Internet of Things, including IoT architectures, enabling technologies, and applications An exploration of the intersection between the Internet of Things and Big Data, including IoT as a source of Big Data, the unique characteristics of IoT data, etc. A discussion of the IoT data analytics, including the data analytical requirements of IoT data and the types of IoT analytics, including predictive, descriptive, and prescriptive analytics A treatment of machine learning techniques for IoT data analytics Perfect for professionals, industry practitioners, and researchers engaged in big data analytics related to IoT systems, Big Data Analytics for Internet of Things will also earn a place in the libraries of IoT designers and manufacturers interested in facilitating the efficient implementation of data analytics strategies.

**Blockchain Cybersecurity, Trust and Privacy**

This book provides the reader with the most up-to-date knowledge of blockchain in mainstream areas of security, trust, and privacy in the decentralized domain, which is timely and essential (this is due to the fact that the distributed and P2P applications is increasing day-by-day, and the attackers adopt new mechanisms to threaten the security and privacy of the users in those environments). This book also provides the technical information regarding blockchain-oriented software, applications, and tools required for the researcher and developer experts in both computing and software engineering to provide solutions.
and automated systems against current security, trust and privacy issues in the cyberspace. Cybersecurity, trust and privacy (CTP) are pressing needs for governments, businesses, and individuals, receiving the utmost priority for enforcement and improvement in almost any societies around the globe. Rapid advances, on the other hand, are being made in emerging blockchain technology with broadly diverse applications that promise to better meet business and individual needs. Blockchain as a promising infrastructural technology seems to have the potential to be leveraged in different aspects of cybersecurity promoting decentralized cyberinfrastructure. Blockchain characteristics such as decentralization, verifiability and immutability may revolve current cybersecurity mechanisms for ensuring the authenticity, reliability, and integrity of data. Almost any article on the blockchain points out that the cybersecurity (and its derivatives) could be revitalized if it is supported by blockchain technology. Yet, little is known about factors related to decisions to adopt this technology, and how it can systemically be put into use to remedy current CTP’s issues in the digital world. Topics of interest for this book include but not limited to: 
Blockchain-based authentication, authorization and accounting mechanisms
Applications of blockchain technologies in digital forensic and threat hunting
Blockchain-based threat intelligence and threat analytics techniques
Formal specification of smart contracts
Automated tools for outsmarting smart contracts
Security and privacy aspects of blockchain technologies
Vulnerabilities of smart contracts
Blockchain for secure cyber infrastructure and internet of things networks
Blockchain-based cybersecurity education systems
This book provides information for security and privacy experts in all the areas of blockchain, cryptocurrency, cybersecurity, forensics, smart contracts, computer systems, computer networks, software engineering, applied artificial intelligence for computer security experts, big data analysts, and decentralized systems. Researchers, scientists and advanced level students working in computer systems, computer networks, artificial intelligence, big data will find this book useful as well.

Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government

This book constitutes the proceedings of the 6th International Conference on Principles of Security and Trust, POST 2017, which took place in Uppsala, Sweden in April 2017, held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017. The 14 papers presented in this volume were carefully reviewed and selected from 40 submissions. They were organized in topical sections named: information flow; security protocols; security policies; and information leakage.

Practical Cryptography

In recent years, the surge of blockchain technology has been rising due to its proven reliability in ensuring secure and effective transactions, even between untrusted parties. Its application is broad and covers public and private domains varying from traditional communication networks to more modern networks like the internet of things and the internet of energy crossing fog and edge computing, among others. As technology matures and its standard use cases are established, there is a need to gather recent research that can shed light on several aspects and facts on the use of blockchain technology in different fields of interest. Enabling Blockchain Technology for Secure Networking and Communications consolidates the recent research initiatives directed towards exploiting the advantages of blockchain technology for benefiting several areas of applications that vary from security and robustness to scalability and privacy-preserving and more. The chapters explore the current applications of blockchain for networking and communications, the future potentials of blockchain technology, and some not-yet-prospected areas of research and its application. This book is ideal for practitioners, stakeholders, researchers, academicians, and students interested in the concepts of blockchain technology and the potential and pitfalls of its application in different utilization domains.

Blockchain for Smart Cities

Data has cemented itself as a building block of daily life. However, surrounding oneself with great quantities of information heightens risks to one’s personal privacy. Additionally, the presence of massive amounts of information prompts researchers into how best to handle and disseminate it. Research is necessary to understand how to cope with the current technological requirements. Large-Scale Data Streaming, Processing, and Blockchain Security is a collection of innovative research that explores the latest methodologies, modeling, and simulations for coping with the generation and management of large-scale data in both scientific and individual applications. Featuring coverage on a wide range of topics including security models, internet of things, and collaborative filtering, this book is ideally designed for entrepreneurs, security analysts, IT consultants, security professionals, programmers, computer technicians, data scientists, technology developers, engineers, researchers, academicians, and students.

The Blockchain Technology for Secure and Smart Applications across Industry Verticals

The purpose of this edited book is to present and showcase the basic fundamentals, applications, and
integration of both IoT and Blockchain. The trend of applying Blockchain to IoT is rapidly growing because it helps to overcome various challenges faced by IoT, from smart manufacturing to unmanned aerial vehicles. This book aims to showcase the basics of both IoT and Blockchain as well as the integration and challenges for existing practitioners. This book initiates conversations among technologists, engineers, scientists, and clinicians to synergize their efforts in producing low-cost, high-performance, highly efficient, deployable IoT systems. This book is theory-based and is useful for engineers from various disciplines, including industrial engineering, computer science, electronics, telecommunications, electrical, agricultural, and cybersecurity, along with researchers, professionals, and students.

**Blockchain Technology**

This book explores the concepts and techniques of cloud security using blockchain. Also discussed is the possibility of applying blockchain to provide security in various domains. The authors discuss how blockchain holds the potential to significantly increase data privacy and security while boosting accuracy and integrity in cloud data. The specific highlight of this book is focused on the application of integrated technologies in enhancing cloud security models, use cases, and its challenges. The contributors, both from academia and industry, present their technical evaluation and comparison with existing technologies. This book pertains to IT professionals, researchers, and academicians towards fourth revolution technologies.

**Large-Scale Data Streaming, Processing, and Blockchain Security**

This new volume looks at the electrifying world of blockchain technology and how it has been revolutionizing the Internet of Things and cyber-physical systems. Aimed primarily at business users and developers who are considering blockchain-based projects, the volume provides a comprehensive introduction to the theoretical and practical aspects of blockchain technology. It presents a selection of chapters on topics that cover new information on blockchain and bitcoin security, IoT security threats and attacks, privacy issues, fault-tolerance mechanisms, and more. Some major software packages are discussed, and it also addresses the legal issues currently affecting the field. The information presented here is relevant to current and future problems relating to blockchain technology and will provide the tools to build efficient decentralized applications. Blockchain technology and the IoT can profoundly change how the world—and businesses—work, and this book provides a window into the current world of blockchain. No longer limited to just Bitcoin, blockchain technology has spread into many sectors and into a significant number of different technologies.

**Enabling Blockchain Technology for Secure Networking and Communications**

Find out what Blockchain is, how it works, and what it can do for you! Blockchain is the technology behind Bitcoin, the revolutionary ‘virtual currency’ that’s changing the way people do business. While Bitcoin has enjoyed some well-deserved hype, Blockchain may be Bitcoin's most vital legacy. Blockchain For Dummies is the ideal starting place for business pros looking to gain a better understanding of what Blockchain is, how it can improve the integrity of their data, and how it can work to fundamentally change their business and enhance their data security. Blockchain For Dummies covers the essential things you need to know about this exciting technology's promise of revolutionizing financial transactions, data security, and information integrity. The book covers the technologies behind Blockchain, introduces a variety of existing Blockchain solutions, and even walks you through creating a small but working Blockchain-based application. Blockchain holds the promise to revolutionize a wide variety of businesses. Get in the know about Blockchain now with Blockchain For Dummies and be ready to make the changes to business that your colleagues and competitors will later wish they'd done. Discover ten ways Blockchain can change business. Find out how to apply a Blockchain solution. See how to make data more secure. Learn how to work with vendors. Filled with vital information and tips on how this paradigm-changing technology can transform your business for the better, this book will not only show you Blockchain’s full potential, but your own as well!

**Hands-On Cybersecurity with Blockchain**

This book presents a detailed exploration of adaption and implementation, as well as a 360-degree view spectrum of blockchain technologies in real-world business applications. Blockchain is gaining momentum in all sectors. This book offers a collection of protocol standards, issues, security improvements, applicability, features, and types of cryptocurrency in processing and through 5G technology. The book covers the evolution of blockchain from fundamental theories to present forms. It offers diversified business applications with usable case studies and provides successful implementations in cloud/edge computing, smart city, and IoT. The book emphasizes the advances and cutting-edge technologies along with the different tools and platforms. The primary audience for this book includes industry experts, researchers, graduates and under graduates, practitioners, and business managers who are engaged in blockchain and IoT-related technologies.
Role of Blockchain Technology in IoT Applications

Blockchain technology is defined as a decentralized system of distributed registers that are used to record data transactions on multiple computers. The reason this technology has gained popularity is that you can put any digital asset or transaction in the blockchain, the industry does not matter. Blockchain technology has infiltrated all areas of our lives, from manufacturing to healthcare and beyond. Cybersecurity is an industry that has been significantly affected by this technology and may be more so in the future. Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications is an invaluable resource to discover the blockchain applications for cybersecurity and privacy. The purpose of this book is to improve the awareness of readers about blockchain technology applications for cybersecurity and privacy. This book focuses on the fundamentals, architectures, and challenges of adopting blockchain for cybersecurity. Readers will discover different applications of blockchain for cybersecurity in IoT and healthcare. The book also includes some case studies of the blockchain for e-commerce online payment, retention payment system, and digital forensics. The book offers comprehensive coverage of the most essential topics, including: Blockchain architectures and challenges Blockchain threats and vulnerabilities Blockchain security and potential future use cases Blockchain for securing Internet of Things Blockchain for cybersecurity in healthcare Blockchain in facilitating payment system security and privacy. This book comprises a number of state-of-the-art contributions from both scientists and practitioners working in the fields of blockchain technology and cybersecurity. It aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this particular area or those interested in grasping its diverse facets and exploring the latest advances on the blockchain for cybersecurity and privacy.

Handbook of Research on Cyber Crime and Information Privacy

In recent years, industries have transitioned into the digital realm, as companies and organizations are adopting certain forms of technology to assist in information storage and efficient methods of production. This dependence has significantly increased the risk of cyber crime and breaches in data security. Fortunately, research in the area of cyber security and information protection is flourishing; however, it is the responsibility of industry professionals to keep pace with the current trends within this field. The Handbook of Research on Cyber Crime and Information Privacy is a collection of innovative research on the modern methods of crime and misconduct within cyber space. It presents novel solutions to securing and preserving digital information through practical examples and case studies. While highlighting topics including virus detection, surveillance technology, and social networks, this book is ideally designed for cybersecurity professionals, researchers, developers, practitioners, programmers, computer scientists, academicians, security analysts, educators, and students seeking up-to-date research on advanced approaches and developments in cyber security and information protection.


Distributed and peer-to-peer (P2P) applications are increasing daily, and cyberattacks are constantly adopting new mechanisms to threaten the security and privacy of users in these Internet of Things (IoT) environments. Blockchain, a decentralized cryptographic-based technology, is a promising element for IoT security in manufacturing, finance, healthcare, supply chain, identity management, e-governance, defence, education, banking, and trading. Blockchain has the potential to secure IoT through repetition, changeless capacity, and encryption. Blockchain for Information Security and Privacy provides essential knowledge of blockchain usage in the mainstream areas of security, trust, and privacy in decentralized domains. This book is a source of technical information regarding blockchain-oriented software and applications. It provides tools to researchers and developers in both computing and software engineering to develop solutions and automated systems that can promote security, trust, and privacy in cyberspace. FEATURES Applying blockchain-based secured data management in confidential cyberdefense applications Securing online voting systems using blockchain Safeguarding electronic healthcare record (EHR) management using blockchain Impacting security and privacy in digital identity management Using blockchain-based security and privacy for smart contracts By providing an overview of blockchain technology application domains in IoT (e.g., vehicle web, power web, cloud internet, and edge computing), this book features side-by-side comparisons of modern methods toward secure and privacy-preserving blockchain technology. It also examines safety objectives, efficiency, limitations, computational complexity, and communication overhead of various applications using blockchain. This book also addresses the combination of blockchain and industrial IoT. It explores novel various-levels of information sharing systems.

Bitcoin and Blockchain Security

The book aims to showcase the basics of both IoT and Blockchain for beginners as well as their integration and challenge discussions for existing practitioner. It aims to develop understanding of the role of blockchain in fostering security. The objective of this book is to initiate conversations among technologists, engineers, scientists, and clinicians to synergize their efforts in producing low-cost, high-performance,
highly efficient, deployable IoT systems. It presents a stepwise discussion, exhaustive literature survey, rigorous experimental analysis and discussions to demonstrate the usage of blockchain technology for securing communications. The book evaluates, investigate, analyze and outline a set of security challenges that needs to be addressed in the near future. The book is designed to be the first reference choice at research and development centers, academic institutions, university libraries and any institutions interested in exploring blockchain. UG/PG students, PhD Scholars of this fields, industry technologists, young entrepreneurs and researchers working in the field of blockchain technology are the primary audience of this book.

Principles of Security and Trust

Like many other scientific innovations, scientists are looking to protect the internet of things (IoT) from unfortunate losses, theft, or misuse. As one of the current hot trends in the digital world, blockchain technology could be the solution for securing the IoT. Blockchain Applications in IoT Security presents research for understanding IoT-generated data security issues, existing security facilities and their limitations and future possibilities, and the role of blockchain technology. Featuring coverage on a broad range of topics such as cryptocurrency, remote monitoring, and smart computing, this book is ideally designed for security analysts, IT specialists, entrepreneurs, business professionals, academicians, researchers, students, and industry professionals seeking current studies on the limitations and possibilities behind competitive blockchain technologies.

Blockchain for Cybersecurity and Privacy

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2: ChinaTech, Mobile Security, and Distributed Ledger emphasizes technological developments that introduce the future of finance. Descriptions of recent innovations lay the foundations for explorations of feasible solutions for banks and startups to grow. The combination of studies on blockchain technologies and applications, regional financial inclusion movements, advances in Chinese finance, and security issues delivers a grand perspective on both changing industries and lifestyles. Written for students and practitioners, it helps lead the way to future possibilities. Explains the practical consequences of both technologies and economics to readers who want to learn about subjects related to their specialties Encompasses alternative finance, financial inclusion, impact investing, decentralized consensus ledger and applied cryptography Provides the only advanced methodical summary of these subjects available today

Cross-Industry Use of Blockchain Technology and Opportunities for the Future

Role of Blockchain Technology in IoT Applications, Volume 115 in the Advances in Computers series, reviews the latest information on this topic that promises many applications in human life. According to forecasts made by various market research/survey agencies, there will be around 50 Billion connected devices (IoT) by 2020. Updates in this new release include chapters on the Technical Aspects of Blockchain and IoT, Integrated Platforms for Blockchain-Enablement, Intersections Between IoT and Distributed Ledger, Blockchain and Artificial Intelligence: How and Why Combining These Two Groundbreaking Technologies, Blockchain Applications in Health Care and Opportunities and Advancements Due to New Information Technology Frameworks, and more. Explores blockchain technology research trends in secured device to device communication Includes updates on secure vehicular communication (VANET) using blockchain technology Provides the latest on secure IoT communication using blockchain technology Presents use cases of blockchain technology in healthcare, the food chain, ERP and other emerging areas

Communications and Networking

This book features high-quality research papers presented at the 3rd International Conference on Computational Intelligence in Pattern Recognition (CIPR 2021), held at the Institute of Engineering and Management, Kolkata, West Bengal, India, on 24 - 25 April 2021. It includes practical development experiences in various areas of data analysis and pattern recognition, focusing on soft computing technologies, clustering and classification algorithms, rough set and fuzzy set theory, evolutionary computations, neural science and neural network systems, image processing, combinatorial pattern matching, social network analysis, audio and video data analysis, data mining in dynamic environments, bioinformatics, hybrid computing, big data analytics and deep learning. It also provides innovative solutions to the challenges in these areas and discusses recent developments.

Blockchain Technology and Applications

In an era of unprecedented volatile political and economic environments across the world, computer-based cyber security systems face ever growing challenges. While the internet has created a global platform for the exchange of ideas, goods and services, it has also created boundless opportunities for cyber crime. The debate over how to plan for the cyber security of the future has focused the minds of developers and
Where To Download A Survey Of Blockchain Security Issues And Challenges

scientists alike. This book aims to provide a reference on current and emerging issues on systems security from the lens of autonomy, artificial intelligence and ethics as the race to fight and prevent cyber crime becomes increasingly pressing.

Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)

Handbook of Research on Blockchain Technology presents the latest information on the adaptation and implementation of Blockchain technologies in real world business, scientific, healthcare and biomedical applications. The book’s editors present the rapid advancements in existing business models by applying Blockchain techniques. Novel architectural solutions in the deployment of Blockchain comprise the core aspects of this book. Several use cases with IoT, biomedical engineering, and smart cities are also incorporated. As Blockchain is a relatively new technology that exploits decentralized networks and is used in many sectors for reliable, cost-effective and rapid business transactions, this book is a welcomed addition on existing knowledge. Financial services, retail, insurance, logistics, supply chain, public sectors and biomedical industries are now investing in Blockchain research and technologies for their business growth. Blockchain prevents double spending in financial transactions without the need of a trusted authority or central server. It is a decentralized ledger platform that facilitates verifiable transactions between parties in a secure and smart way. Presents the evolution of Blockchain, from fundamental theories, to present forms Explains the concepts of blockchain related to cloud/edge computing, smart healthcare, smart cities and Internet of Things (IoT) Provides complete coverage of the various tools, platforms and techniques used in blockchain Explores smart contract tools and consensus algorithms Covers a variety of applications with real world case studies in areas such as biomedical engineering, supply chain management, and tracking of goods and delivery

Artificial Intelligence

The Blockchain Technology for Secure and Smart Applications across Industry Verticals, Volume 121, presents the latest information on a type of distributed ledger used for maintaining a permanent and tamper-proof record of transactional data. The book presents a novel compendium of existing and budding Blockchain technologies for various smart applications. Chapters in this new release include the Basics of Blockchain, The Blockchain History, Architecture of Blockchain, Core components of Blockchain, Blockchain 2.0: Smart Contracts, Empowering Digital Twins with Blockchain, Industrial Use Cases at the Cusp of the IoT and Blockchain Paradigms, Blockchain Components and Concepts, Digital Signatures, Accumulators, Financial Systems, and more. This book is a unique effort to illuminate various techniques to represent, improve and authorize multi-institutional and multidisciplinary research in a different type of smart applications, like the financial system, smart grid, transportation system, etc. Readers in identity-privacy, traceability, immutability, transparency, auditability, and security will find it to be a valuable resource. Provides a snapshot of the state of current research based on the decentralized system that provides security and privacy to the smart applications Chapters cover the fundamental concepts of the newly emerged Blockchain technology along with, the various smart applications Helps to elucidate new trading platforms that provides business benefits like efficiency, auditability, traceability, transparency, feedback, and security

Big Data Analytics for Internet of Things

Develop blockchain application with step-by-step instructions, working example and helpful recommendations Key Features Understanding the blockchain technology from the cybersecurity perspective Developing cyber security solutions with Ethereum blockchain technology Understanding real-world deployment of blockchain based applications Book Description Blockchain technology is being welcomed as one of the most revolutionary and impactful innovations of today. Blockchain technology was first identified in the world’s most popular digital currency, Bitcoin, but has now changed the outlook of several organizations and empowered them to use it even for storage and transfer of value. This book will start by introducing you to the common cyberthreat landscape and common attacks such as malware, phishing, insider threats, and DDoS. The next set of chapters will help you to understand the workings of Blockchain technology, Ethereum and Hyperledger architecture and how they fit into the cybersecurity ecosystem. These chapters will also help you to write your first distributed application on Ethereum Blockchain and the Hyperledger Fabric framework. Later, you will learn about the security triad and its adaptation with Blockchain. The last set of chapters will take you through the core concepts of cybersecurity, such as DDoS protection, PKI-based identity, 2FA, and DNS security. You will learn how Blockchain plays a crucial role in transforming cybersecurity solutions. Toward the end of the book, you will also encounter some real-world deployment examples of Blockchain in security cases, and also understand the short-term challenges and future of cybersecurity with Blockchain. What you will learn Understand the cyberthreat landscape Learn about Ethereum and Hyperledger Blockchain Program Blockchain solutions Build Blockchain-based apps for 2FA, and DDoS protection Develop Blockchain-based PKI solutions and apps for storing DNS entries Challenges and the future of cybersecurity and Blockchain
Who this book is for
The book is targeted towards security professionals, or any stakeholder dealing with cybersecurity who wants to understand the next-level of securing infrastructure using Blockchain. Basic understanding of Blockchain can be an added advantage.

Handbook of Research on Blockchain Technology

This book presents chapters from diverse range of authors on different aspects of how Blockchain and IoT are converging and the impacts of these developments. The book provides an extensive cross-sectional and multi-disciplinary look into this trend and how it affects artificial intelligence, cyber-physical systems, and robotics with a look at applications in aerospace, agriculture, automotive, critical infrastructures, healthcare, manufacturing, retail, smart transport systems, smart cities, and smart healthcare. Cases include the impact of Blockchain for IoT Security; decentralized access control systems in IoT; Blockchain architecture for scalable access management in IoT; smart and sustainable IoT applications incorporating Blockchain, and more. The book presents contributions from international academics, researchers, and practitioners from diverse perspectives. Presents how Blockchain and IoT are converging and the impacts of these developments on technology and its application; Discusses IoT and Blockchain from cross-sectional and multi-disciplinary perspectives; Includes contributions from researchers, academics, and professionals from around the world.

Blockchain Technology and the Internet of Things

There is a lot of buzz about Bitcoin and Blockchain lately, our expert authors will help to answer some imperative questions about the security involved in this new digital asset and ledger. This comprehensive new resource presents a thorough overview and analysis of the security and privacy provisions of Bitcoin and its underlying blockchain clients. This book goes beyond the analysis of reported vulnerabilities of Bitcoin, evaluating a number of countermeasures to deter threats on the system. Readers are given concrete solutions and recommendations on the best practices to use when relying on Bitcoin as a payment method. This resource provides a clear explanation of assumptions governing the security of Bitcoin, including the scalability measures adopted in Bitcoin, privacy for clients, and the proper means of securing Bitcoin wallets. Readers learn how the security and privacy provisions of other blockchain technologies compare to Bitcoin and the security lessons learned after extensive research of Bitcoin since the inception of the currency.