1.	Record Nr.	UNINA9910416086503321
	Titolo	Financial Cryptography and Data Security : FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers / / edited by Matthew Bernhard, Andrea Bracciali, L. Jean Camp, Shin'ichiro Matsuo, Alana Maurushat, Peter B. Rønne, Massimiliano Sala
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
	ISBN	3-030-54455-9
	Edizione	[1st ed. 2020.]
	Descrizione fisica	1 online resource (XXIV, 622 p. 838 illus., 81 illus. in color.)
	Collana	Security and Cryptology ; ; 12063
	Disciplina	005.82 005.824
	Soggetti	Data encryption (Computer science) Computer organization Data structures (Computer science) Computer security Cryptology Computer Systems Organization and Communication Networks Data Structures and Information Theory Systems and Data Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Tale of Two Browsers: Understanding Users' Web Browser Choices in South Korea -- User-Centered Risk Communication for Safer Browsing -- The Effects of Cue Utilization and Cognitive Load in the Detection of Phishing Emails -- Cue Utilization, Phishing Feature and Phishing Email Detection -- Dis-Empowerment Online- An Investigation of Privacy & Sharing Perceptions & Method Preferences -- Security and Privacy Awareness in Smart Environments – A Cross-Country Investigation -- Understanding Perceptions of Smart Devices -- In Our Employer We Trust: Mental Models of Office Worker’s Privacy Perceptions -- Behaviour of Outsourced Employees as Sources of Information System Security Threats -- Exploring Effects of Auditory Stimuli on CAPTCHA

Performance -- PassPage: Graphical Password Authentication Scheme Based on Web Browsing Records -- Empathy as a Response to Frustration in Password Choice -- Fixing the Fixes: Assessing the Solutions of SAST Tools for Securing Password Storage -- Incorporating Psychology into Cyber Security Education: A Pedagogical Approach -- Effectiveness of multi-stakeholder discussions for decentralized finance: a conference report of CoDeFi 2020 -- Multistakeholder Governance for the Internet -- Future of Finance: From G20 to practical implementation of multi-stakeholder governance on blockchain based finance -- Securing Cryptocurrency Exchange: Building up Standard from Huge Failures -- Origami voting: a non-cryptographic approach to transparent ballot verification -- Towards Improving the Efficacy of Code-Based Verification in Internet Voting -- Mechanized Proofs of Verifiability and Privacy in a paper-based e-voting Scheme -- Sets of Half-Average Nulls Generate Risk-Limiting Audits: SHANGRLA -- A Note on Risk-Limiting Bayesian Polling Audits for Two-Candidate Elections -- Vote selling resistant voting -- An Update on Marked Mix-Nets: An Attack, A Fix and PQ Possibilities -- Performance of Shuffling: Taking it to the Limits -- Characterizing Types of Smart Contracts in the Ethereum Landscape -- Smart Contract Development from the Perspective of Developers: Topics and Issues Discussed on Social Media -- Bypassing Non-Outsourceable Proof-of-Work Schemes Using Collateralized Smart Contracts -- Scalable Open-Vote Network on Ethereum -- How to Dynamically Incentivize Sufficient Level of IoT Securitx -- Confidential and auditable payments -- MAPPCN: Multi-hop Anonymous and Privacy-Preserving Payment Channel Network -- Marlowe: implementing and analysing financial contracts on blockchain -- Load Balancing for Sharded Blockchains -- The Extended UTXO Model -- Privacy-Preserving Cross-Chain Atomic Swaps -- A Blockchain Based Approach to Resource Sharing in Smart Neighbourhoods -- Enforcing Determinism of Java Smart Contracts -- Albert, an intermediate smart-contract language for the Tezos blockchain -- A Formally Verified Static Analysis Framework for Compositional Contracts.

Sommario/riassunto

This book constitutes the refereed proceedings of two workshops held at the 24th International Conference on Financial Cryptography and Data Security, FC 2020, in Kota Kinabalu, Malaysia, in February 2020. The 39 full papers and 3 short papers presented in this book were carefully reviewed and selected from 73 submissions. The papers feature four Workshops: The 1st Asian Workshop on Usable Security, AsiaUSEC 2020, the 1st Workshop on Coordination of Decentralized Finance, CoDeFi 2020, the 5th Workshop on Advances in Secure Electronic Voting, VOTING 2020, and the 4th Workshop on Trusted Smart Contracts, WTSC 2020. The AsiaUSEC Workshop contributes an increase of the scientific quality of research in human factors in security and privacy. In terms of improving efficacy of secure systems, the research included an extension of graphical password authentication. Further a comparative study of SpotBugs, SonarQube, Cryptoguard and CogniCrypt identified strengths in each and refined the need for improvements in security testing tools. The CoDeFi Workshop discuss multi-disciplinary issues regarding technologies and operations of decentralized finance based on permissionless blockchain. The workshop consists of two parts; presentations by all stakeholders, and unconference style discussions. The VOTING Workshop cover topics like new methods for risk-limited audits, new ethods to increase the efficiency of mixnets, verification of security of voting schemes election auditing, voting system efficiency, voting system usability, and new technical designs for cryptographic protocols

for voting systems, and new way of preventing voteselling by de-incentivising this via smart contracts. The WTSC Workshop focuses on smart contracts, i.e., self-enforcing agreements in the form of executable programs, and other decentralized applications that are deployed to and run on top of specialized blockchains.