1.	Record Nr.	UNISA996418218803316
Titolo	Financial Cryptography and Data Security [[electronic resource]] : FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers / / edited by Andrea Bracciali, Jeremy Clark, Federico Pintore, Peter B. Rønne, Massimiliano Sala
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-43725-6
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XIV, 347 p. 216 illus., 29 illus. in color.)
Collana	Security and Cryptology ; ; 11599
Disciplina	005.82
Soggetti	Data encryption (Computer science) Application software Architecture, Computer Database management Computer communication systems Cryptology Information Systems Applications (incl. Internet) Computer System Implementation Database Management Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Two-Party State Channels with State Assertions -- Secure Offline Payments in Bitcoin -- Proof-of-Work Sidechains -- You Sank my Battleship! A Case Study to Evaluate State Channels as a Scaling Solution for Cryptocurrencies -- Game-theoretic Analysis of an Incentivized Verifiable Computation System -- Sluggish Mining: Profiting from the Verier's Dilemma -- Deploying PayWord on Ethereum -- SoK: Development of Secure Smart Contracts - Lessons from a Graduate Course -- Verification-Led Smart Contracts -- A Java Framework for Smart Contracts -- Is Solidity solid enough -- Building Executable Secure Design Models for Smart Contracts with Formal

Methods -- SoK: Transparent Dishonesty: Front-running Attacks on Blockchain -- Trustee: Full Privacy Preserving Vickrey Auction on top of Ethereum -- Election Manipulation 100 -- A Manifest Improvement for Risk-Limiting Audits -- k-Cut: A Simple Approximately-Uniform Method for Sampling Ballots in Post-Election Audits -- How to Assess the Usability Metrics in E-Voting Schemes -- Improving the Performance of Cryptographic Voting Protocols (SoK) -- Short Paper: Coercion-Resistant Voting in Linear Time via Fully Homomorphic Encryption -- Priv-Apollo - Secret Ballot E2E-V Internet Voting -- End-to-End Verifiable Quadratic Voting with Everlasting Privacy -- Lattice-Based Proof of a Shuffle.

Sommario/riassunto

This book constitutes the refereed proceedings of two workshops held at the 23rd International Conference on Financial Cryptography and Data Security, FC 2019, in St. Kitts, St. Kitts and Nevis, in February 2019. The 20 full papers and 4 short papers presented in this book were carefully reviewed and selected from 34 submissions. The papers feature the outcome of the 4th Workshop on Advances in Secure Electronic Voting, VOTING 2019 and the Third Workshop on Trusted Smart Contracts, WTSC 2019. VOTING covered topics like election auditing, voting system efficiency, voting system usability, and new technical designs for cryptographic protocols for voting systems. WTSC 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. .