

1. Record Nr.	UNISA996542665503316
Autore	Matsuo Shin'ichiro
Titolo	Financial Cryptography and Data Security. FC 2022 International Workshops [[electronic resource]] : CoDecFin, DeFi, Voting, WTSC, Grenada, May 6, 2022, Revised Selected Papers // edited by Shin'ichiro Matsuo, Lewis Gudgeon, Aariah Klages-Mundt, Daniel Perez Hernandez, Sam Werner, Thomas Haines, Aleksander Essex, Andrea Bracciali, Massimiliano Sala
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	3-031-32415-3
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (704 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13412
Altri autori (Persone)	GudgeonLewis Klages-MundtAariah Perez HernandezDaniel WernerSam HainesThomas EssexAleksander BraccialiAndrea SalaMassimiliano
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	CoDecFin22 -- Stakechains: A Bitcoin-backed Proof-of-Stake -- Drivers of Bitcoin Energy Use and Emissions -- Integrated Power Plant and Bitcoin Mining Economics -- Carbon-neutral bitcoin adoption for nation states -- Soundness of Stablecoins -- Estimating (Miner) Extractable Value is Hard, Let's Go Shopping! -- Explaining Proof Of Work in a classroom -- The compatibility of CBDCs with "DeFi" protocols: a governance rather than a technological issue to comply with financial crime regulations -- Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges -- Privacy-Preserving

Post-Quantum Credentials for Digital Payments -- ZKFlow: Private Transactions in Corda with ZKP -- User-Perceived Privacy in Blockchain -- DeFi22 -- A Short Survey on Business Models of Decentralized Finance (DeFi) Protocols -- On-Chain Auctions with Deposits -- Beyond Staking: An Aphoristic design for Staking and Rewards -- The Case for Variable Fees in Constant Product Markets: An Agent Based Simulation -- An Empirical Study of Market Inefficiencies in Uniswap and SushiSwap -- SoK: Mitigation of Front-running in Decentralized Finance -- A Systematic Investigation of DeFi Compositions in Ethereum -- Privacy Preserving Decentralized Netting -- NFT Wash Trading: Quantifying suspicious behaviour in NFT markets -- Voting22 -- Individual Verifiability and Revoting in the Estonian Internet Voting System -- Breaking and Fixing Vote Privacy of the Estonian E-Voting Protocol IVXV -- German voters' attitudes towards voting online with a verifiable system -- Simulations of Ballot Polling Risk-Limiting Audits -- Simulations of Ballot Polling Risk-Limiting Audits -- Short Paper: Verifiable Decryption for BGV -- RemoteVote and SAFE Vote: Towards Usable End-to-End Verification for Vote-by-Mail -- WTSC 2022 -- (short summary: WTSC22 - Current and future trends) -- Spark: Secure and Flexible Private Transactions -- Fides: A System for Verifiable Computation Using Smart Contracts -- Towards Smart Contract-based Verification of Anonymous Credentials -- Dispute-free Scalable Open Vote Network using zk-SNARKs -- Not All Code are Create2 Equal -- Not so immutable: Upgradeability of Smart Contracts on Ethereum -- Protocol-based smart contract generation -- Distributed and Adversarial Resistant Workflow Execution on the Algorand Blockchain -- Experimenting with On-chain Order Books -- Experimenting with On-chain Order Books. -A Scalable Architecture for Electronic Payments -- UTS: the Universal Token Swapper.

Sommario/riassunto

This book constitutes revised selected papers from the workshops that were affiliated with the 26th International Conference on Financial Cryptography and Data Security, FC 2022, which was held in Grenada during May 2022. FC 2022 presents the following four workshops: CoDecFin 2022: 3rd Workshop on Coordination of Decentralized Finance DeFi 2022: 2nd Workshop on Decentralized Finance Voting 2022: 7th Workshop on Advances in Secure Electronic Voting WTSC 2022: 6th Workshop on Trusted Smart Contracts.
