1.	Record Nr.	UNISA996465331403316
	Titolo	Financial Cryptography and Data Security [[electronic resource]] : FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers / / edited by Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner, Kurt Rohloff
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
	ISBN	3-662-53357-X
	Edizione	[1st ed. 2016.]
	Descrizione fisica	1 online resource (XII, 343 p. 45 illus.)
	Collana	Security and Cryptology ; ; 9604
	Disciplina	005.82
	Soggetti	Computer security Data encryption (Computer science) E-commerce Application software Computers and civilization Management information systems Computer science Systems and Data Security Cryptology e-Commerce/e-business Computer Appl. in Administrative Data Processing Computers and Society Management of Computing and Information Systems
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Intro -- BITCOIN 2016: Third Workshop on Bitcoin and Blockchain Research -- VOTING 2016: First Workshop on Advances in Secure Electronic Voting Schemes -- WAHC 2016: 4th Workshop on Encrypted Computing and Applied Homomorphic Cryptography -- Contents -- Third Workshop on Bitcoin and Blockchain Research, BITCOIN 2016 -- Stressing Out: Bitcoin ``Stress Testing'' -- 1 Introduction -- 2

Background -- 2.1 DoS Targets Inherent in Bitcoin -- 3 Data Collection -- 4 Spam Clustering -- 4.1 Methodology -- 4.2 Results and Motifs -- 4.3 Validation -- 5 Impact on Bitcoin -- 6 Discussion -- 7 Related Work -- 8 Conclusion -- References -- Why Buy When You Can Rent? -- 1 Introduction -- 2 Renting Mining Capacity -- 2.1 Out-of-Band Payment -- 2.2 Negative-Fee Mining Pool -- 2.3 In-Band Payment via Forking -- 3 Bribery Attacks -- 3.1 Counter-Bribing by Miners -- 4 Analysis of Mitigating Factors -- 4.1 Miners May Be Too Simplistic to Recognize or Accept Bribes -- 4.2 The Attack Requires Significant Capital and Risk-Tolerance -- 4.3 Profit from Double-Spends May Not Be Frictionless or Boundless -- 4.4 Extra Confirmations for Large Transactions -- 4.5 Counter-Bribing by the Intended Victim -- 4.6 Miners May Refuse to Help an Attack Against Bitcoin -- 5 Concluding Remarks -- References -- Automated Verification of Electrum Wallet -- 1 Context -- 2 Electrum Wallet -- 3 Modeling BIP32 -- 4 ASLan++ Wallet Model -- 4.1 Attacker Model and Assumptions -- 4.2 Security Properties -- 4.3 User Role -- 4.4 Client Role -- 4.5 Server Registration Role -- 4.6 Server Confirmation Role -- 4.7 Server Signature Role -- 5 Results -- 5.1 Executability Checking -- 5.2 Attack by Confirmation Replay -- 5.3 Security Analysis -- 6 Conclusion -- References -- Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions -- 1 Introduction -- 1.1 Related Work. 2 Overview and Security Properties -- 2.1 Anonymity Properties -- 2.2 Security Properties -- 3 Implementing Fair Exchange via Scripts and Blind Signatures -- 4 On-Blockchain Anonymous Protocols -- 4.1 Anonymous Fee Vouchers -- 4.2 Anonymity Analysis -- 5 Off-Blockchain Anonymous Payments over Micropayment Channel Networks -- 5.1 Micropayment Channel Networks -- 5.2 Anonymizing Micropayment Channel Networks -- 5.3 Anonymity Analysis -- 6 Security Analysis -- 7 Conclusion -- References -- Proofs of Proofs of Work with Sublinear Complexity -- 1 Introduction -- 2 Preliminaries -- 3 Interconnected Blockchains -- 3.1 Description of the Interlink-Update Algorithm -- 4 Proving Proof of Work with Sublinear Complexity -- 4.1 Description of the Prover -- 4.2 Description of the Lite Verifier -- 5 Efficiency Analysis -- 5.1 Space Complexity -- 5.2 Communication and Time Complexity -- 6 Security Analysis -- References -- Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab -- 1 Introduction -- 2 Background -- 2.1 Background on Decentralized Cryptocurrencies -- 2.2 Background on Smart Contracts -- 2.3 A Taste of Smart Contract Design -- 3 A Recount of Our Smart Contract Programming Lab -- 4 Pitfalls of Smart Contract Programming -- 4.1 Errors in Encoding State Machines -- 4.2 Failing to Use Cryptography -- 4.3 Misaligned Incentives -- 4.4 Ethereum-Specific Mistakes -- 4.5 Complete, Fixed Contract -- 5 Conclusion -- 5.1 Open-Source Course and Lab Materials -- 5.2 Cryptocurrency and Smart Contracts as a Cybersecurity Pedagogical Platform -- 5.3 The ``Build, Break, and Amend Your Own Programs'' Approach to Cybersecurity Education -- 5.4 Subsequent Pedagogical Efforts and Research -- References -- EthIKS: Using Ethereum to Audit a CONIKS Key Transparency Log -- 1 Introduction -- 2 CONIKS Overview -- 3 Ethereum Overview.
4 EthIKS -- 5 Implementation and Costs -- 6 Concluding Discussion -- References -- On Scaling Decentralized Blockchains -- 1 Introduction -- 2 Bitcoin Scalability Today: A Reality Check -- 3 Scaling by Parameter Tuning and Fundamental Limits -- 3.1 Measurement Study -- 3.2 Limits of Scalability by Reparametrization -- 3.3 Bottleneck Analysis -- 4 Rethinking the Design of a Scalable Blockchain -- 4.1 Network Plane -- 4.2 Consensus Plane -- 4.3 Storage Plane --

4.4 View Plane -- 4.5 Side Plane -- 5 Conclusion -- A BFT Experiments (Consortium Consensus) -- B Use of SNARKs for Outsourcing View Computation -- References -- Bitcoin Covenants -- 1 Introduction -- 2 Preliminaries -- 3 Covenants -- 3.1 Basic Covenants -- 3.2 Recursive Covenants -- 3.3 Distinguished Coins -- 3.4 Overhead -- 3.5 Discussion -- 4 Vault Transactions -- 4.1 Overview -- 4.2 Architecture -- 4.3 Script Programs -- 5 Bitcoin-NG Overlay -- 5.1 Preliminaries: Bitcoin-NG Operation -- 5.2 Overlaying Bitcoin-NG on Top of Bitcoin -- 5.3 Poison Transactions -- 6 Related Work -- 7 Conclusions -- References -- Cryptocurrencies Without Proof of Work -- 1 Introduction -- 2 Pure Proof of Stake -- 2.1 The PPCoin System -- 2.2 The CoA Pure Proof of Stake System -- 2.3 The Dense-CoA Pure Proof of Stake Variant -- 3 Solidification of the Ledger History -- 4 Conclusion -- References -- First Workshop on Secure Voting Systems, VOTING 2016 -- Coercion-Resistant Internet Voting with Everlasting Privacy -- 1 Introduction -- 1.1 Related Work -- 1.2 Contribution -- 1.3 Paper Overview -- 2 Coercion-Resistant Internet Voting with Everlasting Privacy -- 2.1 Adversary Model and Trust Assumptions -- 2.2 Protocol Overview -- 2.3 Discussion of Coercion-Resistance -- 3 Detailed Cryptographic Protocol -- 3.1 Cryptographic Preliminaries -- 3.2 Protocol Description -- 3.3 Security Properties -- 4 Conclusion. References -- Selene: Voting with Transparent Verifiability and Coercion-Mitigation -- 1 Introduction -- 2 Background -- 3 Cryptographic Primitives -- 4 Related Work -- 5 The Set-Up Phase -- 5.1 Distributed Generation of the Tracker Number Commitments -- 5.2 Voting -- 5.3 Mixing and Decryption -- 5.4 Notification of Tracker Numbers -- 6 The Voter Experience -- 6.1 The Core Ceremony -- 6.2 The Ceremony in the Event of Coercion -- 6.3 Selene as an Add-On -- 7 Analysis -- 7.1 Verifiability and Verification -- 7.2 Ballot Privacy -- 7.3 Receipt-Freeness -- 7.4 Coercion: Threats and Mitigation -- 7.5 Dispute Resolution -- 8 Alternative Selene Scheme -- 9 Conclusions -- References -- On the Possibility of Non-interactive E-Voting in the Public-Key Setting -- 1 Introduction -- 1.1 Multiple Non-interactive Elections in the PK Setting -- 1.2 Relation to Secure Computation -- 1.3 Our Results in a Nutshell -- 2 Definitions -- 2.1 Non-interactive Voting Scheme in the PK Setting -- 2.2 Bilinear Maps -- 2.3 NIZK in the RO -- 3 NIVS for YES/NO Elections -- 3.1 Properties and Security of the Scheme -- 4 Future Directions -- References -- Efficiency Comparison of Various Approaches in E-Voting Protocols -- 1 Introduction -- 2 Methodology -- 2.1 Election Phases -- 2.2 Time Estimations -- 3 Individual Calculations -- 3.1 Mix Net -- 3.2 Homomorphic Tallying -- 3.3 Distributed Decryption -- 4 Prototype Evaluation Tool -- 4.1 Relevant Parameters -- 4.2 Software -- 5 Evaluation of Example Settings -- 5.1 Description of Example Settings -- 5.2 Results and Discussion -- 6 Conclusion -- References -- Remote Electronic Voting Can Be Efficient, Verifiable and Coercion-Resistant -- 1 Introduction -- 2 Preliminaries -- 2.1 Classical Tools -- 2.2 Algebraic MACs -- 2.3 Our Sequential Aggregate MAC Scheme -- 3 A MAC Based Coercion Resistant Voting Scheme.
3.1 An Overview of the Scheme -- 3.2 Our Novel Coercion-Resistant Voting Scheme -- 4 Conclusion -- References -- Universal Cast-as-Intended Verifiability -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Structure of the Paper -- 2 Electronic Voting Definitions -- 2.1 Syntactical Definition -- 2.2 Security Definitions -- 3 Building Blocks -- 4 Core Voting Protocol -- 4.1 Overview -- 4.2 2-cnf-Proof of Knowledge -- 4.3 Detailed Protocol -- 5 Security of the Protocol -- 6 A Possible Instantiation -- 7 Towards Designing Usable UCIV Systems -- 8 Future Work -- References -- 4th Workshop on

Encrypted Computing and Applied Homomorphic Cryptography, WAHC 2016 -- Hiding Access Patterns in Range Queries Using Private Information Retrieval and ORAM -- 1 Introduction -- 2 Background -- 2.1 Privacy Preserving Range Queries Using Bucketization -- 2.2 Lipmaa's BddCPIR Protocol for PIR -- 2.3 Path ORAM -- 3 Privacy Preserving Range Query Using PIR and ORAM -- 3.1 CPIR for Privacy Preserving Range Queries -- 3.2 Path ORAM for Privacy Preserving Range Queries -- 4 Analysis of Security in Privacy Preserving Range Queries -- 4.1 Security Analysis of CPIR -- 4.2 Security Analysis of Path ORAM -- 5 A Quantitative Analysis of Path ORAM and CPIR -- 5.1 Communication Complexity Analysis -- 5.2 Computational Complexity Analysis -- 6 Experiments -- 6.1 Single-Node Experiments -- 6.2 Multi-node Experiments -- 7 Conclusion -- References -- Optimizing MPC for Robust and Scalable Integer and Floating-Point Arithmetic -- 1 Introduction -- 2 Background -- 3 Improvements in Protocol Design -- 3.1 Efficient Polynomial Evaluation -- 3.2 Additional Improvements to Floating-Point Protocols -- 3.3 New Floating-Point Protocols -- 4 Optimization Techniques -- 4.1 Shared Random Number Generators -- 4.2 Symmetric Protocols -- 4.3 Speedup over Previous Results. 5 Large-Scale Performance Evaluation.

Sommario/riassunto

This book constitutes the refereed proceedings of three workshops held at the 20th International Conference on Financial Cryptography and Data Security, FC 2016, in Christ Church, Barbados, in February 2016. The 22 full papers presented were carefully reviewed and selected from 49 submissions. They feature the outcome of the Second Workshop on Bitcoin and Blockchain Research, BITCOIN 2016, the First Workshop on Secure Voting Systems, VOTING 2016, and the 4th Workshop on Encrypted Computing and Applied Homomorphic Cryptography, WAHC 2016.