1. Record Nr. UNISA996464531903316

Titolo	Financial cryptography and data security : 25th International Conference, FC 2021, Virtual event, March 1-5, 2021, Revised selected papers. Part II / / edited by Nikita Borisov and Claudia Diaz
Pubbl/distr/stampa	Berlin, Germany : , : Springer, , [2021] ©2021
ISBN	3-662-64331-6
Descrizione fisica	1 online resource (611 pages)
Collana	Lecture Notes in Computer Science ; ; v.12675
Disciplina	005.824
Soggetti	Data encryption (Computer science) User-centered system design Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part II -- Contents - Part I -- Blockchain Protocols -- SoK: Communication Across Distributed Ledgers -- 1 Introduction -- 2 The Cross-Chain Communication Problem -- 2.1 Historical Background: Distributed Databases -- 2.2 Distributed Ledger Model -- 2.3 Cross-Chain Communication System Model -- 2.4 Formalization of Correct Cross-Chain Communication -- 2.5 The Generic CCC Protocol -- 3 Impossibility of CCC Without a Trusted Third Party -- 3.1 What Is a Trusted Third Party? -- 3.2 Relating CCC to Fair Exchange -- 3.3 Incentives and Rational CCC -- 4 The CCC Design Framework -- 4.1 (Pre-)Commit Phase -- 4.2 Verification Phase -- 4.3 Abort Phase -- 5 Classification of Existing CCC Protocols -- 5.1 Exchange Protocols -- 5.2 Migration Protocols -- 5.3 Insights and General Observations -- 6 CCC Challenges and Outlook -- 6.1 Heterogeneous Models and Parameters Across Chains -- 6.2 Heterogeneous Cryptographic Primitives Across Chains -- 6.3 Collateralization and Exchange Rates -- 6.4 Lack of Formal Security Analysis -- 6.5 Lack of Formal Privacy Analysis -- 6.6 Upcoming Industrial and Research CCC Trends -- 7 Concluding Remarks -- A Fair Exchange Using CCC -- References -- Reparo: Publicly Verifiable Layer to Repair Blockchains -- 1 Introduction

-- 1.1 Existing Solutions and Their Limitations -- 1.2 Our Contributions -- 2 A Primer on Ethereum -- 2.1 Ethereum Ledger -- 3 Repairability in Ethereum -- 3.1 Repairing Ethereum Using Reparo -- 3.2 Discussion -- 4 Experiments in Ethereum -- 4.1 Special Transactions: repairTx, voteTx -- 4.2 Performing Repairs -- 5 Conclusion and Future Work -- A Prominent Bugs -- References -- Short Paper: Debt Representation in UTXO Blockchains -- 1 Introduction -- 2 Transactions in the UTXO Model -- 3 Debt-Enabling UTXO Blockchain -- 3.1 Debt Transactions.
3.2 Outstanding Debt Transactions and Debt Pools -- 4 Prototype -- 4.1 System Architecture -- 4.2 Implementation -- 5 Conclusion -- References -- Instant Block Confirmation in the Sleepy Model -- 1 Introduction -- 2 Technical Roadmap -- 2.1 Starting Point: Algorand -- 2.2 Selecting a Committee -- 2.3 Consensus with Different Committees -- 2.4 Summary of Challenges and Theorem Statement -- 3 Related Work -- 3.1 Comparison of Confirmation Times and Communication Complexity -- 4 Definitions -- 4.1 Blockchain Execution Model -- 4.2 Tools -- 4.3 Other Notation -- 5 The Blockchain Protocol -- 5.1 Committee Selection -- 5.2 Binary Byzantine Agreement -- 5.3 Block Proposal -- 5.4 Putting It All Together -- References -- Blockchain CAP Theorem Allows User-Dependent Adaptivity and Finality -- 1 Introduction -- 1.1 Our Contributions -- 2 Related Work -- 3 Security Model -- 4 Protocol Description -- 5 Main Result -- 6 Conclusion -- A Algorand BA is a Checkpointing Protocol -- References -- PoSAT: Proof-of-Work Availability and Unpredictability, Without the Work -- 1 Introduction -- 1.1 Dynamic Availability -- 1.2 Static vs Dynamic Adversary -- 1.3 PoSAT Achieves PoW Dynamic Availability -- 1.4 PoSAT Has PoW Unpredictability -- 1.5 Related Work -- 1.6 Outline -- 2 Protocol -- 2.1 Primitives -- 2.2 Protocol Description -- 3 Model -- 4 Security Analysis -- 4.1 Main Security Result -- 4.2 Step 1: Mining Lag of Newly Joined Nodes -- 4.3 Step 2: Simulating a Static System -- 4.4 Step 3: Upgrading the Adversary -- 4.5 Step 4: Growth Rate of the Adversarial Tree -- 4.6 Step 5: Existence of Nakamoto Blocks -- 4.7 Step 6: Putting Back All Together -- 5 Discussion -- References -- Payment Channels -- Post-Quantum Adaptor Signature for Privacy-Preserving Off-Chain Payments -- 1 Introduction -- 2 Preliminaries -- 2.1 Adaptor Signatures (AS).
2.2 Elliptic Curves and Isogenies -- 2.3 Security Assumptions: GAIP and MT-GAIP -- 3 CSI-FiSh -- 3.1 Zero-Knowledge Proof for Group Actions -- 4 IAS: An Adaptor Signature from Isogenies -- 4.1 Our Construction -- 5 Performance Evaluation -- 5.1 Evaluation Results -- 5.2 Comparison with LAS -- 6 Building Payment-Channel Networks from IAS -- 7 Conclusion -- References -- FPPW: A Fair and Privacy Preserving Watchtower for Bitcoin -- 1 Introduction -- 1.1 Our Contribution -- 2 Preliminaries and Notations -- 2.1 Preliminaries -- 2.2 Notations -- 3 FPPW Overview -- 3.1 System Model -- 3.2 FPPW Overview -- 3.3 Watchtower Service Properties -- 4 FPPW Channel -- 4.1 FPPW Channel Establishment -- 4.2 FPPW Channel Update -- 4.3 FPPW Channel Closure -- 4.4 FPPW Watchtower Abort -- 5 Security Analysis -- 6 Fee Handling -- References -- Congestion Attacks in Payment Channel Networks -- 1 Introduction -- 2 Background on the Lightning Network -- 3 Lightning Network Analysis -- 3.1 Default Parameter Values -- 3.2 Network Statistics -- 4 Attacking the Entire Network -- 4.1 Evaluation -- 5 Attacking Hubs - Attack on a Single Node -- 5.1 Evaluation -- 6 Mitigation Techniques -- 7 Related Work -- 8 Conclusions and Future Work -- References -- Payment Trees: Low Collateral Payments for Payment Channel Networks -- 1 Introduction -- 2 Background -- 3 The Channel Closure Attack on

AMCU -- 4 Protocol Overview -- 5 Transactions -- 6 Our Payment Tree Construction -- 7 Collateral Efficiency and Security Analysis -- 8 Conclusion -- References -- Brick: Asynchronous Incentive-Compatible Payment Channels -- 1 Introduction -- 2 Protocol Overview -- 2.1 System Model -- 2.2 Brick Overview -- 2.3 Reward Allocation and Collateral -- 2.4 Protocol Goals -- 3 Brick Design -- 3.1 Architecture -- 3.2 Incentivizing Honest Behavior -- 4 Brick Analysis -- 5 Evaluation of Brick -- 6 Related Work.
7 Conclusion, Limitations and Extensions -- References -- Mining -- Ignore the Extra Zeroes: Variance-Optimal Mining Pools -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Model of Miners -- 2.2 Reward Sharing Schemes -- 2.3 Message-Independence and Symmetrization -- 2.4 A Reward-Sharing Scheme as a Hashrate Estimator -- 2.5 When t is Random -- 3 Warm-Up: Maximizing Likelihood -- 4 Main Results: Variance-Optimality -- 4.1 Single-Class Shares Are Optimal -- 4.2 PPS is Variance-Optimal -- 4.3 Variance-Optimality of PPLNS -- 4.4 Relaxing the Constraints -- 5 Conclusions and Discussion -- References -- HaPPY-Mine: Designing a Mining Reward Function -- 1 Introduction -- 1.1 Main Contributions -- 2 Background -- 3 Hashrate-Pegged Block Reward -- 4 HaPPY-Mine Equilibrium Analysis -- 4.1 Examples with Diverse Cost Scenarios -- 4.2 General Analysis of HaPPY-Mine -- 5 Impact of Attacks and Currency on Equilibria -- 6 Discussion -- 7 Related Work -- References -- Selfish Mining Attacks Exacerbated by Elastic Hash Supply -- 1 Introduction -- 2 Empirical Findings -- 3 Model with Elastic Hash Supply -- References -- Scaling Blockchains -- Fraud and Data Availability Proofs: Detecting Invalid Blocks in Light Clients -- 1 Introduction and Motivation -- 2 Background -- 3 Assumptions and Threat Model -- 3.1 Blockchain Model -- 3.2 Participants and Threat Model -- 4 Fraud Proofs -- 4.1 State Root and Execution Trace Construction -- 4.2 Data Root and Periods -- 4.3 Proof of Invalid State Transition -- 5 Data Availability Proofs -- 5.1 2D Reed-Solomon Encoded Merkle Tree Construction -- 5.2 Random Sampling and Network Block Recovery -- 5.3 Fraud Proofs of Incorrectly Generated Extended Data -- 5.4 Security Probability Analysis -- 6 Performance and Implementation. -- 7 Related Work -- 7.1 SParse FrAud pRotection (SPAR).
8 Conclusion -- References -- ACeD: Scalable Data Availability Oracle -- 1 Introduction -- 2 System and Security Model -- 2.1 Network Model and Assumptions -- 2.2 Oracle Model -- 3 Technical Description of ACeD -- 3.1 Coded Interleaving Tree -- 3.2 Dispersal Protocol -- 3.3 Retrieval Protocol and Block Decoding -- 3.4 Protocol Summary -- 4 Performance Guarantees of ACeD -- 4.1 Security -- 4.2 Efficiency -- 5 Algorithm to System Design and Implementation -- 6 Evaluation -- 7 Conclusion and Discussion -- References -- Efficient State Management in Distributed Ledgers -- 1 Introduction -- 2 A UTxO Model -- 3 Transaction Optimization -- 3.1 Transaction Logical Operators - Ledger State Algebra -- 3.2 A Transaction Optimization Framework -- 3.3 Transaction Optimization Techniques -- 3.4 The Transaction Optimization Problem -- 4 State Efficiency in Bitcoin -- 4.1 A State Efficient Bitcoin -- 5 Conclusion -- References -- Fast Isomorphic State Channels -- 1 Introduction -- 2 Preliminaries -- 3 The Hydra Protocol -- 3.1 Protocol Setup -- 3.2 Mainchain (Simplified) -- 3.3 Head (Simplified) -- 3.4 Extensions for the Full Protocol -- 4 Experimental Evaluation -- 4.1 Applying the Methodology -- 4.2 Experimental Results -- 4.3 Larger Clusters -- 4.4 Discussion -- References -- Authentication and Usability -- What's in Score for Website Users: A Data-Driven Long-Term Study on Risk-Based

Authentication Characteristics -- 1 Introduction -- 2 RBA Models -- 3 Data Set -- 4 Attacker Models -- 5 Evaluating RBA Practice (RQ1) -- 5.1 Results -- 5.2 Discussion -- 6 Analyzing RBA Features (RQ2) -- 6.1 Study Setup -- 6.2 Results -- 6.3 Discussion -- 7 Analyzing RBA Configuations (RQ3) -- 8 Limitations -- 9 Related Work -- 10 Conclusion -- A Survey -- A.1 Online Service -- A.2 Demographics -- B Features -- References.

DAHash: Distribution Aware Tuning of Password Hashing Costs.