Academic Papers I Slowly Working My Way Through These

I will be printing out each paper, reading and annotating it. At which point I will scan the paper (so long as it's not too long) and will upload it to the repo under **'examined_papers'**.

1. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol
2. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake protocol
3. Stake-Bleeding Attacks on Proof-of-Stake Blockchains
4. TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake
5. Formal specification for a Cardano wallet
6. Self-Reproducing Coins as Universal Turing Machine
7. Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability
8. Ouroboros-BFT: A Simple Byzantine Fault Tolerant Consensus Protocol
9. Comparison of Block Expectation Time for Various Consensus Algorithms
10. Marlowe: financial contracts on blockchain
11. A Formal Treatment of Hardware Wallets
12. Proof-of-Work Sidechains
13. The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment
14. SoK: A Taxonomy for Layer-2 Scalability Related Protocols for Cryptocurrencies
15. Functional Blockchain Contracts
16. Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake
17. Proof-of-Stake Sidechains
18. System F in Agda, for fun and profit
19. Unraveling recursion: compiling an IR with recursion to System F
20. A Type and Scope Safe Universe of Syntaxes with Binding: Their Semantics and Proofs
21. Proof-of-Stake Blockchain Protocols with Near-Optimal Throughput
22. The Combinatorics of the Longest-Chain Rule: Linear Consistency for Proof-of-Stake Blockchains
23. Bypassing Non-Outsourceable Proof-of-Work Schemes Using Collateralized Smart Contracts
24. Marlowe: implementing and analysing financial contracts on blockchain
25. Non-Interactive Proofs of Proof-of-Work
26. One-shot Signatures and Applications to Hybrid Quantum/Classical Authentication
27. Proof-of-Burn
28. Stake Shift in Major Cryptocurrencies: An Empirical Study
29. The Extended UTXO Model

30. Full Analysis of Nakamoto Consensus in Bounded-Delay Networks
31. SoK: A Taxonomy of Cryptocurrency Wallets
32. Smart Contract Derivatives
33. Consensus Redux: Distributed Ledgers in the Face of Adversarial Supremacy
34. Introduction to the design of the Data Diffusion and Networking for Cardano Shelley
35. The Architecture of Decentralised Finance Platforms: A New Open Finance Paradigm
36. Account Management in Proof of Stake Ledgers
37. Reward Sharing Schemes for Stake Pools
38. Updatable Blockchains
39. Upper Bound Probability of Double Spend Attack on SPECTRE
40. A Gas-Efficient Superlight Bitcoin Client in Solidity
41. Native Custom Tokens in the Extended UTXO Model
42. Models of distributed proof generation for ZK-SNARK-based blockchains
43. Efficient static analysis of Marlowe contracts
44. Timed Signatures and Zero-Knowledge Proofs –Timestamping in the Blockchain Era–
45. UTxO- vs account-based smart contract blockchain programming paradigms
46. UTXOma:UTXO with Multi-Asset Support
47. Blockchains from Non-Idealized Hash Functions
48. Consistency of Proof-of-Stake Blockchains with Concurrent Honest Slot Leaders
49. Ledger Combiners for Fast Settlement
50. Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains
51. Security Limitations of Classical-Client Delegated Quantum Computing
52. Efficient State Management in Distributed Ledgers
53. Hydra: Fast Isomorphic State Channels
54. Pay To Win: Cheap, Crowdfundable, Cross-chain Algorithmic Incentive Manipulation Attacks on PoW Cryptocurrencies
55. Post-Quantum Security of the Bitcoin Backbone and Quantum Multi-Solution Bernoulli Search
56. SoK: Algorithmic Incentive Manipulation Attacks on Permissionless PoW Cryptocurrencies
57. SoK: Communication Across Distributed Ledgers
58. Standardized crypto-loans on the Cardano blockchain
59. Cardano Disaster Recovery Plan
60. How to Prove Work: With Time or Memory (Extended Abstract)
61. Mining in Logarithmic Space
62. Securing Proof-of-Work Ledgers via Checkpointing
63. Consistency for Functional Encryption
64. Kachina - Foundations of Private Smart Contracts
65. Mithril: Stake-based Threshold Multisignatures
66. Probability of double spend attack for network with non-zero synchronization time
67. Conclave: A Collective Stake Pool Protocol