Contents

1. Introduction **1**
- 1.1. Gambling . . . 1
- 1.2. Cryptocurrency . . . 2
- 1.3. Gambling using cryptocurrencies . . . 3
- 1.4. Objectives . . . 3
  - 1.4.1. Specific objectives . . . 4
- 1.5. Methodology . . . 4
- 1.6. The proposed protocol . . . 4
  - 1.6.1. Oracle Selection . . . 5
  - 1.6.2. Bet Resolution . . . 5

2. Preliminaries **6**
- 2.1. Hash functions . . . 6
- 2.2. Cryptographic hash function . . . 6
- 2.3. Digital Signatures . . . 7
- 2.4. Ecash . . . 8
- 2.5. Bitcoin . . . 9
  - 2.5.1. Transactions . . . 9
  - 2.5.2. Blockchain . . . 10
  - 2.5.3. Script . . . 13
- 2.6. Previous work . . . 15
  - 2.6.1. Distributed oracles: Orisi . . . 16
  - 2.6.2. Trustless distributed casino: Winsome.io . . . 16
  - 2.6.3. Secure data feeds . . . 16

3. The Protocol **18**
- 3.1. Overview . . . 18
  - 3.1.1. First part: Oracle selection . . . 18
  - 3.1.2. Second part: The Bet . . . 19
- 3.2. Oracles . . . 19
- 3.3. Players . . . 20
- 3.4. Protocol Description . . . 20
  - 3.4.1. Notation . . . 20
  - 3.4.2. First part: Oracle Selection . . . 21
  - 3.4.3. Second part: The bet . . . 24
- 3.5. Cost analysis . . . 29

3.5.1. Concrete costs . . . 32
3.6. Communication . . . 33
3.6.1. Secure communication . . . 33
3.6.2. Channel . . . 34
3.7. Implementation . . . 34

4. Discussion **36**
4.1. Incentives . . . 36
4.1.1. Players . . . 36
4.1.2. Oracles . . . 37
4.2. Costs . . . 37
4.2.1. Attacks . . . 38
4.3. Limitations . . . 40
4.3.1. Number of participants . . . 40
4.3.2. Bet prize . . . 40
4.4. Extensions . . . 40
4.5. Comparison with Existing Solutions . . . 41
4.6. Future work . . . 42
4.6.1. Protocol extension . . . 42
4.6.2. Oracle reutilization . . . 43

5. Conclusion **44**

6. Bibliography **47**

7. Appendix **50**
7.1. Transactions . . . 50
7.1.1. Oracle registration . . . 50
7.1.2. Bet promise . . . 51
7.1.3. Oracle enrollment . . . 55
7.1.4. Bet . . . 58
7.1.5. Oracle answer . . . 66
7.1.6. Winner prize collect . . . 68
7.2. Bitcoin scripting . . . 77

List of Tables

2.1. Script evaluation to check a P2PKH transaction. 14
2.2. Script evaluation of a P2SH transaction. 15

3.1. Transaction notation example. 20
3.2. Oracle Registration. 22
3.3. Bet Promise 24
3.4. Oracle Enrollment 25
3.5. Bet 27
3.6. Timeouts 28
3.7. Transactions size and fee. 30
3.8. Successful run, costs for the players 31
3.9. Successful run, oracle cost and earning 31

4.1. Oracle exits after Oracle Enrollment 38

List of Figures

2.1. Simplified Transaction 10
2.2. Blocks linked to each other in the blockchain. 11
2.3. Block Structure 12
2.4. A fork in the blockchain. 12
2.5. Wire format of an Input. 13
2.6. Wire format of an Output 13