King’s College London

Online Examination Answer Sheet

**ACADEMIC HONESTY AND INTEGRITY STATEMENT**

Students at King’s are part of an academic community that values trust, fairness and respect and actively encourages students to act with honesty and integrity. It is a College policy that students take responsibility for their work and comply with the university’s standards and requirements.

Online proctoring/invigilation will not be used for our online assessments. By submitting their answers students will be confirming that the work submitted is completely their own.

Misconduct regulations remain in place during this period and students can familiarise themselves with the procedures on [the College website](https://www.kcl.ac.uk/campuslife/acservices/academic-regulations/assets-19-20/g27.pdf)

|  |  |
| --- | --- |
| *I agree to abide by the expectations as to my conduct, as described in the academic honesty and integrity statement.* | |
| **Signed:** | Ricky |

|  |  |
| --- | --- |
| **Student number:** | K1234567 |

|  |  |
| --- | --- |
| **Question Number: 1** | **Part:** |
| **Answer:**   1. **Distributed system:** each node could maintain a copy of all transactions to construct a decentralized ledger. **Asymmetric encryption:** create anonymous payment. **Hash function:** to combine transactions and chain the blocks 2. A batch of transactions are packed into a block, and blocks are linked by a hash chain 3. **Proof-of-work consensus protocol:** nodes compete by solving hard mathematical problems. The first node finding the correct answer win the right to pack transactions into a block and get all reward. 4. **Miners** are nodes to verify transactions and pack them into blocks. 5. **Proof-of-work** is essentially one-CPU-one-vote, so nodes spend computational power to propose blocks. One that wish to control the blockchain would theoretically require 51% of total computational power, where it become uneconomic because in this case the best strategy is to be honest. | |
| **Question Number: 2** | **Part:** |
| **Answer:**   1. Money is whatever people accept in payment; Money is whatever the Government says it is 2. a medium of exchange; a common measure of value and a unit of account; a store of value; a means of anonymous payments; a means of deferred payments 3. except a means of anonymous payments 4. Bitcoin is decentralized, meaning that no central authority can take charge of it. 5. A limit of number for a currency to be issued eliminate the possibility of inflation, yet it must casue deflation. | |

|  |  |
| --- | --- |
| **Question Number: 3** | **Part:** |
| **Answer:**   1. Consensus protocol is a set of rules for nodes in distributed ledger to reach agreement on the value of transactions. A fundamental problem in distributed systems is to achieve overall system reliability in the presence of a number of faulty/malicious nodes. Consensus protocols could be used to tackle this problem. 2. **Proof-of-work:** nodes compete by solving hard mathematical problems. The first node finding the correct answer win the right to pack transactions into a block and get all reward. **Proof-of-stake:** nodes deposit financial stake to get right to propose blocks that could be appended to the chain, and get paid in proportion to the amount of stake they hold. Dishonest nodes would forfeit their stake. **Proof-of-authority:** nodes with authority are chosen to propose blocks. Authority might be assigned randomly, or according to some rules. 3. I would recommend Proof-of-authority. Number of participants in a permissioned system should be relatively low. PoW would cost a huge amount of energy and computational power, and PoS is relatively unfair because the richer are more likely to be chosen and get more reward. PoA could avoid those drawbacks, also easy to implement, and thus suitable for commercial permissioned system. | |
| **Question Number: 4** | **Part:** |
| **Answer:**   1. I would recommend permissioned system, because it would give more security than public system. Also, it would be more easy to implement and maintain with only related stakeholders. 2. R3 Corda is an enterprise-level blockchain platform in various domains, including energy. 3. I suggest Ethereum, which is the largest DLT platform nowadays. Also Corda, and Hyperledger, which are designed and supported by big business. 4. Platforms and tools are still immature; Current DLT are hard to scale; It would be troublesome to integrate with legacy systems; Creating user-friendly interface are not trivial; Difficult to come up with appropriate design that fits security, compliance & monitoring requirements, analytics capabilities. | |