Diploma Programme
Programme du diplôme
Programa del Diploma

Markscheme

November 2020

Computer science

Higher level

Paper 3

7 pages

Computer science HL paper 3 markscheme

Mark allocation

Candidates are required to answer **all** questions. Total 30 marks.

General

A markscheme often has more specific points worthy of a mark than the total allows. This is intentional. Do not award more than the maximum marks allowed for that part of a question.

When deciding upon alternative answers by candidates to those given in the markscheme, consider the following points:

- Each statement worth one point has a separate line and the end is signified by means of a semi-colon (;).
- An alternative answer or wording is indicated in the markscheme by a "/"; either wording can be accepted.
- Words in (…) in the markscheme are not necessary to gain the mark.
- If the candidate's answer has the same meaning or can be clearly interpreted as being the same as that in the markscheme then award the mark.
- Mark positively. Give candidates credit for what they have achieved and for what they have got correct, rather than penalizing them for what they have not achieved or what they have got wrong.
- Remember that many candidates are writing in a second language; be forgiving of minor linguistic slips. In this subject effective communication is more important than grammatical accuracy.
- Occasionally, a part of a question may require a calculation whose answer is required for subsequent parts. If an error is made in the first part then it should be penalized. However, if the incorrect answer is used correctly in subsequent parts then **follow through** marks should be awarded. Indicate this with "**FT**".
- Question 4 is marked against markbands. The markbands represent a single holistic criterion applied to the piece of work. Each markband level descriptor corresponds to a number of marks. When assessing with markbands, a "best fit" approach is used, with markers making a judgment about which particular mark to award from the possible range for each level descriptor, according to how well the candidate's work fits that descriptor.

General guidance

Issue	Guidance
Answering more than the quantity of responses prescribed in the questions	● In the case of an "identify" question read all answers and mark positively up to the maximum marks. Disregard incorrect answers. ● In the case of a "describe" question, which asks for a certain number of facts *eg* "describe two kinds", mark the first two correct answers. This could include two descriptions, one description and one identification, or two identifications. ● In the case of an "explain" question, which asks for a specified number of explanations *eg* "explain two reasons …", mark the first two correct answers. This could include two full explanations, one explanation, one partial explanation *etc*.

1. (a) *Award **[2 max]**.*
Many clients connect directly to many other clients;
Clients also act as servers;
No centralized administration for the network/decentralized network;
Network is more resilient to failure;
Is more scalable than a client server network;
There are no "bottlenecks" as with Client Server model; **[2]**

***Note:** Do not accept "widely used for illegal file sharing" (or similar).*

(b) *Award **[2 max]**.*
Answers may include:

atmospheric noise;
radioactivity;
thermodynamics;
Brownian motion of particles;
mouse movements;
algorithmic sources;

***Note:** Do not accept "Entropy can be obtained from physical sources" as this is clearly stated in the case study. A physical source must be stated (eg radioactivity) to get that mark*.

2. (a) *Award **[4 max]**.*
Balances are not stored in the blockchain/calculated in real time;
A digital signature/hash address is used to identify the user;
An algorithm must go through the entire blockchain examining all transactions that match the signature/address;
Relevant transactions debits and credits are added to calculate the balance;
Third party services are available to monitor the blockchain and provide a balance for the specified addresses;
It is likely that the wallet (app) will regularly compute the balance by verifying all the MONS it contains, but to do a complete confirmation could take a long time (*eg* 10–60 mins on bitcoin); **[4]**

(b) *Award **[4 max]**.*
Proof of work delays the creation of new blocks and therefore avoid spamming and/or instant re-writing of the blockchain;
A certain amount of time is required to make sure that there are not too many blocks mined;
If mining takes much longer than 10 minutes, it may discourage miners from mining
If mining takes much longer than 10 minutes it may make cryptocurrency transactions too slow;
Miners are required by the network so therefore a balance must be found which takes miners with standard hardware the correct time to solve;
Complexity of the PoW (and therefore time required) can be altered by changing the nonce value used to create a valid hash;
Difficulty of PoW can be adjusted so that miners take that time to create blocks;
if the number of miners rises too much so the time drops, the reward can be decreased to try to reduce the attractiveness of mining;
Many cryptocurrencies (*eg* Bitcoin) modify the difficulty of their PoW to attract miners while maintaining the minimum time for a candidate block hash to be generated;
[4]

***Note:** Do not accept "adding more (powerful) GPUs", as this will simply increase the chance of a particular miner solving the proof of work first, not the difficulty of the task for all miners.*

3. *Award **[6 max]**.*

Negative impacts on the environment:

Miners which work on the network require energy to process proof of works;
Farms of miners will need energy for cooling systems such as AC, which have negative environmental results (e.g. greenhouse gases);
The use of computers to maintain the network may result in e-waste, which would be detrimental to the environment;
The mining of raw materials for electronic products (e.g. silicon, aluminum, copper, lead, and gold) can damage natural habitats for animals/pollutes water;

Positive/Mitigating factors:

Renewable energy may be used (solar energy is used by Bitcoin Miners now)
Low power specific computational devices (ASICS) are now widely used which reduces power consumption;
As miners aim to make a profit, they will always use the cheapest source of energy and therefore prefer solar *etc*;
A moving towards a proof of stake rather than a proof of work would reduce the amount of processing required, therefore reducing cost and environmental damage;
Moving away from physical currency would reduce cotton/paper/plastic production;
The new computing machinery would replace the older physical technology (banks, counting machines, printing, *etc*); **[6]**

4. *Award **[12 max]**.*
Answers may include:

Security features

All transactions are recorded into files called blocks.
Each block contains a hash of the previous block as well as some transactions.
Every transaction is visible to everyone, which makes it difficult to change existing data which may be replicated on thousands of computers (decentralisation).
Any change to any historic transaction would be noticeable because the hashes of all subsequent blocks would not agree.
Transactions are confirmed many times (consensus control).
The more users of MONS there are, the more likely that there will be additional miners, which will increase the security of the network.
A proof of work is required when creating a new block, which makes the effort required to falsify many blocks unfeasible.
Each user has his own private key which is unknown to anyone else, as well as a public key (cryptography).
With no central authority there is no focus point for hackers to attack.
As MONS uses a private blockchain then only verified and approved computers could mine.
The larger and more distributed the network is, the safer it is considered to be.

Security concerns

Ledgers are technically not immutable (but to do so would require unfeasible computing power and taking over >51% of the network within the space of 10 minutes (ie a 51% attack).
The 51% attack is more likely to be successful on a small private blockchain rather than a large public one.
Attacks on cryptocurrencies have been documented (reference opportunities).
These attacks related to access to wallets (obtaining private keys).
Currency transfer websites are a target and have been hacked with cryptocurrencies stolen.
With no central control it is difficult to rollback transactions.
DDoS attacks on cryptocurrency services may slow transactions slightly/may affect MONS value.
Future concerns have been expressed about the scalability of the blockchain, lack of standards, and how it can be used if laws on data privacy become tighter.

[12]

Marks	Level descriptor
No marks	• No knowledge or understanding of the relevant issues and concepts. • No use of appropriate terminology.
Basic 1–3 marks	• Minimal knowledge and understanding of the relevant issues or concepts. • Minimal use of appropriate terminology. • The answer may be little more than a list. • No reference is made to the information in the case study or independent research.
Adequate 4–6 marks	• A descriptive response with limited knowledge and/or understanding of the relevant issues or concepts. • A limited use of appropriate terminology. • There is limited evidence of analysis. • There is evidence that limited research has been undertaken.
Competent 7–9 marks	• A response with knowledge and understanding of the related issues and/or concepts. • A response that uses terminology appropriately in places. • There is some evidence of analysis. • There is evidence that research has been undertaken.
Proficient 10–12 marks	• A response with detailed knowledge and clear understanding of computer science. • A response that uses terminology appropriately throughout. • There is competent and balanced analysis. • Conclusions are drawn that are linked to the analysis. • There is clear evidence that extensive research has been undertaken.