M21/4/COMSC/HP3/ENG/TZ0/XX/M

Markscheme

May 2021

Computer science

Higher level

Paper 3

10 pages

Subject details: **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]***

Anonymity (signature key identifies the user but not their real name).
Asymmetric (cryptography);
Certificate authority stamp;
Collision resistant;
Data / transaction / message;
Deterministic;
Hash / bitstring;
Non-invertibility;
Non-repudiation;
Private key / Secret key
Public key / key generation;
Randomness (for Private key generation);
Secure / encryption;
Signature function / signing algorithm;
Timestamp (sometimes);
Unique.

[2]

(b) Award ***[2 Max]***

Candidate block is formed from transactions in the pool
Nonce is generated (based on difficulty level);
Miners try to find the nonce / Hash generated and compared to target / mathematical calculations / solving the problem;
Puzzle solved / Hash smaller than target;
Broadcast to distributed ledgers;
Other miners verify/validate;
Block added;
Reward is issued to successful miner;

[2]

2. (a) Award ***[4 Max]***

A transaction is hashed and added (as a leaf node);
A pair of leaf nodes are combined (hashed) to form the hash of a parent;
When the number of nodes on the same level is odd the rightmost node is copied to the parent (For example, 10, 5, 3, 2, 1);
This is repeated (recursively) until the Merkle root node is created;
The root node hash is created to represent all of the hashes of the nodes;

Award marks for a diagram that shows the steps.

[4]

(b) Award ***[4 Max]***
Award **[2 max]** for a Governance technology concern with example and a further **[2 max]** for expansion and consequence.

Technology example answer 1 [4 marks]
Concerns that there is no way to correct errors;
A transaction sent to the wrong person;
Relies on the receiver's honesty to return the funds;
But difficult to identify the receiver from their signature;

Technology example answer 2 [4 marks]
Residences may be concerned that errors or mistakes won't be corrected;
Their wallet password may be compromised and transactions made from their account;
They would need to put in a request to Pablo (Santa Monica mayor) to trace the transactions;
Pablo (Mayor) is unlikely to act since it isn't a major breech on the blockchain;

Technology example answer 3 [4 marks]
The MONS currency may be subject to a 51% attack;
With no central authority to roll back the blockchain;
Double spend problem will occur;
Currency would lose credibility/residences may stop using it.

Technology example answer 4 [4 marks]
Residences are trusting that the software is designed well and secure;
Since it is open-source they may be concerned that hackers will find a flaw;
With no central authority to manage the blockchain, which is distributed;
There could be concerns that necessary updates/patches won't get rolled out.

Award **[2 max]** for a Governance non-technology example

Non-technology example answer 1 [2 marks]
Human nature to trust in authority;
When there is no Governance there may be irrational concern;
They may worry about the currency's value going down;
Because there is no way to influence the exchange rate;

Non-technology example answer 2 [2 marks]
The MONS currency could be abused by the criminal element;
It may be used for money laundering / fraud / illegal payments;
The anonymity of digital signatures makes this possible;
No central authority to prevent this;

[4]

Do not award marks for saying how to overcome concerns.

3. Award ***[6 Max]***

Determinism:
The hash algorithm must always generate the same output for the same input;
when replicated on different nodes;
Otherwise, the consensus cannot be reached;

Without determinism different miners would get different results;
And there would be no consensus;
So, the distributed ledger would be different for every node;

Without determinism one block could not link to the next / prevHash;
Therefore, transactions could be edited / blockchain would not be immutable;
The blockchain would be insecure;

Merkle tree and the block are validated many times by miners;
Without determinism the Merkle proof won't work;
So, transactions can't be validated;

Without determinism, when a sender signs a transaction, other nodes on the blockchain wouldn't be able to be certain it was them;
Which may result in an increase in illegal payments and corruption;

Non-invertibility:
A public key is hashed to provide a unique encrypted public address that can be published;
Whereas private keys are not publishable and can be hashed (needed to access the wallet);
Non-invertibility guarantees that publishable information is protected, and separated from private key;

Prevents the private key from being calculated if you have the public key;
Non-invertibility/secure private key prevents false transactions being made;
So that "digital signatures" can authenticate the person who made the transactions;

If the nonce used an invertible hash it could be calculated;
So, it would be solved quickly / difficulty level could not be set;
And fake branches could be created / double spend could occur;

Mark as 3 and 3.
Award **[1 max]** for definition + **[2 max]** for explanation, for both sections (determinism and non-invertibility) **[6]**

4. 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 (decentralization).
- 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 (intractable).
- 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.

Scalability

- Scalability is defined as the capacity for a system or network to grow in size to manage increased demand.
- Thus, scalability refers to the ability of the MONS currency to continue to function when the number of transactions increases.
- Number of miners are likely to increase in proportion to the number of transactions because there are more rewards.
- A peer-to-peer network makes scalability possible because it is easy to add new nodes.
- A peer-to-peer network is unlikely to bottleneck with increased transactions.
- An increase in processing speeds for miners causes the nonce difficulty level to adjust and allows the blockchain to function (regardless of the number of miners).
- Due to the limitations of proof of work, blocks should take a minimum time (e.g. 10 minutes) to create and should hold in the region of 1MB of data, which is about 1000 to 3000 transactions.
- Other consensus methods can be used to increase scalability at a slight cost of decentralization, e.g. using proof of stake, proof of ownership, instead of PoW;
- However, if the network becomes heavily congested, a MONS currency transaction might take longer to be processed.
- If a network is running slowly, the mining fees have to increase or there is a risk that miners will stop mining.

- These increased fees will need to be paid by the users making a cryptocurrency transfer. Small cryptocurrency transfers may incur high charges making the currency undesirable.
- Blockchain ledgers are more scalable than centralized ledgers because they are distributed and there is no bottleneck.

Strategies to improve scalability include
Increasing the block size to include more transactions.

- The initial reason behind block size limits is to prevent Denial-of-Service (DOS) attacks by hackers seeking to create huge (or infinite) blocks that would harm and paralyze the blockchain.
- Increasing the block size to cope with increased demand may place the MONS currency at a risk of attack.

Modifying the underlying protocol (although the issue with this is that there needs to be some central governance to make these decisions).

- The code is open source and a consensus (proposal and voting on forums and discussions boards) would be need to change the protocol.
- Since its creation there have been very few changes to the bitcoin source code so is unlikely that MONS blockchain code would be open to frequent changes.
- In Santa Monica, the MONS project would need some form of governance so that decisions to change the protocol and improve scalability could be made.

Sharding and other “Layer 2” solutions can be implemented to reduce congestion on blockchains, in which slower transaction types are put on a different chain which deals only with that type.
For example, Lightning networks, which is a layer 2 payment protocol designed to be layered on top of a blockchain-based cryptocurrency.

Security could be optimized according to the "Blockchain Trilemma".

Scalability concerns

- The lack centralized servers means that there is no control over the amount of hardware that can be added to the system (i.e. If centralized, scalability could be improved by the central authority by adding more processing power).
- Making decisions / governance of a distributed ledger is more difficult and has to rely on voting and an agreement before proceeding.
- The increased network traffic of many nodes on the blockchain can have a greater overall requirement for network bandwidth than (for example) centralized miners.
- Scalability in distributed ledger systems such as blockchain depends on the participation of the whole network, whereas centralized ledger systems (for example VISA) which depend only on the service provider and can scale quickly, but with hard limits imposed by the infrastructure.

Conclusion
A reasonable conclusion that includes both security and scalability.

[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. • Responses need limited knowledge of both security and scalability or more detailed knowledge of one or the other. • 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. • Responses need competent knowledge of one area (security or scalability) and limited knowledge of the other. • 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 a detailed knowledge and clear understanding of the computer science. • Responses need detailed knowledge of both security and scalability. • 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.

[12]

Total: [30]