Computer science
Case study: A local economy driven by blockchain

For use in May and November 2020

Instructions to candidates

- Case study booklet required for higher level paper 3.

8 pages

© International Baccalaureate Organization 2019

Introduction

Santa Monica is typical of many towns around the world. Over the past few decades the population has declined and many local businesses have closed. When the people of Santa Monica spend their pesos in the stores owned by multinational companies, the money leaves the town.

Pablo, the mayor, wants to reverse this process. He has investigated towns that have created their own local currency, and thinks that this is an idea that could work in Santa Monica. He found that these local currencies worked alongside the national currency. For example, one unit of the local currency would equal one peso. The local currency also had no value outside of the local area, so it could not be exchanged for other currencies, such as US dollars. However, if adopted in Santa Monica, citizens would be able to change the new local currency back to pesos whenever they wanted.

Pablo’s investigations showed that once a local currency had become established it brought considerable benefits to a town. Local businesses had more customers and were able to provide discounts for those who decided to use the new local currency. Many local workers saw the benefits of using the local currency and decided to accept some of their salary in it. However, many of these local currencies failed because of the administration costs they incurred, such as the cost of printing notes, combating fraud and providing additional banking services.

One Santa Monica resident, Dolores, a local computer science graduate, has suggested a way to overcome these problems. She has explained that “a *cryptocurrency* based on *blockchain* could help Santa Monica to avoid these problems because it doesn’t require any central administration. People who don’t know each other can transact without any need for a central authority, and that will remove these costs”. Pablo and Dolores have decided that the next step would be to promote the idea of a new cryptocurrency, called MONS, for Santa Monica.

The MONS project

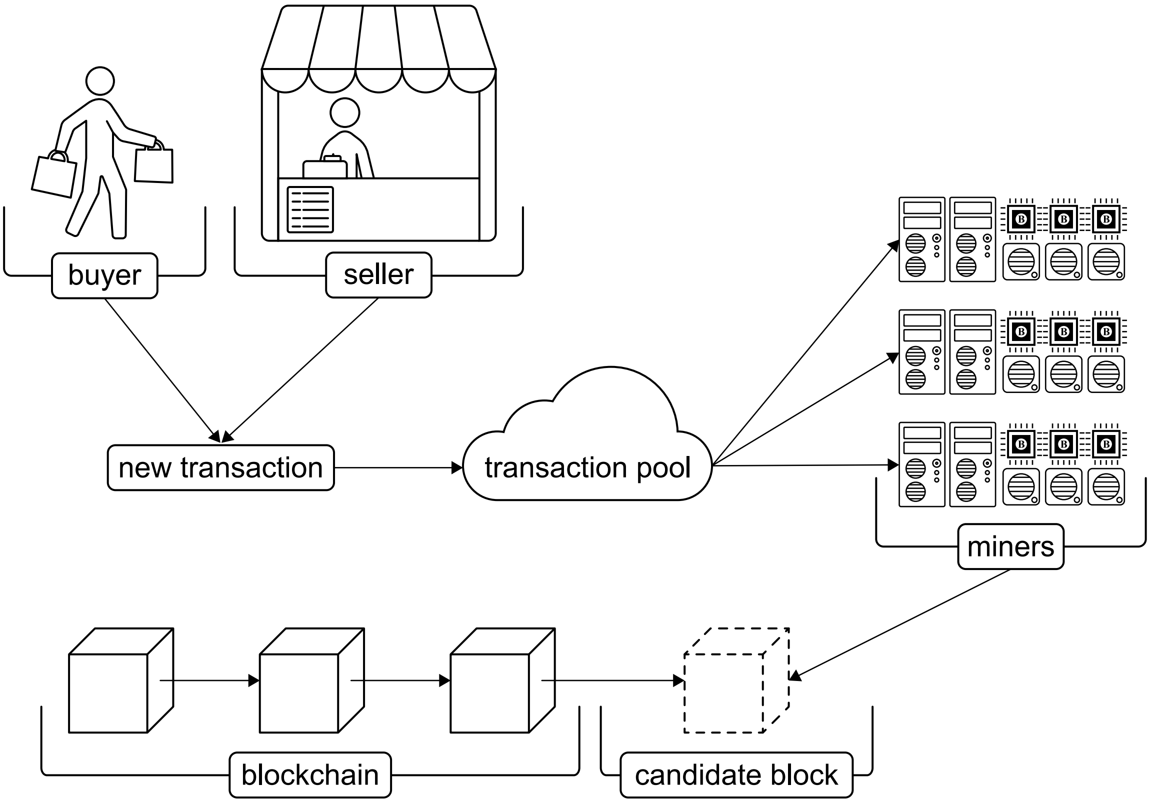
In a traditional banking system, a payment goes through a clearing process that may take as many as ten working days. During this time, the payer’s bank and the payee coordinate to validate the transaction, move the money, and verify that the payment has been successful. MONS would not have a central bank to do this, so an alternative would have to be found.

Some challenges of using a cryptocurrency are:

- how to create a transaction
- how to check that the transaction is accurate
- how to record a transaction in such a way that it cannot later be changed.

Dolores has explained to Pablo how MONS transactions could be created and validated by the nodes in the network, rather than a central authority. These can then be added in groups called *blocks*, which are similar to pages in a digital *ledger*. “Once a transaction has been validated, a new block can be added to the blockchain,” she said. “It can be viewed by everyone but it cannot be changed.”

Figure 1: The journey of a transaction



Dolores explained that “modern cryptocurrencies operate using a peer-2-peer (P2P) network to make and receive payments. The device of each MONS user is a node on the network and has an address consisting of 26 alphanumeric characters. When a user spends the currency, they transfer the MONS value from their address to the account address of the person that they are paying. The details of this transaction are then broadcast onto the network.”

“The other nodes on the network validate each transaction independently by running a range of checks. One check uses the transaction’s *digital signature* to verify the identity of the sender. Another check ensures that the buyer has not already spent the MONS being used in this transaction (known as the *double-spend problem*).” If the transaction is valid, the node sends it to its own neighbouring nodes, which also check it and send it on. In this way, only valid transactions are propagated across the network and, crucially, there is no single authority that determines transaction validity. The set of validated transactions is known as the *transaction pool*.

Even though transactions in the transaction pool have been validated, they remain unconfirmed. There are also specialized nodes on the network called *miners*. They are responsible for grouping unconfirmed transactions from the pool into *candidate blocks* to be added to the blockchain. The blockchain contains all the confirmed transactions that have ever taken place.

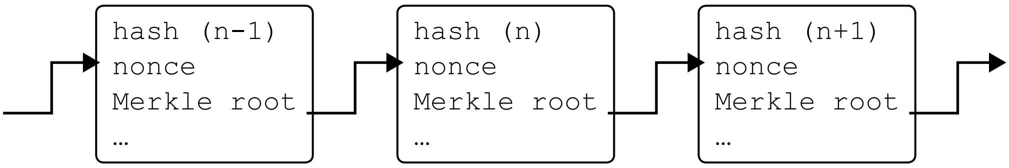
A *proof of work* is calculated by the miners. This is required to find a *nonce* to solve a block, and then add the candidate block to the blockchain. The incentive for miners to do this work is that they will receive a small amount of MONS from the network together with a nominal transaction fee from the participants of the sale. Dolores said that “the amount of time needed to solve a block should not be too short, but it should not be too long either. We will aim for around 10 minutes”.

Miners can improve their chances of being the first to solve a block by using large numbers of graphics processing units (GPUs). She explained that, “as the currency becomes more widely used, there will be more miners trying to solve the proof of work and of course more miners will be able to solve each block more quickly. However, one of the great things about the blockchain is that we can ensure that the solution time remains at 10 minutes, and we can do this even as the number of MONS miners increases.”

The structure of the blockchain

The blockchain is a *self-referential data structure* in which each block contains a reference to the next block.

Figure 2: A diagrammatic representation of the blockchain



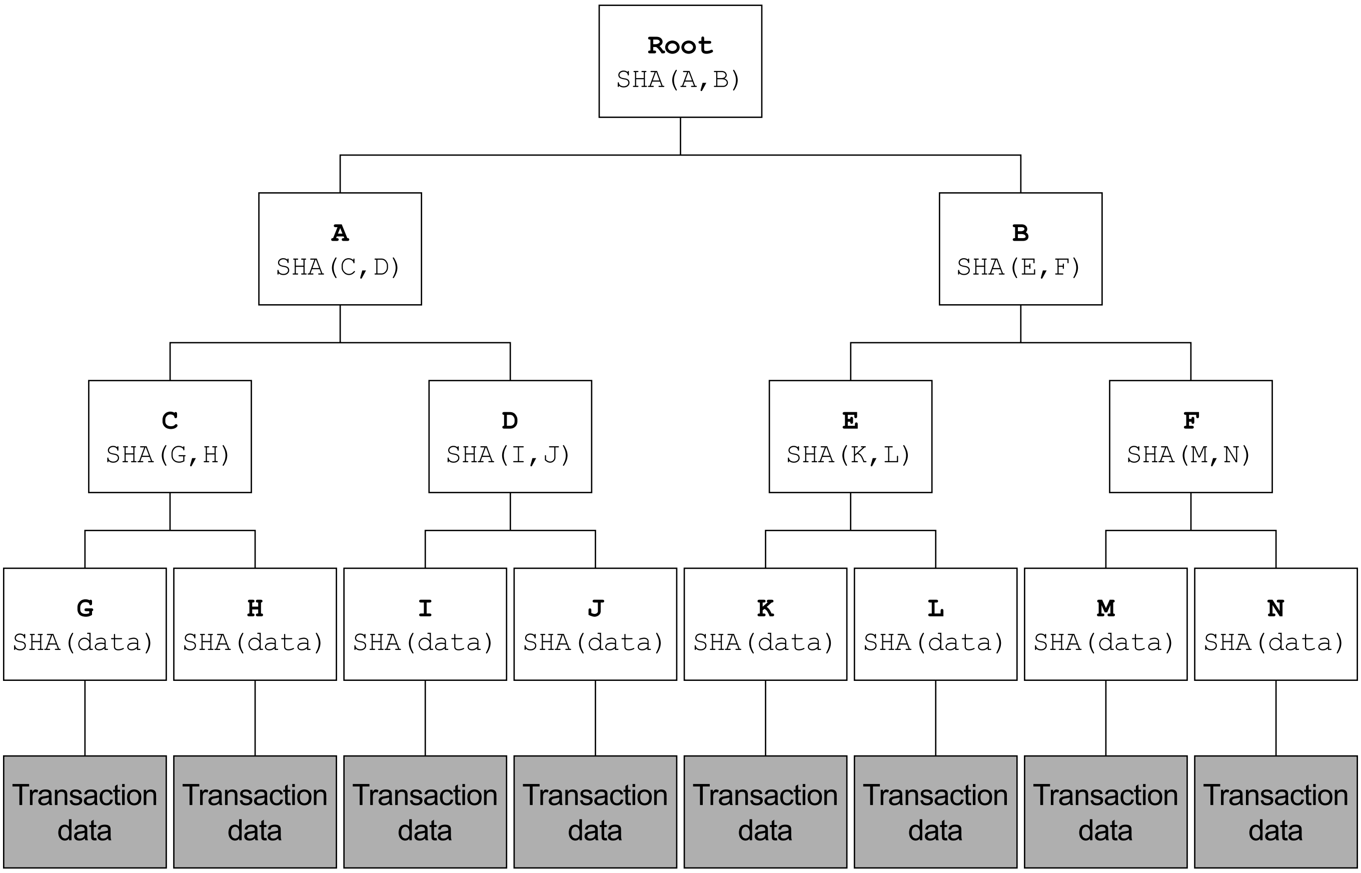
A set of metadata called the *block header* contains detailed information about each block.

Figure 3: An example of a block header

```
"number_of_transactions":188
"height":5432
"block_reward":2
"timestamp":1391270636
"merkle_root":0e83db9efb10076982a……94574318e7e
"previous_block":5341
"difficulty":2548.2
"bits":172758700
"size":317202
"version":912
"nonce":196898444
"next_block":5433
```

70 The list of transactions in each block is stored in a *Merkle tree*, the root of which is referenced by the block header. A Merkle tree is a binary tree in which each parent node contains the *cryptographic hash* of its child nodes, and each leaf node contains the cryptographic hash of its single data node. In the MONS blockchain, each data node stores the details of one transaction.

Figure 4: An example of a Merkle tree



The use of cryptography in the MONS project

Dolores was keen to emphasize the role of cryptographic algorithms in the proposed MONS project. “Cryptography will be used throughout the system, particularly hashing algorithms such as *SHA256*,” she explained. “The essential characteristics of good hashing algorithms are *determinism*, *non-invertibility* and *collision resistance*.”

Table 1: Some examples of SHA256 input and output

Input	Output
`"a"`	`87428fc522803d31065e7bce3cf03fe475096631e5e07bbd7a0fde60c4cf25c7`
`"The quick brown fox jumps over the lazy dog"`	`c03905fcdab297513a620ec81ed46ca44ddb62d41cbbd83eb4a5a3592be26a69`
`"The quick brown fox jumps over the lazy dog."`	`b47cc0f104b62d4c7c30bcd68fd8e67613e287dc4ad8c310ef10cbadea9c4380`
`[The IB Computer Science Guide PDF]`	`370e5655ff2e4e63e307e09e560639c72abbb8b5066616a72a130e2eb0240b8a`

Dolores went on to identify the following four key areas of the project in which cryptographic algorithms will play a central role.

The digital signature

The digital signature relies on asymmetric key cryptography and hashing to guarantee three crucial criteria. These criteria are:

- Authentication
- *Non-repudiation*
- Integrity

Digital signatures are used to validate MONS transactions before they are added to the transaction pool. There are three steps in the validation process:

- Key generation
- Creation of a signature
- Verification of a signature

“Key generation software, such as *PuTTYgen*, often uses a physical source of *entropy* to generate key pairs,” she stated.

The proof of work

In addition, the proof of work will require miners to find a hash with a particular characteristic, which we can decide. Some existing cryptocurrencies specify that the hash has to begin with a certain number of zeroes, for instance.

The blockchain

The blockchain uses hashing to ensure that transactions in the ledger, while accessible to every user of the network, cannot be altered.

The Merkle tree

The Merkle tree is also known as a hash tree. It allows the existence of a transaction in a block to be determined much more efficiently than if the transactions were just held in a list.

Promoting MONS to the citizens of Santa Monica

Dolores has convinced Pablo about the benefits of adopting MONS as a local cryptocurrency, but he is concerned that the citizens of Santa Monica may be reluctant to switch from the peso to MONS.

He points out one difference between a traditional currency and MONS that will need to be explained carefully: “In a traditional banking system, users trust the banks to keep everyone’s money safe; but with MONS, the whole blockchain, right from the very first transaction, would be visible to all MONS users, so it is important to be able to explain to citizens how their money is guaranteed to be safe.”

Dolores replies that “a user’s MONS balance is not stored, but it is calculated in real time by checking all the previous transactions. So, as long as all the previous transactions are still accurate, their current balance will also be accurate. The blockchain relies on a *distributed consensus* across all the nodes of the network, so in a sufficiently large network it is difficult to stage a *51% attack*.”

Pablo is also wondering about some of the potential consequences for the residents of the lack of a central authority managing MONS, as well as other potential disadvantages of a cryptocurrency.

Challenges faced

There are a number of challenges that are linked to the introduction of MONS. These include:

- understanding how new blocks are added to the ledger and how the proof of work prevents malicious nodes from taking over the MONS network
- understanding how the MONS architecture is scalable and can remain efficient as the number of users increases
- understanding the use of cryptographic techniques in the MONS project
- explaining to the Santa Monica citizens how their MONS balance is calculated from transaction data securely stored in a publicly accessible blockchain ledger
- investigating how the distributed nature of a blockchain cryptocurrency and the confirmation process may have disadvantages for the citizens of Santa Monica.

Candidates are not required to know the details of how any particular hashing algorithm is implemented.

Discussion of the economic arguments for or against local currencies and cryptocurrencies is beyond the scope of this case study.

Turn over

Additional terminology to the guide

51 % attack
Block
Blockchain
Block header
Candidate block
Collision resistance
Cryptocurrency
Cryptographic hash
Determinism
Digital signature
Distributed consensus
Double-spend problem
Entropy
Genesis block
Immutable transactions
Key pair generation
Ledger
Merkle proof
Merkle tree
Miner
Mining
Nonce
Non-invertibility
Non-repudiation
One-way function
Proof of work
PuTTYgen
Self-referential data structure
SHA256
Takeover attack
Transaction pool

Some companies, products, or individuals named in this case study are fictitious and any similarities with actual entities are purely coincidental.