SHA-3 and the use of Hashing in Cryptocurrencies

UNIVERSITY of LIMERICK
OLLSCOIL LUIMNIGH

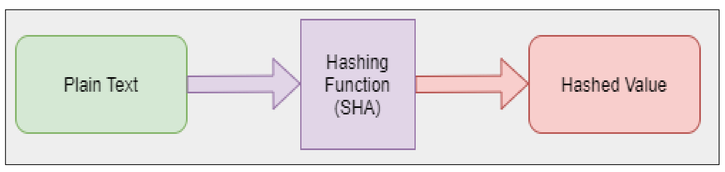
Piotr Kurzynoga

Specialist Diploma in Information and Network Security

Introduction

Hashing is a one-way algorithm this means that once a value is hashed there is no way to “un-hash” the value, hence hashing is described as a one-way function.

Each hashed value will return a value of a fixed length combined of various characters, being more precise a string of bits.



Simple representation of a one-way function.

Hashing is the building block behind all blockchains where each block chain network has its own “block of origin”, as the name implies a block chain is a forever growing list of data that are linked to each other and uses a similar concept as a linked list where in a block chain records cannot be inserted in the middle of a list but can only be appended to the end of an already existing chain.

Aim

The main goal of this paper is to present and showcase the importance of hashing in the cryptocurrency world and consequently blockchain networks.

Key points discussed in the paper:

- Highlighting how hashing is leveraged in building the blocks of a blockchain
- The relationship between the total hashing rate of a network and the difficulty to mine a block.
- Comparison of hashing functions mainly the SHA-3 and the older functions in the SHA family.

Method

Writing the paper begun with setting out and writing the Abstract which helped to set out the key goals and elements of the final paper:

- Checking the latest standards for hashing provided by the National Institute of Standards and Technology (NIST), to ensure the correctness of the research.
- Choosing a blockchain network, that facilitates documentation and exists for relatively long on the market to ensure the validity of the research.
- The above was based on being able to explore the blockchain itself and the individual blocks to gain more insights into the topic and validate the concepts presented by the blockchain.
- Showcasing and demonstrating the importance of hashing in cryptocurrencies by combining the above research

With the above mentioned points and a solid agenda for the paper, the research became a lot more structured and allowed me to focus on the relevant information for the final piece.

Results

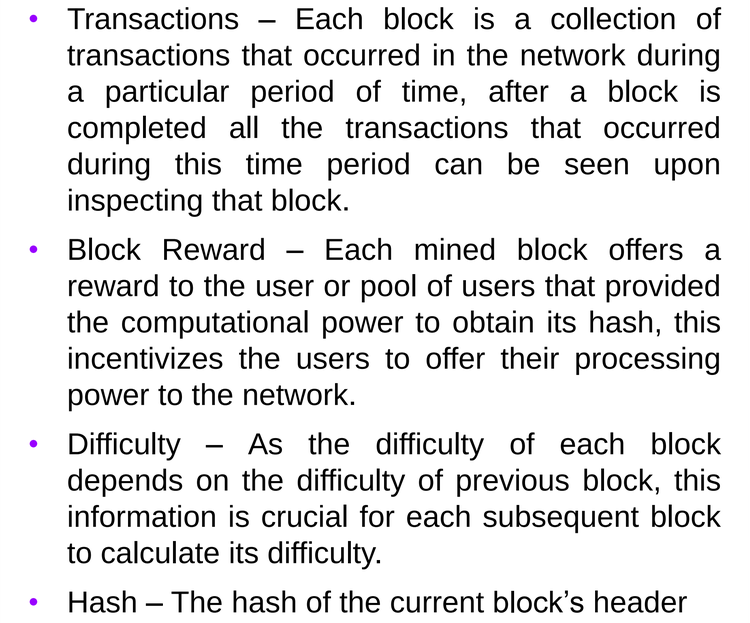
The outcomes of the paper are discussed in this section, focusing on the key concepts covered in the paper.

Below is a demonstration of he output generated by a hashing function for the sentence “Use of Hashing in Cryptocurrencies”, let’s see and compare the SHA-3 digest for 224, 256, 384 and 512 hash sizes.

Hash Size	Output
224	41494182432150ced8f91307580908f58c8f09f91e5917a1a31d4095
256	f3a14350aeadf909a71d3d2d59ccaac30c6196bcf290a9e79c69c7f326d6a09a
384	133e1bb5a88e2f7ccfe2457abab355ac690057060066fc8183ecec5b017c800c7554f18efac013c22eccb6bbe4df79ef
512	91016410cbf3cf5ee841491211eb2fdb574259837a3e3295470452912f3281d265a2a3c7ee588bc7860d587b1ecb06eaff8708d28ec4989672a90ffd635f5ced

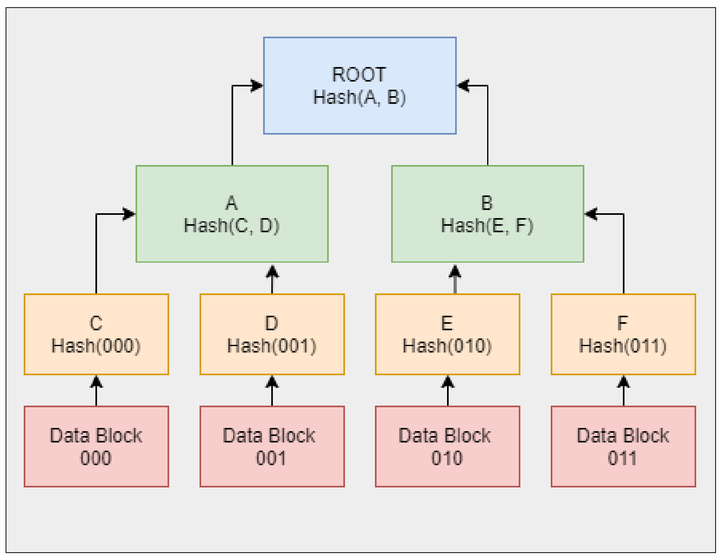
SHA-3 Generated Hashes

In the picture below a representation of the block contents can be seen and a short explanation is given for the most important elements of the block.



Information Contained within a block on the Ethereum blockchain network.

- Block Height – The block number in the chain
- Timestamp – The time at which the block was fully mined by a user or a pool of users
- Transactions – Each block is a collection of transactions that occurred in the network during a particular period of time, after a block is completed all the transactions that occurred during this time period can be seen upon inspecting that block.
- Block Reward – Each mined block offers a reward to the user or pool of users that provided the computational power to obtain its hash, this incentivizes the users to offer their processing power to the network.
- Difficulty – As the difficulty of each block depends on the difficulty of previous block, this information is crucial for each subsequent block to calculate its difficulty.
- Hash – The hash of the current block’s header
- Parent Hash – The parent hash is always included in each new block to from the chain.
- Nonce – A very important value which represents the amount of transactions in the block, knowing the exact number of transactions is important as it prevents a potential replay attack from occurring.



Representation of a Merkle Tree

A Merkle tree or commonly known as a hash tree, in its basic form is a hash-based data structure which represents a way of hashing a large number of data blocks together for efficient data verification.

Merkle tree’s are used as a basis for Merkle Proofs which are the foundation supporting the blockchain core concepts, ease of adoption and scalability. Merkle Proofs allow the verification of data in a Merkle tree structure by navigating through the tree to the chosen data block and validating the hash of the values against the Merkle Root.

Advantages of Merkle Proofs and Merkle trees:

- Possibility to split large amounts of data into smaller chunks
- Validation of small amounts of data within the tree
- Increased performance versus a large chunk of data

Conclusion and personal reflection

This paper highlights the functionalities and the key role, hash functions play in the world of cryptocurrencies and subsequently blockchain networks, from the very first block of origin to the very latest block mined just seconds ago.

With this paper I was able to deepen my knowledge on how blockchain operates and the concepts which revolve around it.

In particular I found the concept of Merkle Proofs ingenious and believe it can be leveraged in standard database applications.

Secondly the relationship between the Difficulty of mining a block and the Hash Rate provided by the network of miners highlights the key role of hashing in a blockchain network.

Acknowledgements

I would like to extend my thanks to all the lecturers and University of Limerick staff that helped to bring completion to this Specialist Diploma during these extraordinary times.

E&CE Department of Electronic & Computer Engineering