Development of an Exploratory Blockchain for Enhanced Data Security in Smart Grids

Nishkar Naraindath[1(✉)], Ramesh Bansal[1,2], and Raj Naidoo[1]

[1] Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria, South Africa
nrnaraindath@gmail.com, raj.naidoo@up.ac.za
[2] Department of Electrical Engineering, University of Sharjah, Sharjah, UAE
rcbansal@ieee.org

Abstract. Data integrity is of paramount importance to the operation and analysis of Microgrids. This paper has developed a functional blockchain system incorporating digital file hashing. The system provides the means to detect file tampering contributing to the advancement of data transparency and security. Opportunities for improvement to the current system have been provided, along with suggestions for future research.

Keywords: cryptography · cyber security · data integrity · file hashing · Proof of Work · SHA256 · transparency

1 Introduction

Data monitoring is essential for Smart grids as it enables stricter control and enhanced reliability [1]. Supervisory Control and Data Acquisition (SCADA) systems are commonly employed to gather data that serves as a necessary testimony to the operational conditions within the microgrid [2]. The system utilises the gathered information to optimise the operation of the grid by employing various energy management techniques [3]. The data may also be used to obtain insight into the performance of a grid by generating and analysing load profiles, load characteristics and power quality [4]. These data records can be subjected to accidental or malicious tampering [5]. Harmonic encryption can be employed to improve the confidentiality of the data; however, the approach cannot verify the integrity of the records [6]. This shortcoming needs to be addressed as it represents one of the three main pillars of cyber security responsible for electric grids' social and economic infrastructure viability [7].

At the same time, the application of blockchain technology has become increasingly prevalent. The need to facilitate data storage on the blockchain is being overlooked for more exciting projects such as financial transactions and smart contracts [8, 9]. Implementing a blockchain may be a promising solution to this challenge of maintaining data integrity due to its well-suited characteristics of immutability, visibility and decentralisation [10]. This paper explores the solution's potential by developing a traditional blockchain system to enhance data integrity from the first principles.

V. E. Balas et al. (Eds.): AITEES 2022, AHIS 3, pp. 281–288, 2023.
https://doi.org/10.2991/978-94-6463-074-9_24

2 The Immutable Blockchain

A blockchain is a distributed data ledger consisting of individual ledgers (represented by blocks) interlinked through cryptography (represented as chains) [11]. These properties enable blockchains to be characterised as reliable, immutable, and transparent.

2.1 Secured Through Cryptography

The concept of a hash stems from the idea that a fingerprint is a person's unique identifier. Hashing algorithms have been developed to securely map digital data to a finite data set in the form of a hash. Numerous hashing algorithms exist; however, some are more secure and reliable than others [12]. There are five requirements for these algorithms: one-way operation, deterministic, fast computational rates, avalanche effect and collision resistance. The hash can be utilised to determine if data has been altered efficiently, thus serving a significant role in the reliability and accountability of blockchain technology [13].

The SHA256 is a popular hashing algorithm employed in blockchains. It analyses digital data to produce a hash consisting of 256 bits equivalent to 64 characters. The main steps in the algorithm are portrayed in [14].

2.2 Consensus Protocols

Validation of a new block and overall blockchain is required before expanding a chain. The consensus among miners (specialised blockchain network participants) is also necessary for two purposes. Firstly, it protects the network from attackers. It achieves this by ensuring that the distributed ledgers are continuously synchronised with invalid chains being removed from the system. Attackers would have to instantaneously alter the majority of the distributed blockchains before synchronisation occurs. Consequently, this feature enables blockchain to be regarded as immutable. Secondly, a consensus protocol caters for conflicting chains in the network by ensuring the network conforms to the longest instantaneous blockchain [8].

A blockchain trilemma exists when collectively considering the three fundamental properties of blockchain technologies (decentralisation, scalability and security) [15]. Present consensus methods are not able to achieve optimisation in all areas. For instance, decentralisation requires decisions to be performed through consensus among distributed nodes in the blockchain. As a result, transactional speeds are reduced. On the other hand, scalability of the system is necessary for mass adoption, which will require faster transactional rates due to the increased number of transactions. Security is an area that often gets neglected. Proof-of-Work (PoW) and Proof-of-Stake (PoS) are the most common mechanisms for consensus [13]. PoW offers the most significant security at the expense of extensive energy usage and transaction processing rates. At the same time, PoS demonstrates enhanced transactional processing costs and rates with an intrinsic limitation on security. On occasion, a hybrid protocol is adapted [16].

The PoW protocol requires mining to be performed. Mining is the process in which numerous nodes compete to add a block to the blockchain, with the winner receiving a financial incentive. Miners iteratively generate nonce values until the block's hash is within a predetermined target hash range. The nonce is a 4-byte field, which increases from 0 until a desirable hash calculation is achieved [10].

2.3 Enabling Data Security Applications

Two options for data security through the blockchain exist. The first option entails storing the entire file in the blocks. There are drawbacks associated with this option, as the data will be publicly accessible. A significant limitation of this approach is the constraints placed on the size of data stored. For instance, the Bitcoin protocol is limited to 1-MB storage [10]. Another disadvantage is the intrinsic access latency, which negatively influences the cost and performance of a large-scale decentralised network. These challenges can be overcome with a more efficient approach. This method entails storing the document's hash on the blockchain while storing the document in a database or storage system. Consequently, tampered data can be identified without hindering the speed and cost-efficiency of the decentralised network.

3 System Development

Python has been selected as the programming language for the system implementation as it can be operated on various operating systems.

3.1 Blockchain Definition

The blockchain is defined as a class containing objects and object methods. Details of each object method have been presented in Fig. 1.

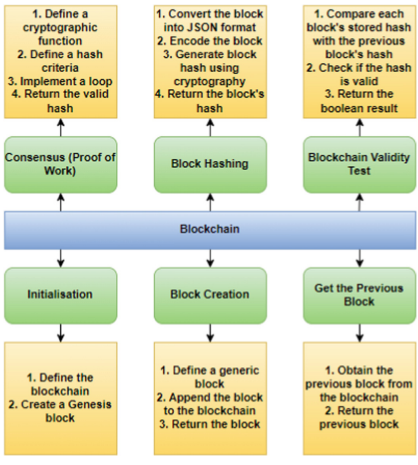

Fig. 1. An overview of the developed blockchain software

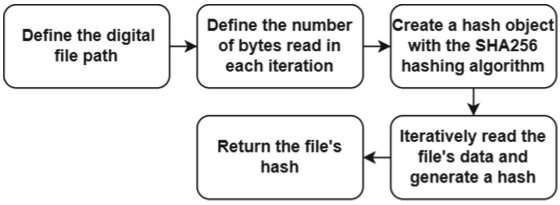

Fig. 2. Steps followed in defining the file hash function

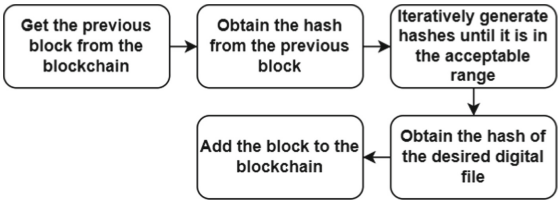

Fig. 3. Block mining process

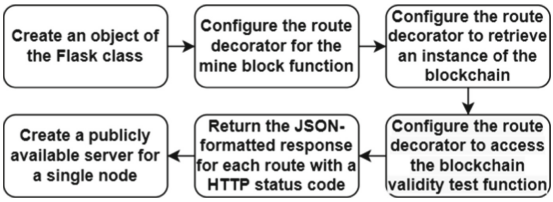

Fig. 4. Configuration process for defining the website application

3.2 Data Security

The digital files have been hashed through the function described in Fig. 2.

3.3 Block Mining

Block mining incorporates object methods defined for the blockchain. The process is depicted in Fig. 3.

3.4 User Interface

User interaction with a blockchain often requires extensive software development; however, a modest application is desired for this study. A website application has been facilitated through Flask. Flask enables interaction with the Blockchain network by implementing various HTTP methods and routes in the server algorithm. The commands used are presented in Fig. 4.

4 Results

The system's functionality is evaluated by creating a blockchain containing numerous blocks, as presented in Fig. 5. The validity of the blockchain is also analysed. Furthermore, the capability of the developed blockchain for data security has been evaluated by making amendments to a single document for each block appended to the chain.

The efficiency of the file hashing is investigated further by generating SHA256 hashes for various digital files of different sizes and types. File 1 is a 17279 kB excel data log. File 2 is a 3 kB text analysis report. File 3 is a 547 kB load profile PNG image. File 4 is a 36176 kB report in pdf format. A summary of the generated hashes is presented in Table 1.


```
{
  "complete_chain":[
    {
      "index":1,
      "previous_hash":"0",
      "proof":1,
      "timestamp":"2021-09-14 21:44:05.444250",
      "file_hash":0
    },
    {
      "index":2,
      "previous_hash":"d1e36afa3382d6a7a80e6e708ff9043b6fab89c5da4d7fbb5037c2893ab9aac5",
      "hash":"d0c89e68d2d8cd29b2f8897e859e4fa862a9f91a9c50a5ef55d8a447dea78cb6",
      "proof":533,
      "timestamp":"2021-09-14 21:44:56.718131",
      "file_hash":"a8a2f6ebe286697c527eb35a58b5539532e9b3ae3b64d4eb0a46fb657b41562c"
    },
    {
      "index":3,
      "previous_hash":"d0c89e68d2d8cd29b2f8897e859e4fa862a9f91a9c50a5ef55d8a447dea78cb6",
      "hash":"3debeaca7b81763991ddc1656388be7c77dc39c4551184efc80e92d18aeb6484",
      "proof":45293,
      "timestamp":"2021-09-14 21:46:34.886954",
      "file_hash":"932353df8a35b902a9854a41f2cca4de2e67c4d7eccb5d607c0c37b51954cef6"
    },
    {
      "index":4,
      "previous_hash":"3debeaca7b81763991ddc1656388be7c77dc39c4551184efc80e92d18aeb6484",
      "hash":"0a45dd0933ea1802a5d024efae48a5f412dc0bba69bc0b4f72a808e16a1e7959",
      "proof":21391,
      "timestamp":"2021-09-14 21:46:57.170236",
      "file_hash":"63108a76041b673e288c40f0f454cdd5223d444063ee3c789518474957fa1742"
    },
    {
      "index":5,
      "previous_hash":"0a45dd0933ea1802a5d024efae48a5f412dc0bba69bc0b4f72a808e16a1e7959",
      "hash":"4cf2ae887ef4e29e5495e7f4cb2878e34f104d3f12bb62725e45d0799005fd69",
      "proof":8018,
      "timestamp":"2021-09-14 21:47:25.629424",
      "file_hash":"736be2d5ebe67111dd8bb214c79fd0b0246bc603f0f9c9b70d379a7795252f77"
    },
    {
      "index":6,
      "previous_hash":"4cf2ae887ef4e29e5495e7f4cb2878e34f104d3f12bb62725e45d0799005fd69",
      "hash":"90be17ba2c63ab2c49dd897b0858be6409c7ff000697f7c25b12630c62f4c57c",
      "proof":48191,
      "timestamp":"2021-09-14 21:47:52.507146",
      "file_hash":"63108a76041b673e288c40f0f454cdd5223d444063ee3c789518474957fa1742"
    },
    {
      "index":7,
      "previous_hash":"90be17ba2c63ab2c49dd897b0858be6409c7ff000697f7c25b12630c62f4c57c",
      "hash":"a931f1af02df9dcfe7d5571f00b3e733a451037fc03dd431eb7d1b463d78a6b4",
      "proof":19865,
      "timestamp":"2021-09-14 21:48:46.718195",
      "file_hash":"932353df8a35b902a9854a41f2cca4de2e67c4d7eccb5d607c0c37b51954cef6"
    },
    {
      "index":8,
      "previous_hash":"a931f1af02df9dcfe7d5571f00b3e733a451037fc03dd431eb7d1b463d78a6b4",
      "hash":"fc762dd528d3562765c1f92e026dd5dd36b66fd03ecb87aa667ce3c7fec70e43",
      "proof":95063,
      "timestamp":"2021-09-14 21:48:46.718195",
      "file_hash":"a8a2f6ebe286697c527eb35a58b5539532e9b3ae3b64d4eb0a46fb657b41562c"
    }
  ],
  "message":"The chain was not replaced as the blockchain is valid."
}
```


Fig. 5. Complete blockchain record

Table 1. Generated SHA256 File Hashes

File	SHA256 Hash
1	b175adf1b001ac01340cc410d2773aab2c001b836ddacea296157034e01f486
2	fc659100fd231e9abb2971551e9d906a08eae3f77add611fcca5a4d9d72d8f5
3	2a1607855029fe8d7885380dec50f863adfcd3ca76f8c1127e3d7b7732fc3a2
4	02ca3b40c91b2182d0ed79ac8c6237fdf113af91b57b6aee00475d05014e6d5

5 Discussion

The SHA256 hashing algorithm proved to generate unique hash values for various digital files. It distinguished between excel, text, png and pdf files of different sizes. The hashing procedure occupied consistent processing times, which are negligible in practical applications. The algorithm can be made more robust by increasing the size of each read in the file. There is a clear opportunity to use file hashing for file identification.

The blockchain developed functions as expected. Each mined block contained a unique 'proof' value, indicating that the system continuously performed the PoW consensus. The challenge defined for the proof of work is relatively simple, which led to blocks being mined at instantaneous rates. A more complex challenge is required for practical applications to enhance the system's security. Considering the presently deployed algorithm, this can be achieved by decreasing the leading zeros for the target hashing range.

The index and timestamp provide a valuable means of determining when digital data has been stored on the blockchain. This experiment provides a timeframe in which the document was changed. The cryptographical linkage between blocks is another essential property of the developed blockchain, demonstrated in Fig. 5. This linkage is evident as each mined block contains the previous block's hash. This relationship has been further confirmed by executing the blockchain validity test described in Fig. 1. The complete blockchain proved valid, as demonstrated in Fig. 5. Consequently, each block mined underwent valid Proof of Work to achieve consensus. Consistency in the cryptographic links was also verified.

The blockchain system displays efficiency in detecting variations made to the text document. Minor amendments to the data within the document led to significant deviations in the hash outcomes. This characteristic can be attributed to the Avalanche effect required in hashing algorithms. The hash output for the document's data was deterministic due to the hashes remaining consistent with the data within the document. Thus, making it significantly simple to determine if data has been subjected to malicious tampering.

Lastly, the functionality of the developed blockchain is evaluated. The system explored incorporates a single node resulting in centralised operation. Additional nodes will contribute to enhanced security in the system. Furthermore, the privacy of the decentralised environment can be improved by implementing asymmetric cryptography for digital signatures. The latter approach is commonly employed in untrustworthy environments.

6 Conclusion

The application of blockchain technology remains a feasible solution to this challenge of maintaining data integrity in general. A python script, operated on a single node, maintained the blockchain server, while Postman was used as the user interface. The system demonstrated the means to detect tampering made to digital files of various types and sizes. The security of the developed blockchain can be enhanced by incorporating additional nodes incentivised through cryptoassets. In addition, asymmetric cryptography can improve the privacy of the environment.

The system proposed presents an opportunity for enhancing the reliability and accountability of data records in microgrids. However, it caters to modest needs. More sophisticated approaches are recommended for future research, such as a hybrid data storage strategy. The approach would entail storing a portion of the data and the data's hash. As a result, decentralisation and transparency can be maintained for relevant data portions while accounting for storage size constraints. Peer-to-Peer File storage systems can also be explored, which entails fragmenting data and storing instances of them across various stakeholders. These storage opportunities will increase the feasibility of the system investigated.

References

1. Bansal, R.C.: Power System Protection in Smart Grid Environment. CRC Press, New York (2019)
2. Bitzer, B., Kleesuwan, T.: Cloud-based smart grid monitoring and controlling system. In: 50th International Universities Power Engineering Conference (UPEC), September 2015, vol. November, pp. 1–5 (2015)
3. Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., Poolla, K.: Smart grid data integrity attacks. IEEE Trans. Smart Grid **4**(3), 1244–1253 (2013)
4. Bansal, R.C., Zobaa, A.F.: Handbook of Renewable Energy Technology & Systems. World Scientific, UK (2022)
5. Li, F., Luo, B.: Preserving data integrity for smart grid data aggregation. In: 2012 IEEE 3rd International Conference on Smart Grid Communications, November 2012, pp. 366–371 (2012)
6. Li, F., Luo, B., Liu, P.: Secure information aggregation for smart grids using homomorphic encryption. In: First IEEE International Conference on Smart Grid Communications, October 2010, pp. 327–332 (2010)
7. Gajrani, K., Bhargava, A., Sharma, K.G., Bansal, R.C.: Cyber security solution for wide area measurement systems in wind connected electric grid. In: IEEE PES Innovative Smart Grid Technologies Asia Conference, 10–13 November 2013, Bangalore (2013)
8. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Bus. Inf. Syst. Eng. **59**(3), 183–187 (2017)
9. Naraindath, N.R., Bansal, R.C., Naidoo, R.M.: Investigating the application of Ethereum smart contracts in energy exchanges. In: 2nd International Conference on Signals, Machines and Automation (SIGMA), 4–5 August 2022, New Delhi, India (2022)
10. Zheng, Z., Xie, S., Dai, H.-N., Chen, X.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)

11. Naraindath, N.R., Bansal, R.C., Naidoo, R.M.: The uprising of blockchain technology in the energy market industry. In: International Conference on Recent Developments in Electrical and Electronics Engineering (ICRDEEE), 15–16 April 2022, Faridabad, India (2022)
12. Preneel, B.: Cryptographic hash functions. Eur. Trans. Telecommun. **5**(4), 431–448 (2010)
13. Sabry, S.S., Kaittan, N.M., Ali, I.M.: The road to the blockchain technology: concept and types. Period. Eng. Nat. Sci. **7**(4), 1821–1832 (2019)
14. Rachmawati, D., Tarigan, J.T., Ginting, A.B.C.: A comparative study of Message Digest 5(MD5) and SHA256 algorithm. J. Phys. Conf. Ser. **978**, 012116 (2018)
15. Zhou, Q., Huang, H., Zheng, Z., Bian, J.: Solutions to scalability of blockchain: a survey. IEEE Access **8**, 16440–16455 (2020)
16. Pilkington, M.: Blockchain technology: principles and applications. In: Research Handbook on Digital Transformations, pp. 225–253 (2016)