The Blockchain Art Simulation (BARTS) and Experiential Exercises

Sean Patrick Sanders*
G. Lawrence Sanders*
spsander@buffalo.edu
mgtsand@buffalo.edu
SUNY-Buffalo
Buffalo, NY, USA

ABSTRACT

This paper introduces the online Blockchain ART Simulation (BARTS) and a set of experiential online exercises that illustrate hashing concepts for validating blockchain transactions. Our premise is that understanding the role of secure hashing algorithms in the mining process is the primary conceptual impediment for students to gain an accurate picture of the validation process for blockchain transactions. The BARTS simulation helps develop the conceptual foundation for understanding hashing concepts, and it also leads to understanding blockchain-related concepts.

In addition to assisting in understating blockchain concepts, the BARTS simulation and the accompanying exercises are useful in understanding and applying hashing concepts related to password verification, verifying software signatures, digital content signature verification, and averting man-in-the-middle threats.

CCS CONCEPTS

• **Applied computing** → **Education**; **Interactive learning environments**; • **Security and privacy** → **Domain-specific security and privacy architectures**;

KEYWORDS

Hashing algorithms, BARTS simulation blockchain concepts, education

ACM Reference Format:
Sean Patrick Sanders and G. Lawrence Sanders. 2021. The Blockchain Art Simulation (BARTS) and Experiential Exercises. In *26th ACM Conference on Innovation and Technology in Computer Science Education V. 2 (ITiCSE 2021), June 26–July 1, 2021, Virtual Event, Germany*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3456565.3460038

*Both authors contributed equally to this research.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ITiCSE 2021, June 26–July 1, 2021, Virtual Event, Germany
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8397-4/21/06…$15.00
https://doi.org/10.1145/3456565.3460038

1 INTRODUCTION AND MOTIVATION

Modern cybersecurity education in the management science and computer science disciplines considers blockchain technology knowledge essential [3]. However, many students find blockchain concepts to be elusive. It is not uncommon for us to hear comments from students and the general public asking how Bitcoin is mined and about the role of hashing in mining. To find the answer requires a modest understanding of a hashing algorithm. However, the existing material on blockchain concepts tends to be either simplistic or technically complex and there are not enough hands-on exercises [1].

We developed the BARTS simulation and exercises to facilitate understanding blockchain mining and the ensuing addition of blockchain transactions. The BARTS simulation is a non-technical simulation where participants mine or validate a digital coin transaction for buying and selling drawings (see Figure 1). The simulation has been successfully used with over 400 graduate students, undergraduate students, and high school students. Participants just need a laptop, a smartphone, or a tablet with access to the internet to participate as a cryptocurrency miner.

The initial version started as an in-class exercise. The current online version easily scales up to 50 participants. Many students participating in the BARTS simulation tell us that they have an aha experience after they go through just a couple of iterations of the mining process. Some of them still may not know the hashing algorithm's inner details any more than they understand how the exhaust valves open and close in four-stroke engines to produce horsepower, but they now know that the hash is the key to understanding the mining process.

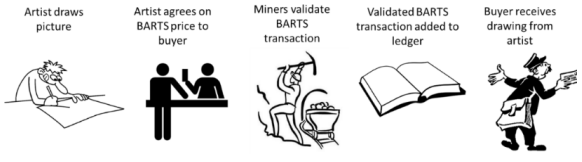

Figure 1: The BARTS Process

2 THE BARTS SIMULATION SCENARIO

BARTS Inc. is a gamified blockchain-based network for buying and selling pencil drawings and sketches (Figure 1). We tell the participants that the initial coin offering for the 200 million BARTS tokens took place in July of 2018. Two hundred famous pencil artists received 1,000 to 20,000 BARTS tokens if they agreed only to sell their

pencil drawings through the ARTBARTS network for three years. Also, over 10,000 gallery owners, investors, dealers, collectors, and even artists purchased 60 million BARTS for approximately $100 million in US funds. There are now over 60,000 artists and buyers participating in the marketplace. BARTS miners must use the interactive online mining software for solving a hash problem. Below are the teaching process steps for the simulation. The PowerPoint slides are available at https://www.artbarts.com.

Step 1. The class before the simulation (takes about 15 minutes)

The instructor reviews the BARTS scenario for 10 minutes. The instructor asks for volunteers to be artists and gallery owners. It is best to have between three and seven people sign up as an artist. Three to five gallery owners or buyers also need to be identified. The instructor sends the drawings to the three gallery owners. The Artists and Gallery Owners negotiate a price for the picture from 1 to 20 BARTS coins for each drawing. The artists then send a picture of the drawing taken with a camera to the instructor with the drawing's negotiated price.

Step 2. The class on simulation Day (takes about 1 hour):

The instructor shows an example of a BARTS blockchain wallet (https://marvelapp.com/prototype/fh036g4). The instructor starts the ledger at https://tinyurl.com/12qfzwpj. The instructor will show the transaction details for the first BARTS transaction. Each class member will use the BARTS Mining Program at https://tinyurl.com/2aegx78v to attempt to generate a hash with a leading zero. The miner that finds a hash value with a leading zero yells out, "EUREKA." The transaction is added to the blockchain ledger if at least three miners validate the transaction. After adding all of the transactions to the ledger, the instructor debriefs the class and tells them how the BARTS mining process is different from Bitcoin mining.

Step 3: The class on simulation day or a class following the simulation (takes about 15 minutes):

We have found that the BARTS simulation is an excellent way to introduce hashing concepts, but the hashing process needs additional discussion because of its importance to several security concepts. These exercises delve deeper into hashing concepts and were also used as the foundation for developing the BARTS simulation [2].

Exercise 1: Generate a nonce that will result in a leading zero for a hash. In blockchain implementations, the nonce is added to the end of the text being hashed to generate a hash with a specified number of leading zeros. The difficulty of the mining process is controlled by requiring more leading zeros. Bitcoin currently requires about 19 leading zeros. Students enter their name along with a nonce of 1 right after their name. This number is incremented by 1 more unit until a hash with one leading zero is generated. This program is available at http://104.156.254.129/Exercise1.php.

Exercise 2: A Hashing program that automatically searches for a nonce. This algorithm is complicated because it has to keep searching until it finds a hash with the correct number of leading zeros. Bitcoin miners use specialized hardware capable of generating trillions of hashes per second. This program is available at http://104.156.254.129/Exercise2.html.

Exercise 3: Mining Computation Issues: The purpose of this exercise is to illustrate the computational demand that is required for using hashing for proof of work. It requires participants to enter the text to be hashed, along with the number of leading zeros, then click on the hashing algorithm desired and the number of times to run the simulation. The program will find the hash by adding a nonce, or random number, to the string until it generates a hash with the appropriate number of leading zeros. This program is available at http://104.156.254.129/Exercise3.html.

Exercise 4: Birthday Paradox and cracking secure hash algorithms: The safety of secure hash algorithms is always an issue of interest. The Birthday Paradox demonstrates the amount of brute force computing necessary to find a hash collision. The program can be found at http://104.156.254.129/BirthdayParadox.php. The number of years needed to find a collision for the 160 bit SHA1 algorithm using 5,000 ASICS computers, each capable of 13TH/s, is 0.74 years. This contrasts with the 208.06 trillion years to find a collision with the SHA256.

Table 1: Effectiveness of blockchain materials

Questions	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
The material covered in the Blockchain Arts Simulation (BARTS) helped me gain a clearer understanding of blockchain concepts	5 (4.7)%	2 (1.9%)	6 (5.7%)	46 (43.4%)	47 (44.3%)
The material covered in the module related to hashing gave me gain a clearer understanding of blockchain concepts	4 (3.8)%	4 (3.8)%	5 (4.7%)	45 (42.5%)	48 (45.3%)

3 CONCLUSION

We sent anonymous surveys in December 2020, and April 2021 to 125 graduate students enrolled in an online synchronous technology management course. One hundred and six students responded (84.8% response rate). We asked the students about the percentage of the new understanding of hashing concepts they received from the teaching module? The mean for the knowledge and understanding increase was 72.1%. The results in Table 1 also reinforce the benefits of the BARTS simulation and experiential exercises. Approximately 88 percent of the students agreed that the teaching material helped gain a clearer understanding of blockchain concepts.

These results are promising, given that many of the individuals in the class had extensive experience in systems development and application programming. We are confident that teaching blockchain and hashing concepts are easier when the teaching is exciting and interactive. We think the approach used here establishes a strong foundation for understanding hashing concepts and creates an opportunity to evaluate and discuss contemporary blockchain concepts and the many applications of hashing algorithms.

REFERENCES

[1] A. R. Rao and R. Dave. 2019. Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications. In *2019 IEEE Integrated STEM Education Conference (ISEC)* (2019-03). 191–198. https://doi.org/10.1109/ISECon.2019.8882068 ISSN: 2330-331X.

[2] Sean Sanders. 2018. A-Noncing the Use and Performance of Hashing Algorithms. In *34th Annual (CCSC) Eastern Regional Conference* (2018-10-01).

[3] Kenneth David Strang, Ferdinand Che, and Narasimha Rao Vajjhala. [n.d.]. Ideologies and Issues for Teaching Blockchain Cybersecurity in Management and Computer Science. In *Innovations in Cybersecurity Education*, Kevin Daimi and Guillermo Francia III (Eds.). Springer International Publishing, 109–126. https://doi.org/10.1007/978-3-030-50244-7_7