A Novel Framework to Teach Hands-on Laboratory Exercises in Blockchains

Bertony Bornelus
Florida Agricultural and Mechanical University, Bertonyl.bornelus@famu.edu

Hongmei Chi
Florida Agricultural and Mechanical University, hongmei.chi@famu.edu

Hossain Shahriar
Kennesaw State University, hshahria@kennesaw.edu

A NOVEL FRAMEWORK TO TEACH HANDS-ON LABORATORY EXERCISES IN BLOCKCHAINS

Bertony Bornelus[1], Hongmei Chi[2] and Hossain Shahriar[3]

[1,2]Florida Agricultural and Mechanical University
Computer Information Science Department
Tallahassee, FL 32301

[3]Department of Information Technology
Kennesaw State University
1100 South Marietta Parkway
Marietta, GA 30060, USA
[1]Bertony1.bornelus@famu.edu [2]hongmei.chi@famu.edu [3]hshahria@kennesaw.edu

ABSTRACT

With the growing demand for blockchain developers there are few hands-on labs/modules available for training current students, the future developer professionals. Our goal is to develop series of hands-on labs that would address every application of blockchain and thus provide practical tools to educate Cybersecurity professionals and equip them to address the cyber security in blockchain. The labs developed will be a part of a new Cyber Security educational framework. There will be a modularized approach to the lab development, to focus development on the skills for each aspect of blockchain and app. The labs will also include integration of all the aspects of blockchain, along with its application. This approach will help students to systematically learn and comprehend the fundamental concepts. The labs would be built based on real-life scenarios, to enhance their ability to understand and solve real-life cybersecurity problems. This integrated approach would expose the students to the cost to risk involved at each stage of the blockchain application, arming them with required information to educate the management.

Keywords: Blockchain, cryptography, bitcoin, hands-on lab, decentralized & distributed ledger

1. INTRODUCTION

Since the interception of Bitcoin in 2009, the first popular (decentralized) peer–to–peer cryptocurrency. Blockchain application has the potentiality to becoming a disruptive revolutionizing e-commerce technology to affect many industries such as financial and non- financial, eliminating the need for third parties, reducing cyberattacks and increase transparency; where typical transactions yield high economic loss and negative socio – technical impacts. Blockchain has multi-contents to support (See Fig.1). There is a big learning curve for students to overcome. It is difficulty for students to follow it in one course. We design a set of hands-on labs to address those challenges one by one.

In recent years financial institution, social media giants such as Facebook, and medical institutions have all faced substantial amount scrutiny for exposure of customers data. With the emergent of Bitcoin, the first popular blockchain decentralized application; blockchain has become a viable solution for recording transactions in a growing list called blocks which are linked and protected using cryptography.

Figure 1. Basic Components in Blockchain

The application of blockchain has shown a promise to various areas such as: Security traceability, Distributed data storage and Identity authentication. Many of the respondent of the survey believe that core features of blockchain technology are "tamper – resistance and distributed system". Moreover, the feedback from companies why they have not applied blockchain technology shows, the biggest challenge is that management has yet to decide to make layout in the field of blockchain, followed by lack of industry standards and third, no talents as shown in Fig.2.

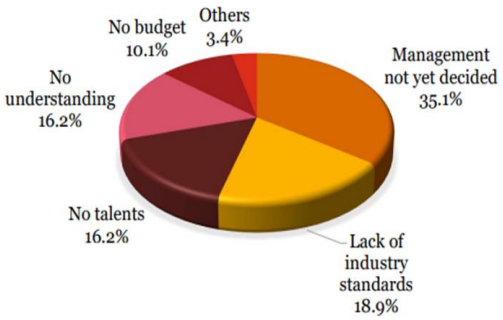

Figure 2: Reasons not consider applying blockchain technology [1]

The cost is not the dominant factor why people have not adopted blockchain technology. Once policy have been normalized, huge number of enterprise will take a chance on blockchain technology. However, according to Fig. 2: from the survey conducted by PwC and VeChain [1] "Talents" is the second leading factor that impedes blockchain technology implementation.

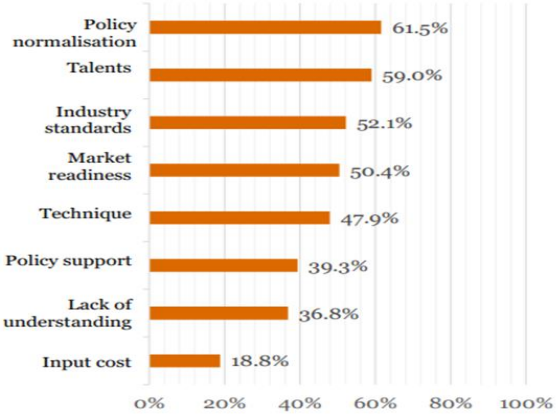

Figure 3: Concerns for blockchain technology

We must prepare our students in this job market via integrating blockchain related hands-on labs into our cyber security courses. According to our plan, we expand the cybersecurity program through educating and training students from different disciplines and backgrounds. Faculty development efforts will build a lab-based teaching environment for our students and learners in blockchain technology.

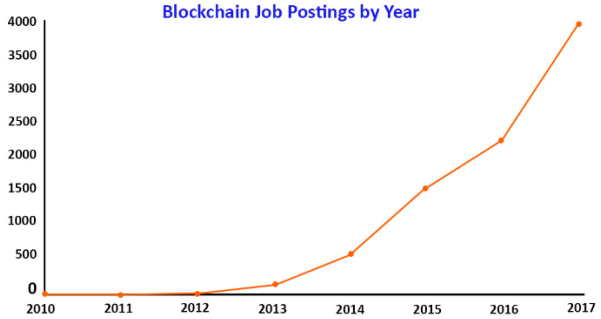

Figure 4: Blockchain job market boom [12]

This paper will examine blockchain application, technology and implementation of smart contract. Then, we will describe how developing a hands-on lab for current and future technology security professionals, will enhance trainee's knowledge and practical skills of how to implement smart contracts and a synopsis of tools such as: Remix IDE, Truffle, Ethereum Virtual Machine, MetaMask and node.js. Throughout this paper will increase computer sciences students' and IT professional awareness of Blockchain technology and development of use cases via various hands-on labs and make future IT professionals ready to be blockchain developers.

2. BLOCKCHAIN &APP

Blockchain is an emerging technology originated from the distributed cryptocurrency Bitcoin, Satoshi Nakamoto in 2008, introduce the peer to peer crypto system in a white paper called "Bitcoin: A peer – to Peer Electronic Cash System". Which explain," Bitcoin", as an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party [2]. Creating transactions that are impossible to reverse which protect seller and buyers from fraud.

2.1 Transactions

As shown in Fig. 5, each bitcoin is electronic chain of digital signatures, where each owner transfers the cryptocurrency to the next by a digital signature of hash for the pervious transaction and the public key of the next owner and added the information at the end of the currency. A payee can easily verify the signatures to verify the validity of the chain owner.

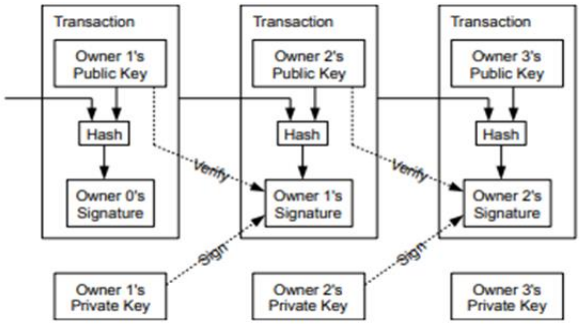

Figure 5: Bitcoin Transactions [2]

To avoid the process of overspending or duplicate transaction, all transactions are included in the chain of the pervious block and are publicly announced to all participants to agree on a single history of the order of the block chain, therefore, a time stamp is needed to verify the order of the chain.

2.2 Timestamp Server

The timestamp server was proposed by Satoshi Nakamoto, to works by taking a hash block of items to be timestamped then broadcast the hash block, each timestamp is included in the previous timestamp hash, creating a chain, with each timestamp strengthening the block before it seen in Fig. 6.

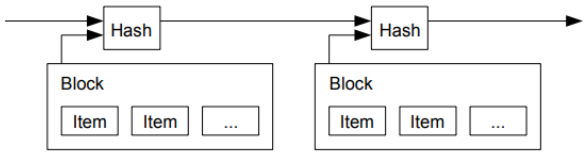

Figure 6: Bitcoin timestamp [2]

2.3 Proof-of-Work

The proof-of-work algorithm (seen in Fig.7) is the cornerstone of bitcoin technology, to create a tampered proof and fraud resistance block. Proof-of-work involves searching for a value that when hashed, such as with SHA-256. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For the

timestamp network, bitcoin implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it [2].

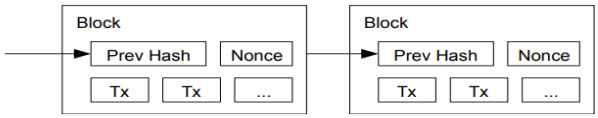

Figure 7: Proof of Work

For instance, given that two blocks exist for the same transaction block A - genuine and Block B- a tampered block, until the next the block is created both blocks are retained, once the next transactions have taken place it will be added to the growing genuine block and shortest block B will be disregard. Authenticating the vitality of the transaction (proof-of-work). Not every block makes it to every node on the peer to peer network, however, when the block reaches the nodes the node will accept the longest block as the genuine.

Once the genuine block grown enough block, Satoshi Nakamoto introduce the Merkle tree to compress disk space and not break the block chain. Thus, transactions are hashed in a Merkle tree. With the root current hashed and all pervious transactions hashed represented in Fig. 8.

A node can create and propose a transaction, validate transactions, and undertake mining to support consensus and establish the integrity of the data. When nodes create transactions, these are signed by nodes using their private key to validate that these nodes are the true owners of the asset that they are transferring to someone else in the blockchain secured network. [14]

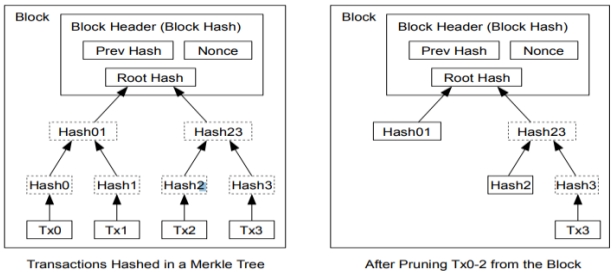

Figure 8: Merkle Tree [2]

3. LITERATURE REVIEW

Currently, there are few research papers about designing hands-on labs that addresses blockchain development and implementation. Mainly due to the infancy of blockchain application students are highly unaware of the use for blockchain application.

Thus, Delmonlino [8] in the Fall 2015, at the University of Maryland, conducted a series of lessons using Smart Contract to create their cryptocurrency labs presented to their undergraduate security -level students. Throughout the series they identified pitfalls in designing a safe and secure contract and advocating the best practices for implementing smart contracts. Smart contracts are user – defined programs that specify the rules governing transaction, and that are enforced by peer network [8] which aim to the lower legal and transaction in comparison to traditional financial contracts. However, there several unique challenges when programming smart contracts “play for keeps”, if a smart contract is buggy the functionality of the contracts could lead to economic loss and or worst the program malfunction. Therefore, smart contract requires “economic thinking” and must be written to ensure that all parties are safeguard when using the program. During the research conducted at University of

Maryland, they used the Ethereum's Serpent language, however, focus was not language-specific but the broad model.

4. HANDS-ON LAB DESIGN

Our goal is to develop series of hands-on labs that would address every main application of blockchain and thus provide practical tools to educate Cybersecurity professionals and equip them to address the cyber security problem blockchain. This approach will help students to systematically learn and comprehend the fundamental concepts in blockchain.

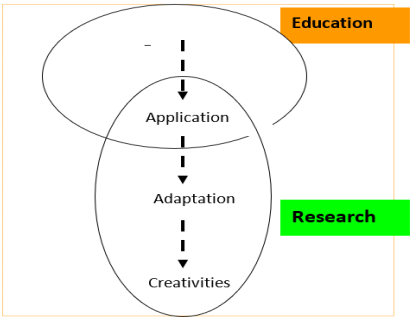

Figure 9. Learning Tree Model

We are following active learning model, which starts from hands-on to creativities educational approach. From education to research given a comprehensive see Fig.9. Stage of the security development of blockchain arming them with required information to educate the management in blockchain.

Solidity is a programming language that is smart contract oriented, Ethereum is a decentralized platform for applications that run exactly as programmed without any chance of fraud, censorship or third-party interference [18]. Truffle is a development environment, testing framework and asset pipeline. Ethereum Ganache quickly fire up a personal Ethereum blockchain which students can use to run tests, execute commands, and inspect state while controlling how the chain operate. Meta Mask allows students to run Ethereum decentralized Apps(d-Apps) right in their browser without running a full Ethereum. Node. JS node is an open-source, cross-platform JavaScript runtime environment that executes JavaScript code outside of a browser [18].

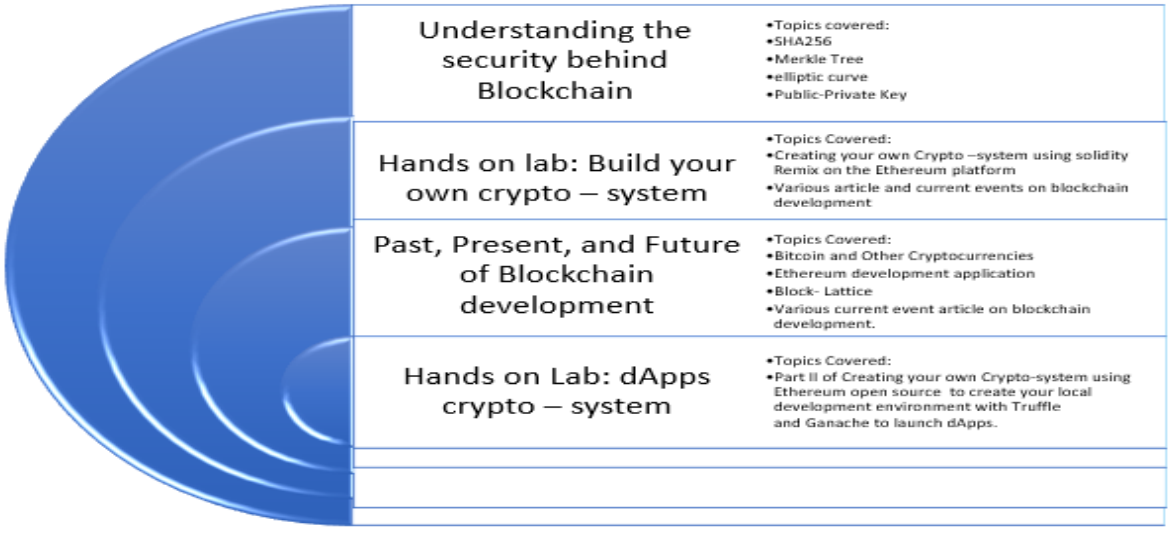

Figure 11. Contents in Hands-on lab

5. CASE STUDY

In this Section, we discuss how to design specific hands-on lab to help students understanding the fundamental concepts of blockchain technology and implementation of smart contract using the Ethereum platform, power point presentation and article written by blockchain developers and enthusiast. We layout a few hands-on labs based on blockchains applications. The labs would be built based on real-life scenarios, to enhance their ability to

Understand and solve real-life cybersecurity problems. This integrated approach would expose the students to the cost to risk involved at each

5.1 Understanding Theory behind Blockchain

The purpose of this topic is to introduce students to Blockchain and the encryption computation behind this technology - Merkle trees are a fundamental part of blockchain technology - SHA - blockchain such as bitcoin uses a SHA256 hash function and Elliptic Curve Cryptography to improve security and privacy. Therefore, we will define and explain the computational properties of these functions.

5.2 Developing cryptocurrency token lab

The purpose of this lab is to introduce students to the leading Blockchain platform Ethereum, via writing smart contract using Solidity a contract-oriented programming language. It is used for implementing smart contracts on various blockchain platforms and Remix a powerful, open source tool that help students write Solidity contracts straight from the browser all running on the Ethereum platform.

5.3 Past, Present & Future

The purpose of this topic is to introduce students to the real life blockchain applications: Bitcoin, AWS Quantum Ledger Database, Azure MS Blockchain, IBM Hyperledger... Future blockchain technology such as Block lattice. Students will further understand the wide use of blockchain technology.

5.4 Case Study: Delivery Drone &Smart Door

The purpose of this lab is to further the student's development capability of Blockchain technology by create decentralized application (d-Apps) using the following tools: Solidity, Ethereum- is a decentralized platform for applications that run exactly as programmed without any chance of fraud, censorship or third-party interference [16]. Truffle - is a development environment, testing framework and asset pipeline for Ethereum Ganache - Quickly fire up a personal Ethereum blockchain which you can use to run tests, execute commands, and inspect state while controlling how the chain operates [18]. Meta Mask - It allows you to run Ethereum decentralized Apps right in your browser without running a full Ethereum node [18]. JS node - is an open-source, cross-platform JavaScript runtime environment that executes JavaScript code outside of a browser.

Lab 1 explains the computation behind blockchain technology we introduce topics such as cryptography, elliptic curves, Merkle tree, and SHA algorithm. Lab 2 students will actively develop and implement smart contract to create a their ever-own cryptocurrency and token using the Solidity programming language on the Ethereum Remix IDE. Lab 3 will be "The Past, Present and Future of Blockchain", which is an overview of blockchain use cases, past and future blockchain applications. Lastly, in Lab

4 we will challenge our students in creating a Decentralized Application (d-Apps) using, the Ethereum open source using tools such as: Truffle and Ganache.

6. STUDENTS' FEEDBACK

During Spring 2018, a joint survey was conducted at our University, Introduction to Computer security. During the survey students were asked a series of questions regarding to blockchain, blockchain development platform and interest in blockchain development. 32 students responded to the questionnaire. We show a few survey results here.

When students were asked, have they heard of blockchain? 46.8% stated, "No" and 56.3 "Yes". Students who stated, "Yes" describes blockchain.

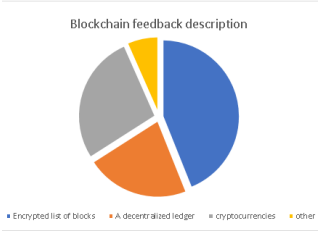

Figure 12: Students description of blockchain

An overwhelming number of students describe blockchain as encrypted list of blocks, followed by cryptocurrencies, lastly a decentralized ledger. Next, we asked students if have they heard of Ethereum open source blockchain platform and cryptocurrency.

65.5% of students stated, "No" they have not heard of Ethereum and 34.3% students have heard of Ethereum, those have heard of Ethereum describes in Fig 13: Students description of Ethereum as:

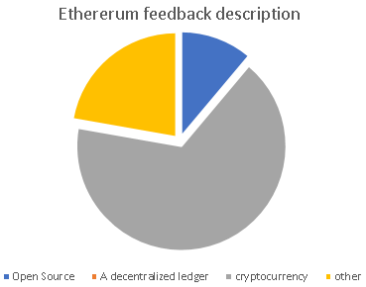

Figure 13: Students description of Ethereum

31% responded, Yes, to knowing about Ethereum, many describe Ethereum as a cryptocurrency, followed by other, and lastly a few said, "open source". Students have stated, overwhelmingly, that they have heard about blockchain and would like to learn more about blockchain technology.

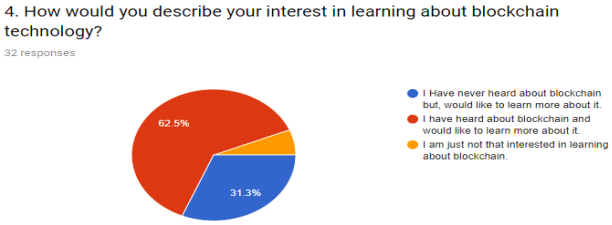

Figure 14: Interest in blockchain technology

Leading is 31.3%, Have not heard of blockchain and would like to learn more about blockchain technology and 6.3% were not interested in learning about blockchain technology.

Lastly, students describe prodigiously at 46.9 % - career opportunities as a reason for increase interest in blockchain technology, followed by 31.3% - cryptocurrencies, 12.5% - cryptography, 9.4% - mining and 0% for d-Apps (decentralized Application web 3.0).

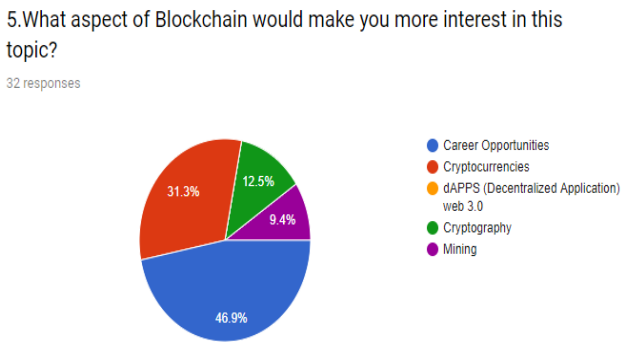

Figure 15: Blockchain area of interest

In summary, students' feedbacks are positive, and they are interested in learning more and love to work as blockchain developers. Lacking proper training materials are key to this trend.

Currently, blockchain technology is safe, reliable and secure technology. With many enthusiasts about the implementation for blockchain technology, however, large number of students' and future IT professional are unaware of blockchain and its use cases. Currently, there are not many blockchain hands-on labs. Thus, we introduce a comprehensive hands-on topics and labs that will enhance student's knowledge of blockchain and blockchain development. According to students feedback they are enthusiastic about blockchain and the career opportunities that it offers. We described a series of hands-on labs, power point presentation and articles.

7. CONCLUSION

To summarize, our objective is to increase our undergraduate security – level students the future IT professional awareness and prepare them for the emergent of the blockchain revolution and Web 3.0. Students overwhelmingly expressed they would like to learn more about blockchain technology to enhance their career prospect opportunities. Thus, creating a comprehensive hands-on lab will bridge the gaps and between rapid advancement of technology and the classroom.

Under our framework, we will develop various hands-on related blockchains. SEED project [25] is good example for us to follow.

REFERENCES

"2018 Market survey report for (non-financial) application of Blockchain in China," PwC China, Dec 2017. Available: https://www.pwccn.com/en/riskassurance/2018-china-blockchain-survery-report-en.pdf.

Firth, D. (2018). Teaching Blockchain in the MIS Curriculum.

Gaur, N.,et. al. (2018). Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. Packt Publishing Ltd.

Reidy, k. M. (2018). Beyond bitcoin: emerging applications for blockchain technology.

Nakamoto s. Bitcoin: a peer-to-peer electronic cash system[j]. 2008.

Phan The Duy, D. T.-H. (2018, December 06). A survey on opportunities and challenges of Blockchain. Danang City, Viet NAM.

Firth, D. R. (2016, December). Teaching Blockchain in the MIS Curriculum. Montana, Montana.

[8] Kevin Delmolino, M. A. (2015, November 18). Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. College Park, Maryland.

[9] Thai, P., Njilla, L., Duong, T., Fan, L., & Zhou, H.-S. (2018, November 05 - 07). A Generic Paradigm for Blockchain Design. New York, NY.

[10] Halaburda, H. (2017). Blockchain Revolution without blockchain? Viewpoints, 27-29.

[11] Hari, A., & Lakshman, T. (2016). The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet. COMM ACM SIGCOMM (pp. 204-210). New York: ACM.

[12] Blockchain, H. t. (2018, September 20). blog:how to develop a career in blockchain. Retrieved from ZaranTech: https://www.zarantech.com/blog/how-to-develop-a-career-in-blockchain/

[13] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza. Snarks for C: verifying program executions succinctly and in zero knowledge. In CRYPTO, 2013.

[14] E. Ben-Sasson, A. Chiesa, M. Green, E. Tromer, and M. Virza. Secure sampling of public parameters for succinct zero knowledge proofs. In S&P, 2015.

[15] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza. Scalable zero knowledge via cycles of elliptic curves. In CRYPTO, 2014.

[16] BUTERIN, V. (2016). Ethereum Foundation. Retrieved from Ethereum Homestead Documentation: http://www.ethdocs.org/en/latest/

[17] I. Bentov and R. Kumaresan. How to Use Bitcoin to Design Fair Protocols. In CRYPTO, 2014.

[18] (n.d.). Retrieved from DOCUMENTATION: https://truffleframework.com/docs

[19] D. Bogdanov, S. Laur, and J. Willemson. Sharemind: A Framework for Fast Privacy-Preserving Computations. In ESORICS. 2008.

[20] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In S&P, 2015.

[21] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In FOCS, 2001.

[22] R. Canetti. Universally composable signature, certification, and authentication. In CSF, 2004.

[23] R. Canetti, Y. Dodis, R. Pass, and S. Walfish. Universally composable security with global setup. In TCC. 2007.

[24] R. Cleve. Limits on the security of coin flips when half the processors are faulty. In STOC, 1986.

[25] Du, W. (2011). SEED: hands-on lab exercises for computer security education. IEEE Security & Privacy, 9(5), 70-73.

