International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

SHA 512 Enhanced Secure Hash Decentralized Response System

Santosh P. Kale[1], Prof. Pankaj D. Khambre[2], Aditya A. Kavitake[3], Aditya B. Tayade[4], Prof. Yamini Warke[5], Devesh P. Mahajan[6]

[1,2,3,4,5,6]Dept. of CSE, MMIT College Lohegaon, Pune

ABSTRACT

Today a very huge lack of confidence about the current EVM/ballot response system like voting has made voting response collection in any democratic country very condemnatory. People have watched their fundamental rights which are being violated. On the other hand the other digital voting systems are also in danger due to a minimal of transparency. Most of the traditional response systems are not clear enough so as to meet today's requirements; this crucial reason makes it very sweaty for the government to come up with voters' trust. The motive behind the downfall of the traditional and current cyber voting system is that it can be easily compromised due to centralized network. The primary objective here is to counter the issues of the traditional digital voting and such response systems, which has any type of mistrust or inequality during the process of accepting responses through response systems like voting. Blockchain technology can be used in such response systems like voting to have a fair response system and reduce wrongdoing. The current physical response systems like voting have many downs in it as well as the digital voting systems are not up to the mark to be implemented on a huge scale. Such all problems raises the need for a solution to secure the democratic rights of the people. This article put-ups a framework based on up-to-date blockchain algorithm technology that provides high clarity and reliability of the system to construct a healthy relationship between response systems and election authorities. The insisted software provides a framework that can be implemented in real world to conduct voting like procedures digitally through blockchain rather than involving any physical polling stations and centralized ledger. Our proposed framework provides an extendible hashing, by using the latest consensus algorithms. The Secure Hash Algorithms applied in the voting system along with Chain Security makes the response systems more secure. Distributed ledger contracts also provide a protected connection between the user and the consensus network while running a transaction in the chain. The security of the blockchain based response system has also been discussed. In Addition to this, encryption of responses using cryptographic hash functions and prevention of exploitation attacks about 51% on the blockchain has also been elaborated. Also, the procedure for carrying out blockchain transactions during the process of response collection has been elaborated using Blockchain. Finally, the throughput performance evaluation of the proposed system shows that such a system can be deployed in a large-scale real time population.

Keywords: Blockchain, Smart Contracts, Cryptography, Elliptic Curve Cryptography, Decentralization, Hyperledger, Tokenization, Immutable Ledger, Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Transparent Wallets, Zero-Knowledge Proofs, Multi-Signature, Wall Security,

Token Privacy-Preserving Technologies, Post-election Verification, Chain Interoperability Third-Party Auditors

INTRODUCTION

We know that the term response system is understood to be an interactive technology. This form of technology can be used during face-to-face instruction, this instruction allows instructors to poll people. The electronic response system is a way in which responses casted by people of a specific electronic medium can be extracted, manipulated and stored electronically. Our project to be developed will highlight on exchanging the current paper based response system that is being used by the University of Westminster Student Union into an electronic system. The current response system being used by the authorities is suffering from a centralized management system hence is not convenient for most large scale applications. Our response system to be developed will cover such issues by providing people with the capability of casting their responses for their chosen candidates through an WWW enabled computer.Our project will enlight on the current response method like voting which is being used by the govt authorities, and find a path in which the system can be modeled with the modern blockchain response system to be implemented. This system will thoroughly implement different response mechanisms used for casting responses Our system will be built to have strict hash function security features. These security features will be deployed from the phase of user login into the response system, to casting their responses for their chosen representative to the phase of their exit from the system. Our system will have secured hashed infrastructure preventing the person from casting responses more than once .Our system to be implemented needs to look after the issues including transparency requirements of a response being casted over the internet.

PROBLEM STATEMENT

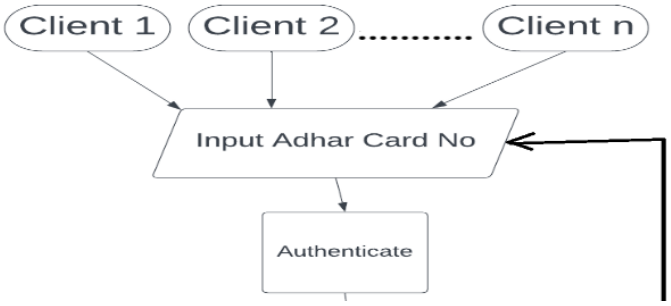
Our response system will be taking manually filled voterID details as input feedings, these input feedings will thereafter processed using hashing mechanisms using hash algorithms of the hash family.

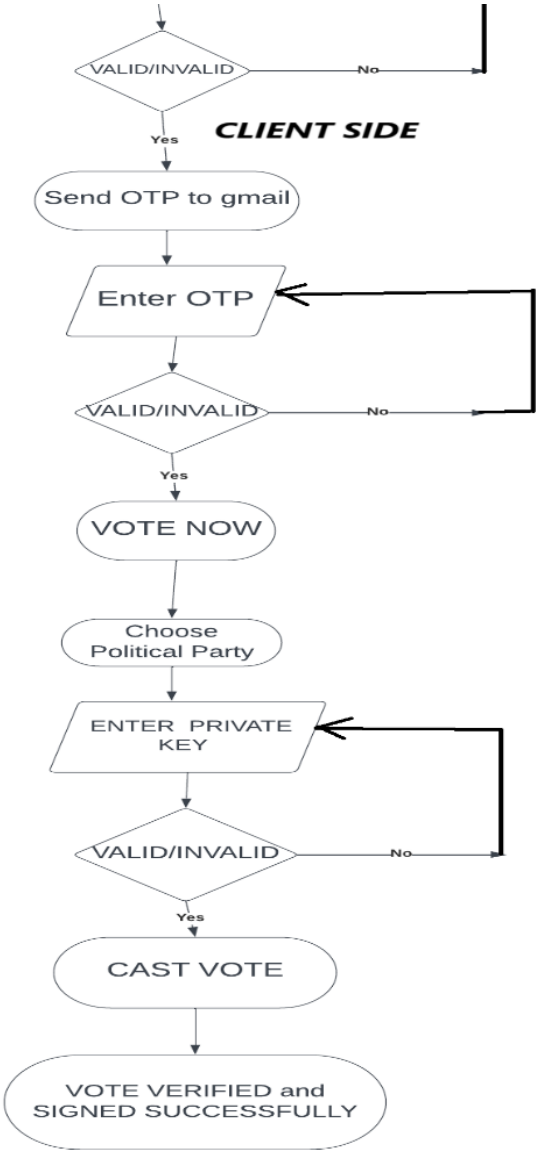
The inputs feeding will undergo hashing mechanism rounds like Secure Hash - 512, the final hash digest will consist of length occupying 512 bits. This hash digest will then after stored in decentralized database by maintaining the consensus layer.

Once input is stored in decentralized database, the response system will share the same security hash key to response caster's mail as a confirmation of his/her casted response for example - the Vote.

SYSTEM ARCHITECTURE

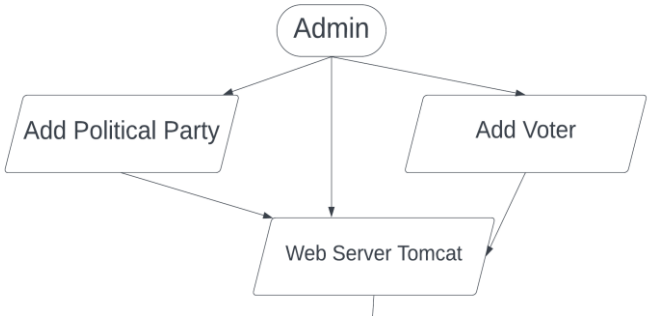
Client Perspective

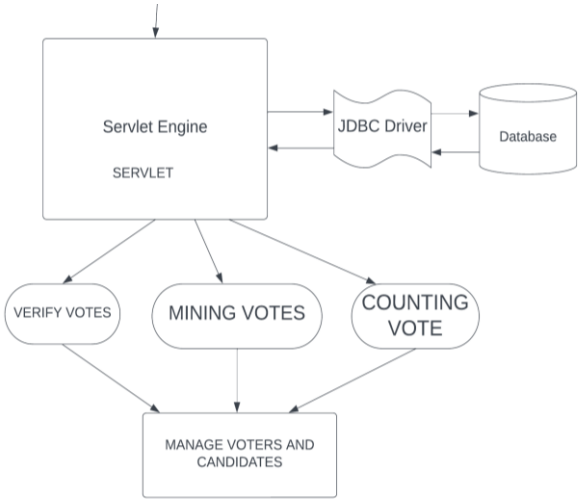




The authentication and voting process involves clients (Client 1, Client 2, Client n) inputting their Adhar Card No for verification. The system then undergoes an authentication process, with a subsequent validation check for Adhar Card No ("VALIOINVALID"). If validated, an OTP is sent to the client's Gmail for further verification. Clients enter the OTP, and the system performs a validation check ("VALIOVINVALID")

Admin Perspective





Voter

Voters are people who have the legal right to vote in elections, or people who are voting in a particular election. A voter, simply put, is either someone who's eligible to vote in an election or someone who actually does vote. According to definition, a participant addresses voters, along with how they are communicating to a group of people, also how they are trying to divert that group's attention towards sanctioning a response for them. When participants pass a rule or give a sanction letter to a school budget, that means that the majority of participants who casted their responses and made those choices.

Administrator

Administration here is done by maintaining Consensus Layer. By consensus, we mean that a general agreement has been reached. Consider a group of people going to the cinema. Let's consider a disapproval of a proposed choice of visualizations, then in such a case a blockchain consensus layer interrupts. Also if a disagreement emerges, the participant's block must have the right to decide which visualization to see. Worst case witnesses the block will ultimately scatter.

Considering the Ethereum currency, procedure is finalized along with touching consensus layer indicates that as low as 66.0001% of the points on the framework connectivities accepts on the global level of the network

Workflow Of Proposed Model

The voter after completing the verification is registered into the Voting Management System. A single chain system is implemented on the blockchain. The national database of the country is also integrated with the system to keep the voter's voting integrity. For every vote, a transaction is being generated against the voter's National ID. The transaction is then mined by the minors and saved in the blockchain. When the voter casts the vote, his Vote Coin in his/her wallet is also being utilized. The voter cannot cast another vote after one vote coin is utilized. As the voter will sign-in through his/her credentials then the voter has been redirected to the election interface where all the candidates who are contesting in his constituency are shown to the voter. Upon the voter's request to cast vote. The voter cannot cast another vote after one vote coin is utilized. As the voter will sign-in through his/her credentials then the voter has been redirected to the election interface where all the candidates who are contesting in his constituency are shown to the voter. Upon the voter's request to cast vote, VMS verifies the voting status of the voter from the blockchain

by checking all transactions hash that already exists against his/her computerized National ID. If a transaction hash is found against the voter's computerized National ID then VMS declined the request and logout the voter from the system. If a voter has not voted yet, the request is transferred to the miner to add the node. The voter selects the desired candidate and casts his vote. The transaction is monitored with the help of a transaction hash and carried out by the miner Voters must have access to any smartphone or web browser to take part in voting. The voter's interface would be provided in multi-languages to make it easy to use for all users. The proposed system can contain a large number of voters at the time of voting. A decentralized blockchain system enables a voter to vote from any part of the world. A person can take part in voting from anywhere

Web Server Tomcat

Tomcat is an open-source web server and servlet. According to the Apache Software Foundation the development of Web Server Tomcat has been accomplished by them. Tomcat is being utilized till date for hosting Java-based applications over wireless world wide web. Tomcat has been constructed on the platform of Java technologies and implements the Java-Servlet and JavaServer-Pages [("JSP")] functionalities. Apache Tomcat behaves like-bridge amongst the wireless world servers and Java-based applications, guiding further towards the execution of dynamic content and processing participants requests.

JDBC Driver

Java Database Connectivity drivers are nothing but participant side functionalities (i.e run on the participants computer, and not on the web) that transforms requests from Java procedures to a systematic order that the Database Management System can understand. There are 4 types of Java Database Connectivities:-

1. "JDBC-ODBC bridge driver"
2. "Native-API driver"
3. "Network Protocol driver"
4. "Thin driver"

Database

A database is an organized collection of structured information, or data, typically stored electronically in a computer system. We can say that a DB is commonly manipulated by a "database-management-system" (DBMS). Combinedly the meaningful information and the database system, together with applications that are clubbed with others, are directed to a database system, often shortened to just a database.

["Java Database Connectivity (JDBC)"] is a form that is also expressed as an application programming interface!

For the sake of the programming language Java, that is supposed to define how a participant may enter into boundaries of any kind of structural information, specifically relational structural information. It is considered a contribution of the Java Standard Edition platform which has come from "Oracle-Corp". Also it behaves as a standard in-between layer functionality between java apps and its DB.

The Java Database Connectivity categories are included in the Javac Package "java.sql and javax.sql".

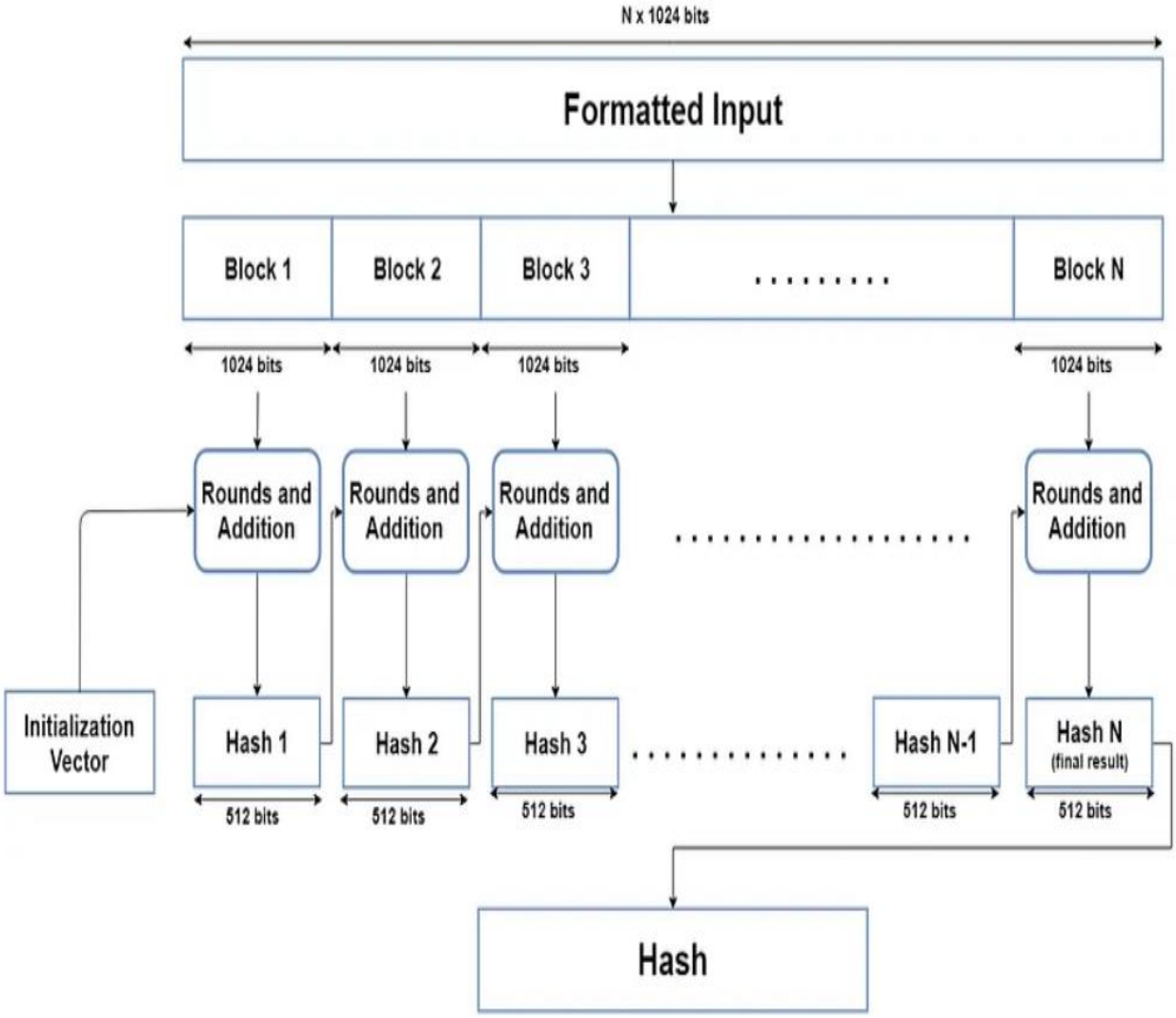
Also the JDBC gives a helping hand for you to write Javac apps that tend to manipulate following three programming activities:

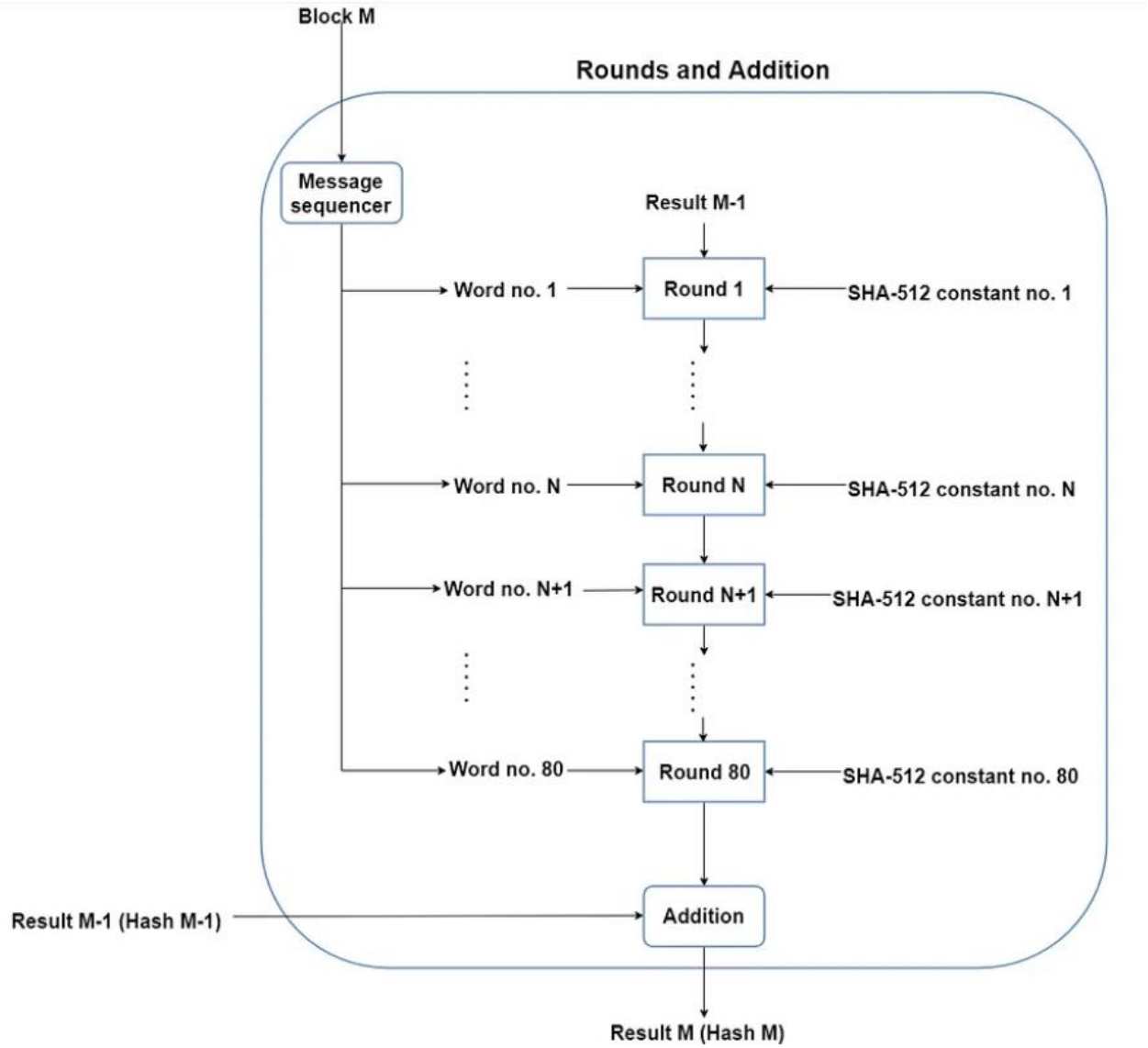
Category 1) We need to connect to the info source, like a DB.
Category 2) Thereafter we need to send doubts and change necessary statements to the DB
Category 3) Followed by extraction and procedure which gives the results retrieved from the DB as feedback to your question

Servlet

A servlet is a Java programming language class that is used to extend the capabilities of servers which in turn hosts the apps gained by means of a claim-feedback programming structure. Even though Java servlets can behave to any type of request, they are certainly utilized in order to enlarge the apps energized by wireless world wide web. In such cases of special apps, the Java-Servlet version defines HyperText transfer specific servlet categories.

MATHEMATICAL MODEL





CONCLUSION

The research work has successfully validated the drawbacks of earlier-developed blockchain algorithm visualizers and how to work around them to make them better. In order to successfully make the desired goals and objectives, we have developed a dedicated system for our secure hash algorithms. This will be very helpful for students, teachers and corporate trainers for a better understanding of decentralized algorithms. Thus, lubricating the way for making feasible and critical response systems is our sole impulse to undertake this project

FUTURE SCOPE

Also, in future such systems would be implemented in real life scenarios like Land Registry, Defense Mechanisms and such critical Govt activities.

REFERENCES

1. S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

2. S. S. Hossain, S. A. Arani, M. T. Rahman, T. Bhuiyan, D. Alam, and M. Zaman, ‘‘E-voting system using blockchain technology,’’ in Proc. 2nd Int. Conf. Blockchain Technology. Appl., Dec. 2019, pp. 113–117, doi: 10.1145/3376044.3376062.
3. B. Shahzad and J. Crowcroft, ‘‘Trustworthy electronic voting using adjusted blockchain technology,’’ IEEE Access, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.
4. A. Paulin and T. Welzer, ‘‘A universal system for fair non-repudiable certified e-mail without a trusted third party,’’ Comput. Secur., vol. 32, pp. 207–218, Feb. 2013.
5. H. Pagnia and F. C. Gärtner, ‘‘On the impossibility of fair exchange without a trusted third party,’’ Darmstadt Univ. Technol.-Karolinenplatz, Darmstadt, Germany, Tech. Rep. TUD-BS-1999-02, 1999. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.44.7863
6. F. P. Hjálmarsson, G. K. Hreiòarsson, M. Hamdaqa, and G. Hjálmtýsson,‘‘Blockchain-based E-Voting system,’’ in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 983–986.
7. M. S. Farooq, M. Khan, and A. Abid, ‘‘A framework to make charity collection transparent and auditable using blockchain technology,’’ Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106588, doi:10.1016/j.compeleceng.2020.106588.
8. N. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, ‘‘Blockchain Technology—Beyond bitcoin,’’ Sutardja Center Entrepreneurship Technol., Univ. California, Berkeley, CA, USA, Tech. Rep., Oct. 2015