Let Upr be the private key of the user, Ubio the biometric information collected from the user.

H is a hashing function that hashes the Ubio.

1: Procedure AUTHENTICATE()

2: Let Upr <- User private key, Ubio<- User Biometric information

3: DbHash<- DBACCESS(Upr)

4:Hbio<-H(Ubio)

5: if Hbio=DbHash then

6: return true

7: else

8: return false

9: End Procedure

Hkey is the hashed value of the user’s private key. Vdb is the voter database that stores the hashed biometric information and user’s private key as key value pairs. DkHash stores the hashed biometric information of users.

1: Procedure DBACCESS(Upr)

2: DbHash<-0

3:Hkey<-H(Upr)

4: if Hkey in Vdb(DkHash) then

5: return DbHash of Vdb(DkHash)

6: else

7: DbHash<-0

8: End Procedure

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%2345678901234567890123456789012345678901234567890123456789012345678901234567890

% 1 2 3 4 5 6 7 8

\documentclass[letterpaper, 10 pt, conference]{ieeeconf} % Comment this line out

% if you need a4paper

%\documentclass[a4paper, 10pt, conference]{ieeeconf} % Use this line for a4

% paper

\IEEEoverridecommandlockouts % This command is only

% needed if you want to

% use the \thanks command

\overrideIEEEmargins

% See the \addtolength command later in the file to balance the column lengths

% on the last page of the document

% The following packages can be found on http:\\www.ctan.org

%\usepackage{graphics} % for pdf, bitmapped graphics files

%\usepackage{epsfig} % for postscript graphics files

%\usepackage{mathptmx} % assumes new font selection scheme installed

%\usepackage{times} % assumes new font selection scheme installed

%\usepackage{amsmath} % assumes amsmath package installed

%\usepackage{amssymb} % assumes amsmath package installed

\usepackage{algorithmic}

\usepackage{algorithm}

\title{\LARGE \bf

Any Time Voting System using Blockchain

}

%\author{ \parbox{3 in}{\centering Huibert Kwakernaak\*

% \thanks{\*Use the $\backslash$thanks command to put information here}\\

% Faculty of Electrical Engineering, Mathematics and Computer Science\\

% University of Twente\\

% 7500 AE Enschede, The Netherlands\\

% {\tt\small h.kwakernaak@autsubmit.com}}

% \hspace\*{ 0.5 in}

% \parbox{3 in}{ \centering Pradeep Misra\*\*

% \thanks{\*\*The footnote marks may be inserted manually}\\

% Department of Electrical Engineering \\

% Wright State University\\

% Dayton, OH 45435, USA\\

% {\tt\small pmisra@cs.wright.edu}}

%}

\author{Nandakishore VV$^{1}$ and Amal C Saji$^{2}$% <-this % stops a space

\thanks{\*This work was not supported by any organization}% <-this % stops a space

\thanks{$^{1}$H. Kwakernaak is with Faculty of Electrical Engineering, Mathematics and Computer Science,

University of Twente, 7500 AE Enschede, The Netherlands

{\tt\small h.kwakernaak at papercept.net}}%

\thanks{$^{2}$P. Misra is with the Department of Electrical Engineering, Wright State University,

Dayton, OH 45435, USA

{\tt\small p.misra at ieee.org}}%

}

\begin{document}

\maketitle

\thispagestyle{empty}

\pagestyle{empty}

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

\begin{abstract}

Any Time Voting system employs blockchain technology to allow voters to cast their valuable votes securely,in a hassle free fashion, with assurance that electoral fraud is impossible.

\end{abstract}

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

\section{INTRODUCTION}

Election is a huge administrational process that takes up a lot of time, effort and monetary resources of a state. In a country like India, where assembly elections are not held uniformly, the entire voting process demands a large scale financial need, workforce and infrastructure. Despite all the shortcomings it has, a lot of countries still follow the traditional paper ballot system, but India has adopted Electronic Voting Machines from 1999 and by 2017, EVMs have replaced paper ballots all over the country. The EVMs, even though are one of the most secure voting systems, yet are not fully foolproof.

\section{Present day scenario}

The present day voting systems, be it paper ballots or EVMs, require armed forces guarding them to ensure the security of the votes casted. The election period witnesses booth capturing to confiscate ballots/EVMs, masquerading as someone else to perform fraudulent voting and many such malpractices. Elections also demand a huge number of government officials to work overtime to ensure everything is carried out as required. All these facts pose a threat to the voters and the votes casted alike.

\section{Why Blockchain?}

Blockchain is a decentralized distributed public ledgering system. It can be used for secure monetary transactions, data storage and retrieval. The problems of the now prevalent EVMs can be overcome if we implement voting using blockchain technology. Blockchain offers a plethora of essential security features to carry out voting in the most secure and transparent manner. It is the most secure system available now to prevent fraudulent voters and multiple voting. This problem can be solved successfully only by using blockchain as all the other implementation techniques would use a traditional database which could be compromised.\\

\hspace{1cm} Blockchain is a disruptive technology and if e-voting is enabled using blockchain, it would disrupt the traditional election process and the working of the election commission in the country. The entire process would become simple and less complicated. The data saved in the blockchain is immutable, unlike the conventional servers. The overall expense required for the entire election process across the country could be reduced and there is no need to give a public holiday and reduce the productivity of the state on election day. Moreover, there is no need of intense security at the ATVs as votes can’t be manipulated or destroyed if the ATVs are destroyed. The counting process and result declaration is made hassle free and simple as votes are counted as they are being casted. This also follows green protocol, and is environment friendly.

\section{Implementation}

\subsection{Voter Database}

The electoral roll database can be maintained in a blockchain. The presently available biometric information from the adhaar database is taken and encrypted using SHA256 algorithm and a specific key is generated for each citizen. This cryptographically secure key is now stored in a blockchain.

From this database the citizen who meet the criteria for casting a vote are assigned with token values set as ‘true’, and are assigned with a private key, by the election commissioner, before each election is declared.

The admin will add the candidates after the nomination scrutiny and they are given a token, a private key, and wallet value initially set as zero.

\subsection{Any Time Voting}

The Election Commissioner decides a period of time when votes can be casted, ie; election process is not confined to a single day. Votes can be casted by eligible voters any time, using ATVs.

Any Time Voting systems (ATV) is a specially designed online platform which would be installed in multiple places in all constituencies. ATVs are equipped with biometric sensors which would be used to identify voters. The biometric information is collected from the ATV and encrypted using SHA256. This key is checked against the keys saved in the Voter database to identify voters. If the key is matched, the voting screen is enabled and votes can be casted.

\subsection{Voting process}

A voter clicks on the name of the candidate and then, the token of the voter is set as ‘false’, the candidate will have a token increased in their wallet and simultaneously, the casted vote is displayed on screen.

\subsection{Result Declaration}

Once the election period has ended, the admin(CEC) can allow the privilege to all the voters to view the number of votes secured by each candidate.

\section{Technical Implementation}

\textbf{Smart Contract:} A computer program that controls the voting process. Each vote is considered as a transaction and each transaction is recorded into the blockchain based on this Smart Contract.

The contract is written using Solidity and compiled using pragma solidity \^0.4.0 \\

\textbf{Ethereum Blockchain:} Voting is a token based transaction, and we prefer to implement the system using Ethereum, which was developed by Vitalik Buterin. \\

\textbf{NodeJS:} The front end of the application is developed using NodeJS since it is fast and dynamic.\\

\textbf{Ganche-cli:} The personal blockchain for ethereum development

\begin{algorithm}

\caption{Authenticate()}\label{alg:euclid}

\begin{enumerate}

\item Let Upr $\leftarrow$ User private key, Ubio $\leftarrow$ User Biometric information

\item DbHash $\leftarrow$ DBACCESS(Upr)

\item Hbio $\leftarrow$ H(Ubio)

\item \textbf{if} Hbio = DbHash \textbf{then}

\item \hspace{0.3cm} return true

\item \textbf{else}

\item \hspace{0.3cm} return false

\item End procedure

\end{enumerate}

\end{algorithm}

\begin{algorithm}

\caption{Authenticate()}\label{alg:euclid1}

\begin{enumerate}

\item DbHash $\leftarrow$ 0

\item Hkey $\leftarrow$ H(Upr)

\item \textbf{if} Hkey in Vdb(DkHash) \textbf{then}

\item \hspace{0.3cm} return DbHash of Vdb(DkHash)

\item \textbf{else}

\item \hspace{0.3cm} DbHash $\leftarrow$0

\item End procedure

\end{enumerate}

\end{algorithm}

\section{Future Scope, Challenges}

The future scope of blockchain enabled E-voting is extensive. Instead of using public ATVs, voting could be carried out using mobile phones having an internet connection. The adhaar model blockchain database could be extended to make it liked with all the personal details and thereby making the financial transactions easy and traceable. It will also make the candidate nomination scrutiny possible with one click. Administrative level implementation of the blockchain would make the working of the government transparent than ever before.

\\

Blockchain enabled E-voting is has the potential to disrupt the whole election process and it would be challenging to implement as it is a must to win the confidence of the authorities and the general public to implement the system. Also, since it would potentially result in losing jobs/ Job posts, some people would be against this system.

\\

\subsection{Units}

\begin{itemize}

\item Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as Ò3.5-inch disk driveÓ.

\item Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.

\item Do not mix complete spellings and abbreviations of units: ÒWb/m2Ó or Òwebers per square meterÓ, not Òwebers/m2Ó. Spell out units when they appear in text: Ò. . . a few henriesÓ, not Ò. . . a few HÓ.

\item Use a zero before decimal points: Ò0.25Ó, not Ò.25Ó. Use Òcm3Ó, not ÒccÓ. (bullet list)

\end{itemize}

\subsection{Equations}

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled. Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in

$$

\alpha + \beta = \chi \eqno{(1)}

$$

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use Ò(1)Ó, not ÒEq. (1)Ó or Òequation (1)Ó, except at the beginning of a sentence: ÒEquation (1) is . . .Ó

\subsection{Some Common Mistakes}

\begin{itemize}

\item The word ÒdataÓ is plural, not singular.

\item The subscript for the permeability of vacuum ?0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter ÒoÓ.

\item In American English, commas, semi-/colons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)

\item A graph within a graph is an ÒinsetÓ, not an ÒinsertÓ. The word alternatively is preferred to the word ÒalternatelyÓ (unless you really mean something that alternates).

\item Do not use the word ÒessentiallyÓ to mean ÒapproximatelyÓ or ÒeffectivelyÓ.

\item In your paper title, if the words Òthat usesÓ can accurately replace the word ÒusingÓ, capitalize the ÒuÓ; if not, keep using lower-cased.

\item Be aware of the different meanings of the homophones ÒaffectÓ and ÒeffectÓ, ÒcomplementÓ and ÒcomplimentÓ, ÒdiscreetÓ and ÒdiscreteÓ, ÒprincipalÓ and ÒprincipleÓ.

\item Do not confuse ÒimplyÓ and ÒinferÓ.

\item The prefix ÒnonÓ is not a word; it should be joined to the word it modifies, usually without a hyphen.

\item There is no period after the ÒetÓ in the Latin abbreviation Òet al.Ó.

\item The abbreviation Òi.e.Ó means Òthat isÓ, and the abbreviation Òe.g.Ó means Òfor exampleÓ.

\end{itemize}

\section{USING THE TEMPLATE}

Use this sample document as your LaTeX source file to create your document. Save this file as {\bf root.tex}. You have to make sure to use the cls file that came with this distribution. If you use a different style file, you cannot expect to get required margins. Note also that when you are creating your out PDF file, the source file is only part of the equation. {\it Your \TeX\ $\rightarrow$ PDF filter determines the output file size. Even if you make all the specifications to output a letter file in the source - if you filter is set to produce A4, you will only get A4 output. }

It is impossible to account for all possible situation, one would encounter using \TeX. If you are using multiple \TeX\ files you must make sure that the ``MAIN`` source file is called root.tex - this is particularly important if your conference is using PaperPlaza's built in \TeX\ to PDF conversion tool.

\subsection{Headings, etc}

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named ÒHeading 1Ó, ÒHeading 2Ó, ÒHeading 3Ó, and ÒHeading 4Ó are prescribed.

\subsection{Figures and Tables}

Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation ÒFig. 1Ó, even at the beginning of a sentence.

\begin{table}[h]

\caption{An Example of a Table}

\label{table\_example}

\begin{center}

\begin{tabular}{|c||c|}

\hline

One & Two\\

\hline

Three & Four\\

\hline

\end{tabular}

\end{center}

\end{table}

\begin{figure}[thpb]

\centering

\framebox{\parbox{3in}{We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an document, this method is somewhat more stable than directly inserting a picture.

}}

%\includegraphics[scale=1.0]{figurefile}

\caption{Inductance of oscillation winding on amorphous

magnetic core versus DC bias magnetic field}

\label{figurelabel}

\end{figure}

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity ÒMagnetizationÓ, or ÒMagnetization, MÓ, not just ÒMÓ. If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write ÒMagnetization (A/m)Ó or ÒMagnetization {A[m(1)]}Ó, not just ÒA/mÓ. Do not label axes with a ratio of quantities and units. For example, write ÒTemperature (K)Ó, not ÒTemperature/K.Ó

\section{CONCLUSIONS}

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

\addtolength{\textheight}{-12cm} % This command serves to balance the column lengths

% on the last page of the document manually. It shortens

% the textheight of the last page by a suitable amount.

% This command does not take effect until the next page

% so it should come on the page before the last. Make

% sure that you do not shorten the textheight too much.

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

\section\*{APPENDIX}

Appendixes should appear before the acknowledgment.

\section\*{ACKNOWLEDGMENT}

The preferred spelling of the word ÒacknowledgmentÓ in America is without an ÒeÓ after the ÒgÓ. Avoid the stilted expression, ÒOne of us (R. B. G.) thanks . . .Ó Instead, try ÒR. B. G. thanksÓ. Put sponsor acknowledgments in the unnumbered footnote on the first page.

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

References are important to the reader; therefore, each citation must be complete and correct. If at all possible, references should be commonly available publications.

\begin{thebibliography}{99}

\bibitem{c1} G. O. Young, ÒSynthetic structure of industrial plastics (Book style with paper title and editor),Ó in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15Ð64.

\bibitem{c2} W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123Ð135.

\bibitem{c3} H. Poor, An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.

\bibitem{c4} B. Smith, ÒAn approach to graphs of linear forms (Unpublished work style),Ó unpublished.

\bibitem{c5} E. H. Miller, ÒA note on reflector arrays (Periodical styleÑAccepted for publication),Ó IEEE Trans. Antennas Propagat., to be publised.

\bibitem{c6} J. Wang, ÒFundamentals of erbium-doped fiber amplifiers arrays (Periodical styleÑSubmitted for publication),Ó IEEE J. Quantum Electron., submitted for publication.

\bibitem{c7} C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

\bibitem{c8} Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, ÒElectron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style),Ó IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740Ð741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].

\bibitem{c9} M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.

\bibitem{c10} J. U. Duncombe, ÒInfrared navigationÑPart I: An assessment of feasibility (Periodical style),Ó IEEE Trans. Electron Devices, vol. ED-11, pp. 34Ð39, Jan. 1959.

\bibitem{c11} S. Chen, B. Mulgrew, and P. M. Grant, ÒA clustering technique for digital communications channel equalization using radial basis function networks,Ó IEEE Trans. Neural Networks, vol. 4, pp. 570Ð578, July 1993.

\bibitem{c12} R. W. Lucky, ÒAutomatic equalization for digital communication,Ó Bell Syst. Tech. J., vol. 44, no. 4, pp. 547Ð588, Apr. 1965.

\bibitem{c13} S. P. Bingulac, ÒOn the compatibility of adaptive controllers (Published Conference Proceedings style),Ó in Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory, New York, 1994, pp. 8Ð16.

\bibitem{c14} G. R. Faulhaber, ÒDesign of service systems with priority reservation,Ó in Conf. Rec. 1995 IEEE Int. Conf. Communications, pp. 3Ð8.

\bibitem{c15} W. D. Doyle, ÒMagnetization reversal in films with biaxial anisotropy,Ó in 1987 Proc. INTERMAG Conf., pp. 2.2-1Ð2.2-6.

\bibitem{c16} G. W. Juette and L. E. Zeffanella, ÒRadio noise currents n short sections on bundle conductors (Presented Conference Paper style),Ó presented at the IEEE Summer power Meeting, Dallas, TX, June 22Ð27, 1990, Paper 90 SM 690-0 PWRS.

\bibitem{c17} J. G. Kreifeldt, ÒAn analysis of surface-detected EMG as an amplitude-modulated noise,Ó presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.

\bibitem{c18} J. Williams, ÒNarrow-band analyzer (Thesis or Dissertation style),Ó Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.

\bibitem{c19} N. Kawasaki, ÒParametric study of thermal and chemical nonequilibrium nozzle flow,Ó M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.

\bibitem{c20} J. P. Wilkinson, ÒNonlinear resonant circuit devices (Patent style),Ó U.S. Patent 3 624 12, July 16, 1990.

\end{thebibliography}

\end{document}