Journal of Advanced Research in Technology and Management Sciences (JARTMS)
Volume: 03 Issue: 04 ISSN: 2582-3078 July 2021
Available online at: http:// www.jartms.org

PERSONALISED SECURE E-IDENTITY CARD

V.V.Bhavani, K.Saisri, K.Naveen, M.Lalitha

***Abstract* :** The Block chain technology is new technology in digital platform for making transactions in decentralized manner. Blockchain is uses from last some year for bitcoin. over the last ten years, the record-keeping technology behind the Bitcoin network is blockchain. In blockchain Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. So, for identity card it is noticeable for security. If we implement blockchain technology for digital identity card it is very secure for the user. Identity card has personal information and some important information included. The identity card like Aadhar card, pan card, etc. have lot personal and important information, if we are not using securely then it will use for any illegal work which is harmful. Now these identity cards are stored in file with encryption method which will hacked by hackers. So we propose our system for e-identity card using blockchain technology. In our proposed system we are using blockchain and IPFS server which is immutable server which helps us to system will more secure. Once one transaction will done before the transaction the block will be created which is hash of information like date, time etc. and this block send to blockchain which will maintain all block. For implement the blockchain we will use Ethereum platform. This solution is secure and more trusted than traditional models.

Keywords: Blockchain, Identity card, IPFS server, Ethereum.

***** Correspondence Author
V.V.Bhavani, Assistant professor, Department of CSE,
UshaRama College of Engineering & Technology,
*Telaprolu***,**
Email: bhavani.vanukurus@gmail.com
K.Saisri ,*Department of CSE,*
UshaRama College of Engineering & Technology,
*Telaprolu***,**
Email: saisri.komma101@gmail.com
K.Naveen, *Department of CSE,*
UshaRama College of Engineering & Technology,
*Telaprolu***,**
Email: naveenkommuri9@gmail.com
M.Lalitha, *Department of CSE,*
UshaRama College of Engineering & Technology,
*Telaprolu***,**
Email: lalithamedasani28@gmail.com

1. INTRODUCTION

Blockchain is an emerging technology. In the recent years, it is not only used for financial use cases but also targeting almost every main field revolving around a human life. It can be business, health, gaming, government system, software/ electrical engineering and many more. Blockchain with personalized identity card: An approach for personalized identity system which is implemented by using blockchain and IPFS server is a new trend. Here, blockchain is used to store and retrieve the user ID. In order to contact the user, block can be retrieved and validated. Also, it is made secure and encrypted by implementing blockchain internally and externally; internally for accessing the list and externally to follow the identities. Blockchain is a decentralized and public ledger, which has introduced tremendous changes during last few years with applicability on financial use cases (e.g.Remittance) and nonfinancial use cases (e.g. documents). Blockchain-based systems provide the possibility for their users to insert their data in this distributed ledger. Users can trust the blockchain as it is leveraging consensus mechanisms to validate and gather the transactions in blocks. Along with distributed ledger, blockchain is also considered as an open ledger where online transactions are recorded and users can connect, send and verify their transactions. In other words, it is a digitized system in order to account the records. These records are set of mathematical rules which are used to stop the illegitimate intrusion. In order to include the data into the blockchain, users and nodes, which obtain an authorize-able address from blockchain, need to set up and communicate with smart contracts to send and retrieve data to/from blockchain. Moreover, blockchain works on the following rules; it represents decentralized, transparent and secure systems. Decentralized can also be called user to user or peer to peer operation without involving any central hub or authority. Transparency means the data is being embedded in the network publicly. Security offers the encryption technology supporting public and private keys. For example, in bitcoin, public key represents the user as address and private key act as a password to access the transaction. Here are few advantages and disadvantages regarding the blockchain. They are good to consider while developing blockchain based applications. It is also important to note that blockchain is facilitating the society/ human beings in many ways due to its advantages. Its disadvantages represent the lack of certain feature.

2. DESIGN

Meta Mask manages your Ethereum wallet, which contains your Ethers (or money), and allows you to send and receive Ethers through a dApp of interest. It is a pretty neat tool. Meta Mask is a simple browser extension that can run on many browsers. To install, you first visit the following link above and install the browser extension with the cute 3D fox image. Once installed, you see a fox on the right top of your browser. Now you can create a new Ethereum account to send and receive Ether and also to run dApps. After creating an account, you get a list of 12 words that can be used to retrieve your account when you forget your password. MAKE SURE to save this somewhere SAFE where no one can see. Now you have your own Ethereum wallet! You can use the main network, which will use real Ethers that cost REAL money, or try some dApps out on test networks such as **RINKEBY Test Network.**This site will give you free Ether to use on the RINKEBY Test Network. After clicking on request 1 free ether, you will find that your account now has 1 ether to use for any dApps! (Again, this is not real ether, think of it as monopoly money.) Now you can use this to run dApps that exist online. You can search for Ropsten dApps for the latest list of dApps to test. Once you feel pretty comfortable with dApps, you can then start running dApps on the main Ethereum network. You should be VERY careful that you are now spending real Ether. I will try to cover in a separate article some cool dApps that run on both types of network.I hope you now have a brief understanding of what distributed web, blockchain, Ethereum, and dApps are and how you can play around with them using MetaMask. Feel free to explore the large space of dApps and have fun, but most importantly be safe and responsible!In this we are using a test network called Rinkeby. Rinkeby is an Ethereum testnet (or test network). Testnets are typically used by developers to run "tests" for their application or software. Currency on test network are valueless. Rinkeby testnetwork, unlike Ethereum mainnet, is a proof-of-authority network, as opposed to a proof-of work network like Ethereum mainnet. Make it simple by create a script vim start.sh . Start command is geth --rinkeby --unlock 0x<your_public_address> --rpc --rpcport <anyport> . You can vim password input your password and add --password passwd to the startup script so that you won't need to input password each time The test-nets (such as Rinkeby) can be thought of as an alternate dimension for all intents and purposes. They are a place to run experiments without modifying the real Ethereum network. The ether there isn't worth anything, but your mistakes there also don't have consequences.To get ETH for Rinkeby Testnet (Closed Beta)

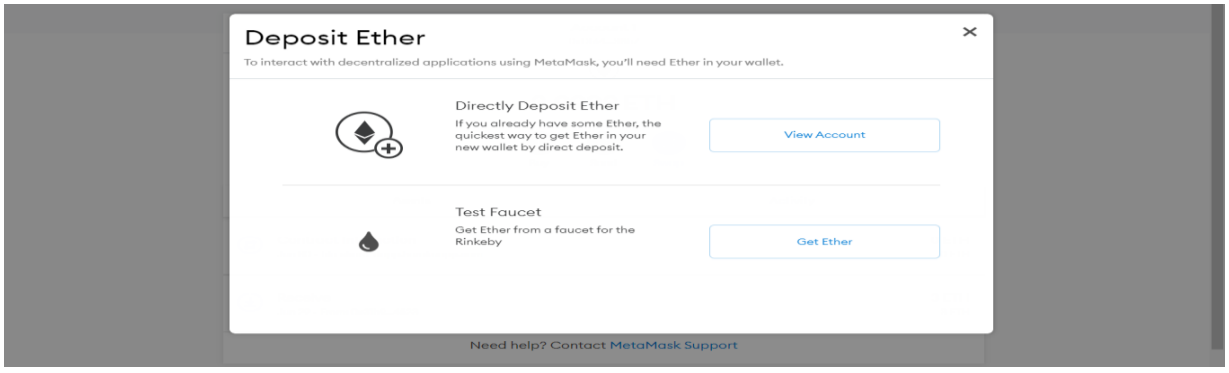

Figure : Get Ether

Go to https://www.rinkeby.io/#faucet
There are 3 options to get ETH on Rinkeby test net. (example with Facebook)
Facebook –Publish a new public post with your ETH address (Surrounding text does not matter) and paste the posts URL into the above input box.
. Click **Give me Ether** and select the length of time and amount of ether you would like. Once you see the Ether in your metamask wallet (make sure you have selected Rinkeby Testnet and not Ethereum Mainnet) you can now send the ether to your in-game MOBOX wallet.
a) Click on the **wallet** and select **deposit**
Copy the ETH address from the pop-up box and past it into your metamask address. Enter the amount you would like to send to your MOBOX wallet and confirm the transaction
5. You will then see the funds show up in your MOBOX wallet. Now you can hire all the talent you want!

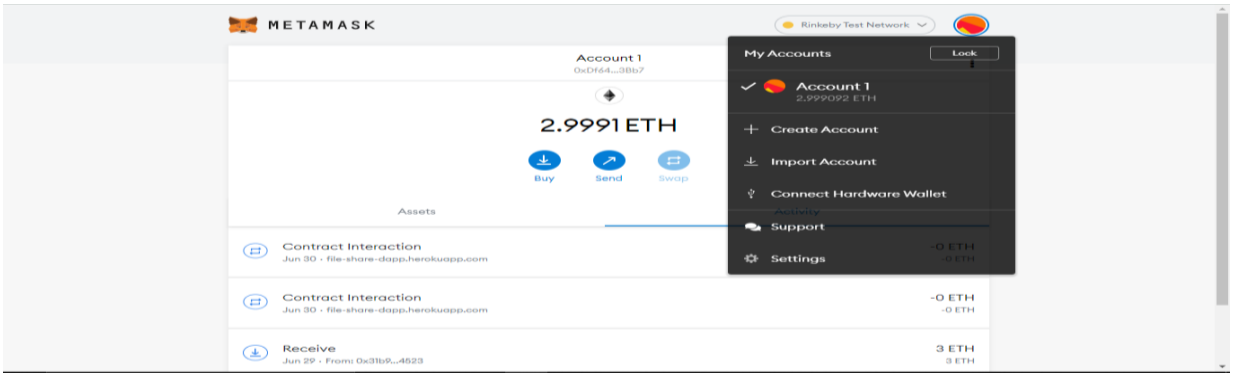

Figure : Wallet

3. ANALYSIS

In the proposed system, blockchain will be implemented by IPFS (InterPlanetary File System) which is an immutable server. It will help to make the system more secure. Users will first have to register in this system. Every user will have a personalized unique password and to add more protection will also have a biometric scanner to login. After successful login, the user will be able to upload documents. In the process of uploading the documents, the system will first encrypt the files containing the documents and the encrypted file will be uploaded to ipfs server. When the file is getting uploaded, it will be stored as a block in the blockchain server. At the same time the transaction hash will be maintained by ethereum. When the document is uploaded successfully it will be stored as a block in the blockchain. Similarly for retrieval of the documents, the user will first have to login. The system will display the documents already uploaded by the user. The user can download the required document by clicking on the download button. The block containing the document will get downloaded. As the document is stored in encrypted format, first it will be decrypted and then would be displayed to the user. As the designed system uses IPFS which is an immutable server, once a document is uploaded, it would be securely stored forever. It cannot be deleted even by the user.

4. RESULTS

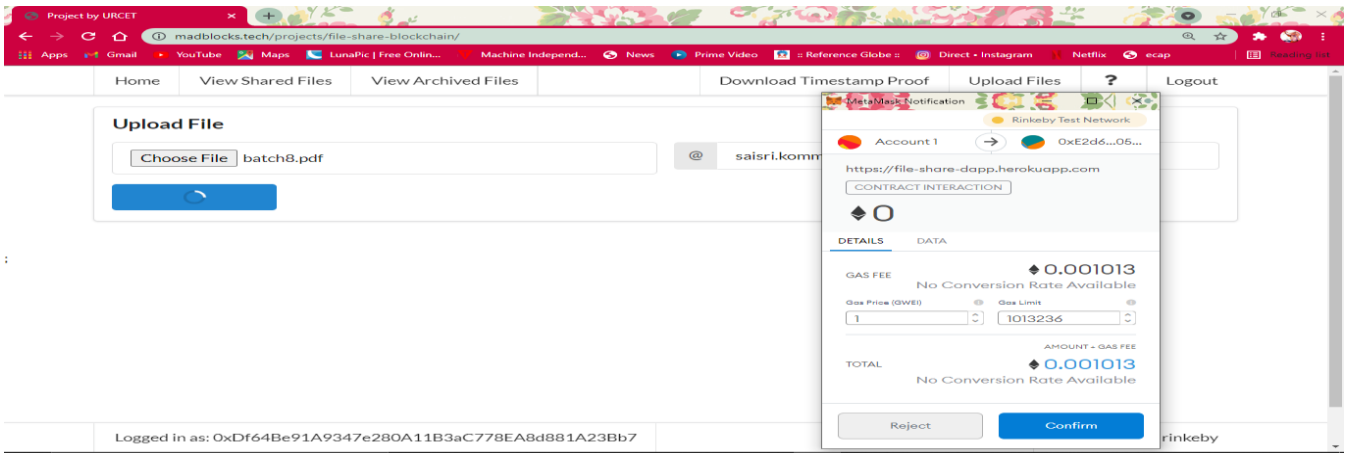

Figure : Upload to IPFS

Journal of Advanced Research in Technology and Management Sciences (JARTMS)
Volume: 03 Issue: 04 ISSN: 2582-3078 July 2021
Available online at: http:// www.jartms.org

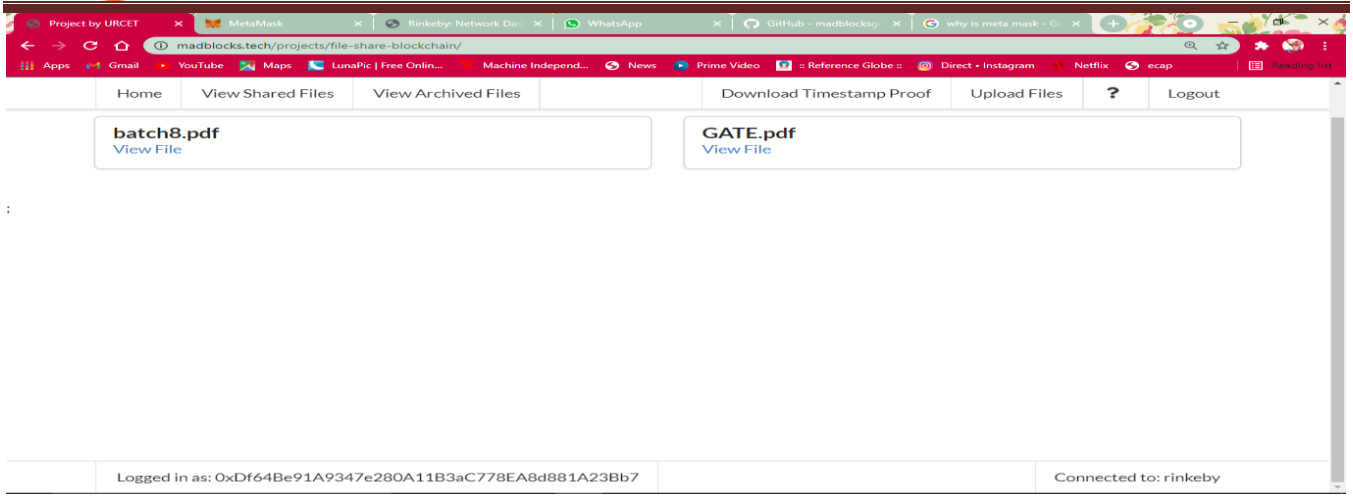

Figure : Uploaded a file

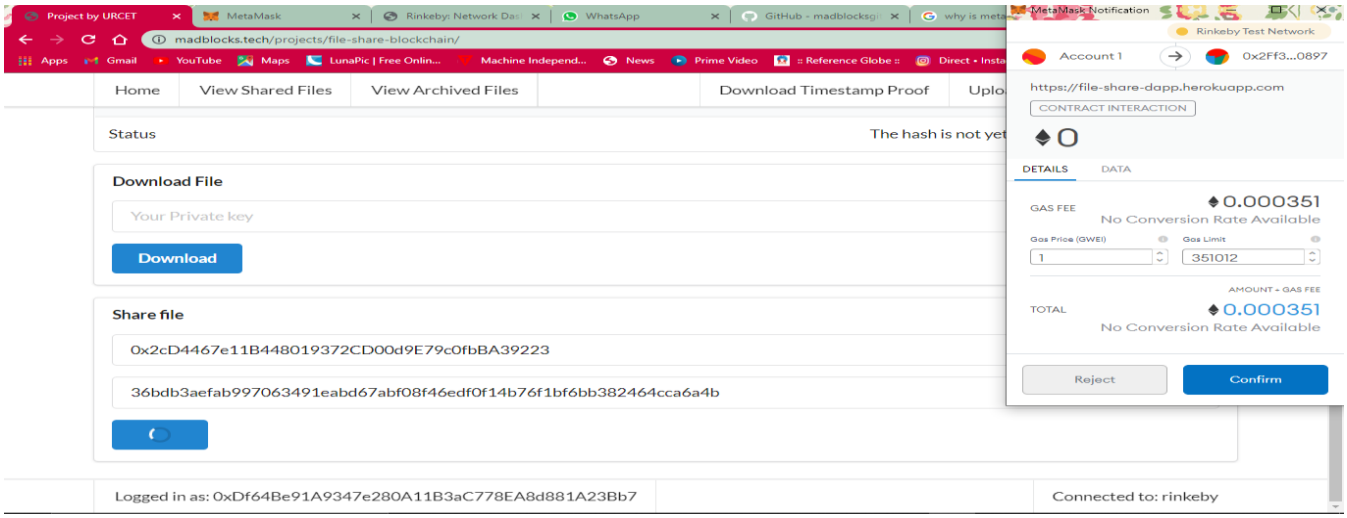

Figure : Sharing a File

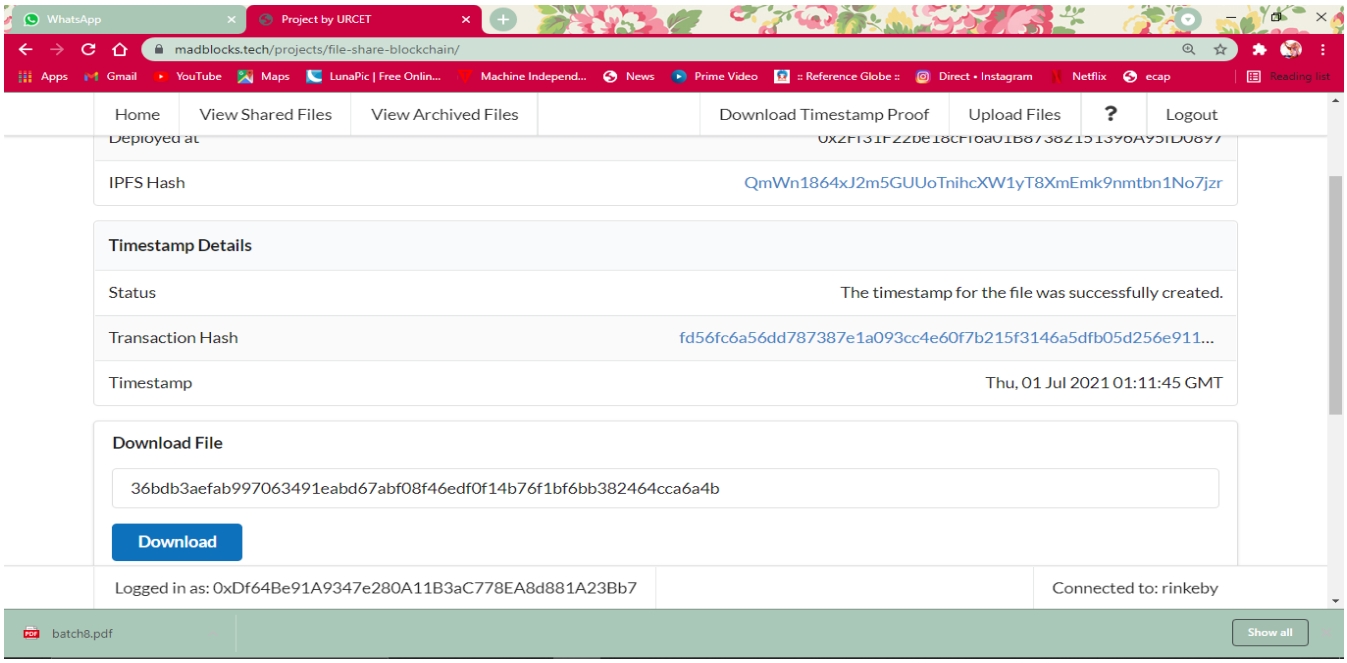

Figure : Downloading a File

5. CONCLUSIONS

The proposed system will takes the advantage of the blockchain and helps to create a trustworthy version which will be used in higher education credit and grading system. As a proof of concept, we showed a prototype implementation of the system platform which is developed on the open-source Ark blockchain platform. Thus by using the Personalized Secure E-Identity Card, users will be able to safely submit documents to various institutions/ Government bodies without the fear of data theft. Users are now free from the fear of losing the documents as they will be stored in digital format. It will also facilitate the user to personalize the card with only the required documents providing the feature of addition or deletion of a document.

REFERENCES

[1] C. K. Wong and S, S. Lam "Digital signatures for flows and multicasts", WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.
[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.
[3] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
[4] Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349
[5] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in proc. IEEE S&P'13, May 2013, pp. 511–525.
[6] L. Zhang, D. Choffnes, D. Levin,et al., "Analysis of SSL certificate reissues and revocations in the wake of Heartbleed," in proc. ACMIMC'14, Nov 2014, pp. 489– 502.
[7] M. Carvalho and R. Ford, "Moving-target defenses for computer networks,"IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.-Apr.2014.
[8] Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.
[9] D. Ferraiolo, R. Kuhn, and R. Sandhu, "Rbac standard rationale: Comments on "a critique of the ansi standard on role-based access control", "IEEE Security Privacy, vol. 5, no. 6, pp. 51–53, Nov 2007.
[10] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacypreserving access control model based on blockchain technology in iot," in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523– 533. [11]L. Y. Chen and H. P. Reiser, "Distributed applications and interoperable systems, 17th ifip wg 6.1 international conference, dais 2017, held as part of the 12th international federated conference on distributed computing techniques, discotec 2017, neuchtel, switzerland, june 1922, 2017." Springer, 2017.
[12]Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.
[13] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," no. Iccet, 2012.
[14] J. van Beusekom, F. Shafait, and T. M. Breuel,"Text-line examination for document forgery detection," Int. J. Doc. Anal. Recognit., vol. 16, no. 2, pp. 189– 207, 2013.
[15] Mahamat, M. B. (2016), A Web Service Based Database Access for Nigerian Universities' Certificate Verification System.
[16] Osman Ghazali, Omar S. Saleh, "Cloud Based Graduation Certificate Verification Model". [17] Lisha Chen-Wilson, Dr David Argles,"Towards a framework of A Secure EQualification Certificate System. [18] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen," Blockchain and Smart Contract for Digital Certificate".