DAuth: A Decentralized Web Authentication System using Ethereum based Blockchain

Shibasis Patel
Dept. of CSE
IIIT Bhubaneswar
Odisha, India
B115050@iiit-bh.ac.in

Anisha Sahoo
Dept. of CSE
IIIT Bhubaneswar
Odisha, India
B115008@iiit-bh.ac.in

Bhabendu Kumar Mohanta
Dept. of CSE
IIIT Bhubaneswar
Odisha, India
C116004@iiit-bh.ac.in

Soumyashree S Panda
Dept. of CSE
IIIT Bhubaneswar
Odisha, India
C117011@iiit-bh.ac.in

Debasish Jena
Dept. of CSE
IIIT Bhubaneswar
Odisha, India
debasish@iiit-bh.ac.in

***Abstract*—Over the past decade, a lot of evolution has happened in the field of security specifically authentication system. The most commonly used authentication service we use now is OAuth 2.0 based authentication. In this method, we are dependent on a 3rd party authentication service provider to which we need to trust. Though this model is used extensively nowadays, studies show that it is still vulnerable to several hacks. In addition to that, the 3rd party authentication provider has total control over the user data to which they can leak or modify at their will. Thus the use of OAuth 2.0 based protocol has raised security and privacy concerns. In this paper, blockchain and its use cases are studied and an alternative way of authentication service has been proposed based on Ethereum Blockchain called DAuth. Furthermore, a prototype has been developed which enables user authentication on the site. DAuth proposes to enhance transparency and user control in transactions which involves identity management.**

***Index Terms*—Web Authentication, Decentralized, Security, Blockchain, Ethereum, solidity, smart contract**

I. Introduction

The Internet today lacks an identity protocol for identifying people and organizations. We live in an era of convenience and anything that can reduce the time that it takes to complete simple tasks is embraced with open arms. One of the most relevant examples in the online world comes from the realm of user authentication. Previously, we had to keep a collection of our user ids and passwords, now we can quickly and easily login through Facebook, Google and a whole array of other services. But is this wise and are there better alternatives? In this paper, we will take a look at the current state of user authentication as well as some interesting alternatives that are now available due to blockchain technology.

Blockchain is a trustworthy distributed ledger of transactions which can be coded to store not only financial transactions but also essentially everything of value. A Blockchain in general terms is a time-stamped series consisting of immutable records of data which is controlled by a group of devices and is not owned by any single entity. All these blocks are secured and are linked to each other based on cryptographic methods (i.e. chain). In this paper, the main aim is to implement the Blockchain smart contract using Ethereum [6] and [11] platform, where the Web Authentication mechanism takes place using Ethereum Authentication(DAuth). DAuth is an attempt to make a decentralized site login and authentication protocol. Its analogous to the Log In with Facebook button that we have probably become accustomed to. It is a smart contract that will store user IDs and their associated wallet addresses. It works on the concept of Digital Signature and Hashing. A digital signature [9] is a process of verification where the document or message sender (signer) or public/private key provider shares the public key with the end users. The sender, with the help of the private key, appends the encrypted signature to the data. The end user decrypts the data and the signature is verified, which lets the end user know that the data is from the actual or original sender. A hash is a function which helps in converting a set of input of letters and numbers into a set of an encrypted output of a particular fixed length. A hash is generated with the help of an algorithm and is very much required for Blockchain management in cryptocurrency.

II. Related work

Security systems are designed to help the authorized people to access the site (permission problem) and keep unauthorized people out of it(the prevention problem) [2]. Authentication [8] is a process where verification of the identity or the authenticity of a person takes place. Previously, whenever a customer goes to a bank and wants to withdraw money from his account, the teller at the bank used to ask the customer for a verification which leads to confirmation that he/she is a reasonable customer. The customer used to do a signature on a piece of record physically, which is compared to a signature given by the customer during the time of account creation. Due to the origin of computers, the signature was restored by password. Then a password value is set by users during various registrations and they have to provide those every time when the account is accessed. However, as the Internet is emerging hugely, authentication is evolving greatly. The authentication scheme started from the simplest HTTP Basic authentication to greater complicated and secured schemes. In HTTP Basic Authentication, whenever a request is conveyed by any browser for a website and it requires Basic authentication, then answers with an error in the header that contains a www-authenticate attribute is given by server. Users enter their username and password, which is encoded in a Base64-encoded form before it is being sent to the server. Then comes HTTP Digest Authentication, it works the same

978-1-5386-9353-7/19/$31.00 ©2019 IEEE

to Basic and is stronger because it makes use of hashes while username and password are sent to the server. Click pattern helps in providing a strong password rather than plain text [4]. Graphical passwords or captcha are alternatives for plain texts. Here objects are displayed and users just need to draw using mouse, touchpad or touch-screen [4]. Next, the users have to give all their personal details to register on a particular website. This raises the concern of the security issue of the users and creates a problem for database flooding. Now comes the era of OTP(One Time Password) and OAuth 2.0 Authentication. In OTP, a numeric password is generated and is valid for a short period of time and can be used once [4]. But in this case, a security issue may come, if someone has physical access to the device. Then to overcome the problem of database flooding, OAuth 2.0 authentication has emerged. For instance, if we access any website using facebook or google etc and due to some issue, facebook or google blocks that particular website, the user will lose access to that website. Now in this present era, some works on bitid, nameid has been done, where NameID is an experimental attempt of user authentication which uses Namecoin 4.2 and OpenID to provide a secure, unique and decentralized digital identity to the users.NameID relies on OpenID which requires a 3rd party to let us authenticate [1]. So our objective is to use a secure and decentralized network such as Ethereums in order to aid this type of authentication.

- NameID is an experimental attempt of user authentication which uses Namecoin 4.2 and OpenID to provide a secure, unique and decentralized digital identity to the users. Namecoin is a bitcoin [3] based peer-to-peer, completely decentralized platform that allows everyone to register names. Namecoin was initially designed as a decentralized domain name server(DNS). Namecoin ensures that no-one can take away a name which you own without your consent. Data can be associated with the name which can be verified by everyone present in the network but cannot be forged or censored by unauthorized personals.OpenID is an open internet standard that specifies a protocol which allows you to authenticate to multiple services without the need of creating multiple identities and passwords. This method tries to make web-authentication decentralized. However, NameID relies on OpenID which requires a 3rd party to let you authenticate. So, it is not fully decentralized.
- Bitid is an open protocol based on bitcoin which lets its user securely and in a simple manner login based on public key cryptography and blockchain network. The authentication is done by signing a challenge which will prove that we own a specific bitcoin address and after that the data will be securely linked to our session. Its main purpose is to authenticate owners of bitcoin. This is fully decentralized, however, its more like a 2 Factor authentication.

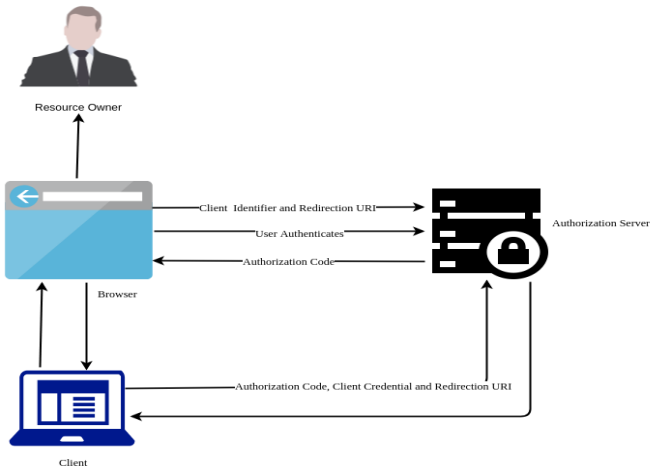

Fig. 1. OAuth 2.0 Architecture

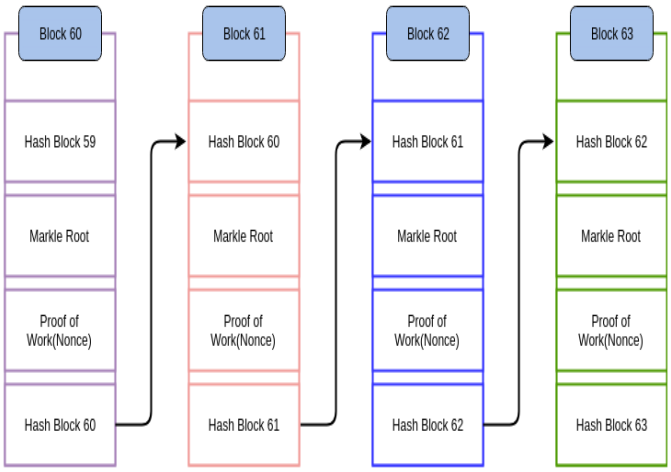

Fig. 2. Basic Blockchain Architecture with its associated attributes

III. Architecture of OAuth 2.0

Authentication is the process of giving access to only trusted parties.OAuth 2.0(fig. 1) an authorization framework helps in enabling applications to acquire access to user accounts on an HTTP service, such as Facebook, GitHub, and DigitalOcean. It works by assigning user authentication to the service which hosts the user account and authorizes the third-party applications to access the user account.

Blockchain uses the concept of the Merkle tree(fig. 3) which is also known as the hash tree. Here the hash of a data block is present in every leaf node. The hash of the labels of its child nodes is present in every leaf node. It contains a cryptographic hash pointer which is used to retrieve information and check whether the hash of the information has not been modified. The data structure used in blockchain is a hash-chain of blocks. Merkle tree helps in timestamping, verification of digital document, peer to peer networks. Merkle tree is important because, if anyone transaction is being changed, the Merkle root changes and again hash of the block containing the Merkle

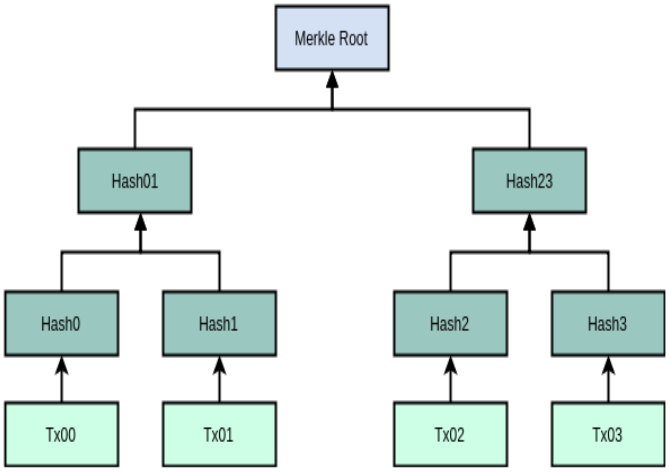

Fig. 3. Merkle root hash of the Blockchain System

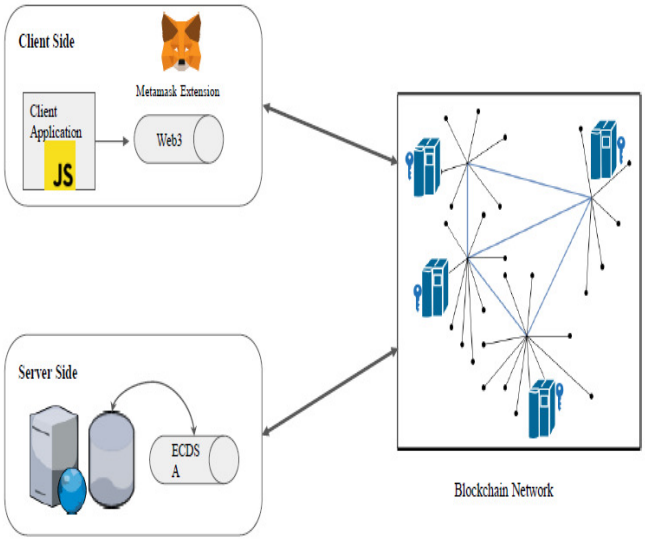

Fig. 4. Architecture Decentralized Web Authentication

tree changes.

IV. Proposed Decentralized Authentication and DAuth Architecture

The Implementation takes place using the Ethereum platform and Web3 client(Ethereum JavaScript API), which is used to communicate smart contract running on blockchain with the Frontend.

A. Blockchain and its properties

Blockchain (fig. 2) is a decentralized platform consisting of a peer-to-peer network having a permission or permissionless environment. It is a pioneering technology to realize smart contracts. The blockchain consists of chains of blocks which contains digitally signed and encrypted transactions verified by the peers. The blocks here contains the hash value of each block and are dependent on the hash code of previous blocks. This makes the blockchain tamper-proof. The mechanism to generate hash is called mining, which is complicated enough to make the blockchain tamperproof.

Advantages of Blockchain: A number of benefits of using blockchain for identity management [7] have already been proposed:

- Decentralized: The information that is held by the blockchain has no single authority that controls.
- Tamper Resistant: The data once committed to the blockchain cannot be deleted. Hence, historical activities available on the blockchain cannot be altered and all the changes done are transparent.
- Cost saving: Shared identity information can lead to a reduction of cost for relying parties. Also, the amount of replicated data in the database is reduced.
- User control: User doesnt lose control of their digital identity even if they lose access to any particular service. All the above points aggregate to use blockchain network for authentication.

Here, Ethereum has been taken as the decentralized network for web authentication. While Bitcoin works fine with storing values and for the financial transaction, It doesn't allow computer application to run on its network. The bitcoin scripting language is a simple, stack-based language only meant for the financial transaction. It isn't a Turing-complete language and doesn't support loops. Ethereum, on the other hand, has a major advantage of being a technology that supports Solidity which is a Turing-complete language and does allow computer application aka. smart contracts to run on its network. This has led to the quick growth of this platform with plenty of decentralized apps built on top of the ethereum platform. Funds can also be raised via initial coin offering(ICO) using the ethereum network in which a new digital coin or a token is being introduced. Also, ethereum being a public ledger allows everyone to participate in the network so that anyone can verify the transactions in the network.

B. DAuth

DAuth(fig. 4) is an attempt to make a decentralized site login and authentication protocol. Using DAuth:

1) The backend requests users ethereum address from the smart contract deployed in the ethereum network.
2) The backend asks the user to sign the generated message using the authKey address of the user.
3) The user signs the message using the metamask plugin from the frontend and sends the signed message to the backend.
4) The backend compares the two signatures, the one which it got from the frontend and the one stored on the blockchain. If the signature is verified, it activates the users session.

C. Smart Contract

A smart contract is a tiny computer program that runs on the blockchain. Smart contract [10] can be used for various applications based on blockchain. It is just like a physical

contract but it doesn't require trusting a 3rd party for operating. It enables a certain task to be automatically executed once some pre-defined conditions are triggered. Because the smart contract is stored inside a blockchain, it runs in a completely decentralized manner. With this technique, no one in the network can gain control of the assets. As they are stored on a blockchain, they inherit some interesting properties.

- It is immutable i.e the smart contract can never be changed once it is deployed into the blockchain. So, no one can tamper the code of the smart contract behind your back.
- It is distributed i.e Everyone in the network validates the output of the smart contract. So, an attacker can't force the contract in a certain way because this attempt will be spotted by the other nodes in the blockchain network and they will mark this attempt as invalid.
- It can work as multi-endorsement accounts, such that smart contract is executed only when a required number of nodes endorses.
- It can store useful information about an application such as registration and domain information.

D. Ethrerum platform

Ethereum is an open-source decentralized public and permissionless blockchain based platform providing computer application to run on top of it. It lets developers program their own smart contract using solidity language without needing to build their own blockchain. The applications running on the blockchain can communicate in the blockchain network with each other and the complete network of an interconnected application called decentralized applications(Dapps) is being developed using this. The major advantages of a Dapp over a conventional centralized application is:

- It doesn't depend on any specific existing party for its operation.
- It's not about only one party selling its services, it's more about a community/network who all share ownership of a piece of software come together without any centralized intermediary.

The ethereum platform has a shorter block time than bitcoin which makes it more convenient to run applications on top of it. Blocks and the record of cryptocurrency transaction are done by Ethereum, which is done very quickly and leads to quicker transactions. Ethereum processes a large number of the transaction happening on the network without the user waiting too long.

As bitcoin, ethereum also currently uses Proof of work(POW) based consensus mechanism. In this mechanism, the miners make transactions and proof their work by accomplishing a computationally complex task called nonce value and include the block with the nonce value to the chain. Here, the first miner who got the nonce value takes the reward. The ethereum network currently moving on to the proof of stake based consensus algorithm. Here the user having the highest stake of the total cryptocurrency, coinage are able to create the blocks and include it to the chain. In this system, the transaction fees are taken by miners as there is no block reward associated. The POS-based system is considered as less computationally expensive for its functioning.

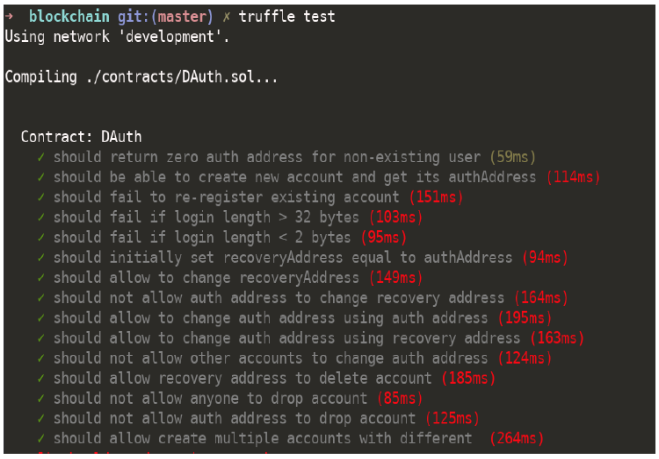

Fig. 5. passing truffle tests

V. Experimental Setup

The smart contract has been programmed in solidity, which is an object-oriented programming language for smart contract development. It is designed to minimize the complexity of smart contract, as more complex code costs more to deploy into the blockchain. We used truffle framework, which is a development and testing framework and enables asset pipeline for ethereum that makes ethereum development faster and structured. We deployed the smart contract into ethereums official test network called Rinkeby. The experiments are performed on a 2.2GHz Intel Core i5-5200U processor with 8GB of RAM and we used Arch Linux as our primary OS. We used metamask plugin which is an extension for having access to the smart contract deployed in ethereum/ Dapps in the browser. This extension injects the ethereum web3 APIs into any websites javascript contents, which results in communication between DApps and the blockchain.

VI. Security Analysis

Information technology has been transformed the manner business is conducted around the world. The Web has evolved to a great extent as compared to what it was a few years ago. Modern technology has put the regulations for how a company does its business and how it conveys with customers and others in the new market places. In today's era, it has been used for application-to-application exchanges. To upgrade the productivity and flexibility of Web communication, Web Services technologies have been advanced. E-business applications tempt attackers who can manipulate the backend of an application which helps in the storage of all personal data. The attacks on various Web Services might generate to stop the entire network communication or might lead to

revealing confidential information in an organization [5]. Input Validation: It attacks directly on the modified data parsed by the server. This includes buffer overflow attack, Dictionary attack, data tampering.

- Buffer Overflow: Here the attacker put a large amount of data than expected in the code variables so that it will execute arbitrary code with the advantage of running the users original code.
- Dictionary attack: Here the attacker randomly tests all passwords for performing dictionary attacks.
- Data Tampering: Here, the attacker changes or modifies the complete data of the user.
- Denial of Service(DoS) attacks: Here, the attacker goal is to disclose the information which he can use it for crashing Web Application Processes.
- Session management Attacks: This leads to vulnerabilities in application which leads to attacks on session management.

Due to all the above security issues, a decentralized web authentication system using blockchain is proposed which is not a password-based authentication and authentication is done using AuthKey which is a 160-bit hash and is secured enough to prevent all the above attacks [5].

VII. Conclusion

The adoption rates for Ethereum based blockchain and cryptocurrencies in general till today is still just a fraction of all users who likes of facebook and google. It will take a bit of time for all people to get comfortable using Ether address rather than a facebook account. However, the crypto adoption rate is emerging hugely and the recent scandals of Facebook have helped users to align towards this. So, it will be very interesting to comprehend whether decentralized authentication can be a valid alternative.

References

[1] Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." 2012 IEEE Symposium on Security and Privacy. IEEE, 2012.

[2] Renaud, Karen. "Quantifying the quality of web authentication mechanisms: a usability perspective." Journal of Web Engineering 3.2 (2004): 95-123.

[3] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[4] Jesudoss, A., and N. Subramaniam. "A survey on authentication attacks and countermeasures in a distributed environment." Indian Journal of Computer Science and Engineering (IJCSE) 5.2 (2014): 71-77.

[5] Moradian, Esmiralda, and Anne Hkansson. "Possible attacks on XML web services." IJCSNS International Journal of Computer Science and Network Security 6.1B (2006): 154-170.

[6] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151 (2014): 1-32.

[7] Dunphy, Paul, and Fabien AP Petitcolas. "A first look at identity management schemes on the blockchain." IEEE Security Privacy 16.4 (2018): 20-29.

[8] Moinet, Axel, Benot Darties, and Jean-Luc Baril. "Blockchain based trust authentication for decentralized sensor networks." *arXiv preprint arXiv:1706.01730* (2017).

[9] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." *2015 IEEE Security and Privacy Workshops*. IEEE, 2015.

[10] Mohanta, Bhabendu Kumar, Soumyashree S. Panda, and Debasish Jena. "An Overview of Smart Contract and Use Cases in Blockchain Technology." 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2018.

[11] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper (2014).