DLT Enabled IoT devices

Submitted By

Harsh Mashru

18MCEN07

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2019

DLT Enabled IoT Devices

Major Project

Submitted in fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering

Submitted By

Harsh Mashru

(18MCEN07)

Guided By

Dr. Vijay Ukani

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INSTITUTE OF TECHNOLOGY
NIRMA UNIVERSITY
AHMEDABAD-382481

December 2019

Certificate

This is to certify that the major project entitled **"DLT Enabled IoT Devices"** submitted by **Harsh Mashru (18MCEN07)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering (Networking Technologies) of Nirma University, Ahmedabad, is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-I, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Dr.Vijay Ukani
Guide & Associate Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Mr. Gaurang Raval
Associate Professor,
Coordinator M.Tech - CSE (CSE-NT)
Institute of Technology,
Nirma University, Ahmedabad

Dr. Madhuri Bhavsar
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr R. N. Patel
I/C Director,
Institute of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Harsh Mashru**, **18MCEN07**, give undertaking that the Major Project entitled "**DLT Enabled IoT devices**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering(Networking Technologies)** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made.It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

____

Signature of Student
Date:
Place:

Endorsed by
Dr. Vijay Ukani
(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to **Dr. Vijay Ukani**, Associate Professor, Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his valuable guidance and continual encouragement throughout this work. The appreciation and continuous support he has imparted has been a great motivation to me in reaching a higher goal. His guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

It gives me an immense pleasure to thank **Dr. Madhuri Bhavsar**, Hon'ble Head of Computer Science And Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr. R. N. Patel**, Hon'ble I/C Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation she has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

- Harsh Mashru
18MCEN07

Abstract

Distributed Ledger/ Blockchain Technology is an Immutable, Digitized and Decentralized set of record which is renown for its security and privacy. Blockchain is basically an append-only ledger which is immutable as the address/hash of each block is dependent on the previous blocks. Since the introduction of Bitcoin, The Blockchain Technology has intrigued developers and researchers and since then there is an exponential growth in the technology. Also there is humongous amount of research going on currently in the field to constantly make it better. Currently what we have done is also a part of evaluation for enhancing the performance of the blockchain. Though I started with a small tutorial to get my Hands-on the technology eventually getting to Universal Logins. Universal Logins is an Ethereum Funded project that is an SDK for Decentralized Application's(DApp's) to make the User Experience better with the DApp's. Currently it is in progress. It basically uses a relayer which helps the user to initiate the transaction and also it allows the user to login into different DApp's using the same Id's that were created using the first transaction. This process is very much easy compared to the conventional process where the user had to initialize the transaction and store the key phrase for every new DApp. Then Perun Networks is a Layer 2 blockchain protocol that is used for performing the off-chain transactions. Basically the summary of the transactions is uploaded to the blockchain and not all the transactions. Basically it creates a virtual channel between peers and till the extent the transactions are on, the channel exist and then it is shut and the final entry is updated in the ledger. Then inferring the knowledge from Perun networks and other state channel protocols we published a paper revolving around the use of the state channel protocols in the Iot Networks. Basically it proposed a framework to select the state channel protocols for the IoT networks. Eventually a Blockchain Enabled hardware device was implemented where Bosch specific sensor devices named XDK was used which communicated within itself and the transaction was stored in the blockchain. The devices acts as a producer and consumer respectively and there is a financial transaction between them as the one who initiates the transaction and requests for the data, pays for it. Currently the evaluation of Hyperledger Avalon a flavor of the Hyperledger framework is in progress.

Abbreviations

DLT	Dristributed Ledger Technology.
PoW	Proof of Work.
PoS	Proof of Stake.
DPoS	Delegated Proof of Stake.
PoET	Proof of Elapsed Time.
PoD	Proof of Deposit.
PBFT	Practical Byzantine Fault Tolerant.
IoT	Internet of Things.
DApp	Decentralized Application.
BIoT	Blockchain Enabled IoT.
L2 Protocols	Layer 2 Protocols.
GSC	General Smart Contract.
VC	Virtual Channel.
ED	Edge Device.

–

Contents

List of Figures

Chapter 1

Introduction

For getting the hands-on in the technology, knowing the basics of the technology is of utmost importance. So I started with the basics of the technology and then getting hands-on through some implemented example i.e., Pet Shop Tutorial and then the actual work. Here I have mentioned the brief of all the topics I have covered which are explained in great detail in the latter part. Introduction is followed by the Literature Survey Summary which highlights the literature I have referred through the course of time. Eventually every topic is explained in great detail.

1.1 Blockchain Technology

Blockchain is a peer-to-peer, distributed ledger that is cryptographically secure, append only, immutable and updatable only via consensus or argument among peers. It is a chain where each peer is connected to the other and the hash of a particular block is dependent on the previous block. Every block basically consists of the transactions and each transaction has the hash value stored in it and not the actual value. First block in the blockchain is generally known as the Genesis block. The nodes connected in the network are either the Miners or the Block signers.

Actually the whole process of blockchain starts with initialization of the transaction. The transaction is signed by the block signer and sent into the transaction pool. Then the transaction is selected by the miner on the basis of incentives it provide. After the miner mines the transaction in the form of solving the puzzle and as soon as the puzzles is solved it is added to the block.Then the block is added to the chain while the consensus approves it. Hence the consensus decides which block will be added to the chain next. After the block is added the updated chain is distributed to the peers.

Some of the key aspects of block-chain are:

- Consensus
- Smart Contracts
- Information stored in blocks linked to previous blocks making a chain
- Each block is stored with a time-stamp
- Crypto Secured peer-to-peer Transactions
- Distributed Decentralized[1].

The block generally contains the block header that consists of A Nonce, Timestamp, Merkle Root and Block body that contains transactions.

- Nonce: It is generated and used only once, mostly it is random number that comes in a particular range. It is used for Replay Protection, Authentication and Encryption.
- Merkle Root: It is basically hash of all Nodes of a merkle tree. Merkle tree is widely used to validate the large data structures efficiently. So verification of only merkle root is required.

1.1.1 Generic Elements of a Blockchain

There are some key elements in a blockchain which as a whole are helpful for the decentralize, immutable, non-updatable technology. Address, Transaction, Block, Peer-to-Peer Networks, Scripting or Programming languages, Virtual Machines, Node, Smart Contracts etc. are some of the elements.

- Address: It is either a public key or derived from public key. It is preferable to generate a new key or address for every transaction as it was found that it is possible to identify a user based on his/her frequent transmission. So it is better to get a new one.

- Transaction: It is basically transfer of data/value from one address to another.
- Block: It is a collection of transaction which eventually added to the chain.
- Peer-to-Peer Networks: It is a distributed system or a network of distributed peers.
- Scrippting and Programming languages: Mostly, Go programming language is used to write smart contracts.
- State Machines: It is basically a state transition mechanism.
- Smart Contacts: It is self executable programs that are used to build agreement between peers.

Advantages of Blockchain Technology,

- Decentralization: There is no single authority to the network. The various decisions of the network is done by the selected consensus mechanisms. Hence the security of the network is better.
- Transperancy and Trust: All the transactions that occurs in the network are updated to every other peer in the network. Hence no one can fake or deny any transactions.
- Immutability: The data or the transactions once recorded in the blobkchain can never be changed as one transaction hash of a particular block depends on the transaction hash of the earlier block, hence if there is any change in a particular block all the previous blocks are to be updated which is almost impossible.
- Availability: Even if there are some issues with some of the peers of the network, there is never a complete shut down of the network as there is no central authority to the network.
- Secure: One there is no authority of a particular in the network and other the Immutability, these two features makes the network more secure.
- Simplify Current Paradigms: The transaction doesn't need to go for the approval to the authorities and hence the complete concept of intermediaries has been discarded.

Disadvantages of Blockchain Technology,

- Scalability: As the number of peers increases the number of transactions also increases and with that increases the load to verify the transaction

- It is a bit slow in various scenario: The increased load to verify the transaction(mining) also results in the slowness if the network

- Cost: There is a minimal mining fee per transaction whih is not feasible in every scenario.

1.1.2 General Scheme for creating blocks

The various steps which taks place which eventually end up being a block,

- Node starts the transactions by first creating and digitally signing it with its private key.

- Basically transactions are data structures that represent transaction between users.

- Then transactions is flooded through Gossip Protocol.

- Then the transaction is added to the block while the confirmation takes place.

1.1.3 Types of Blockchain

There are various types of blockchain including the public and private blockchain. They are:

- Distributed Ledger Technology: It is basically a Permissioned blockchain that are shared and used between the known participants. Also it serves a shared databases between participants those are known and verified.

- Public Blockchain: These are permissionless blockchains. They maintain a copy of the ledger on their local nodes and uses a distributed consensus mechanism to decide the eventual state state of the ledger.

- Private Blockchain: These are permissioned blockchain hence there are various nodes that are added into the blockchain and acts as a consensus.

- Sidechain: They are also known as pegged Sidechains. It is a concept where coins are moved from one blockchain to another and moved back again.They are one-way pegged and two-way pegged. Also they use the consensus mechanism known as Proof-of-Burn(PoB)

- Shared Ledger: Generally all blockchains whether Public or Consortium.
- Tokenized Blockchain: Standard blockchains to generate cryptocurreny as a process of consensus via mining.

1.1.4 Consensus Mechanism

Consensus is an Algorithm that is selected on the basis of the project to take various decisions. It is essential to choose for an appropriate consensus algorithm for a particular blockchain project. Consensus Mechanism:

- Agreement
- Termination
- Validity
- Fault Tolerant
- Integrity

Two Basic categories of Consensus Mechanism:

- Traditional Byzantine Fault Tolerant based
- Leader election based consensus mechanisms

Alternate to it is RAFT. So the nodes are assigned as Candidate or Leader.And the leader is selected after a candidate node receives enough votes and hence all the changes go through the leader.Consensus basically provides means of agreeing to a single version of truth by all peers on the blockchain network. There are different consensus used in blockchain based on the need of project and type of blockchain used. They are:

- PoW: Relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network.
- PoS: Works on the that a user should have adequate stake, the user has invested enough in the system so that any malicious attempt by that user would outweigh the benefits of performing an attack on Network.

- DPoS: Here every node that has a stake in the system can delegate the validation of a transaction. used in Bitshares blockchain.
- POeT: Uses trusted execution environment to provide randomness and safety in leader election process via guaranteed wait time.
- PoD: Nodes that wish to participate have to provide security deposit before thay mine and propose blocks[1].

Also there are certain other consensus which are less used currently. They are Proof of Importance, Reputation based mechanism, Proof of Activity, Proof of Capacity, Proof of Storage, etc. Additionally there is a theorem that is CAP theorem which states that Distributed systems cannot have Consistency, Availability and Partition tolerance simultaneously. Consistency is achieved using consensus algorithm in order to ensure that all nodes have the same copy of data. This is also called State machine replication

1.2 Pet Shop Tutorial

This tutorial basically covers some core aspects of the Blockchain development. Some tasks that are performed in the tutorial are [7]:

- Making the development environment up and running
- Using a Truffle box to create a truffle project
- Developing the smart contract
- Deploying the smart contract
- Testing the smart contract
- Develop a UI to interact with smart contract
- Testing the DApp in the browser

The whole idea behind this tutorial is the owner named Pete wants to use Ethereum as a medium for their Pet adoption store. In total there is a capacity for maximum 16 pets to be displayed at a time, hence the store capacity is 16. Though they have a database which contains all the information for all the pets that are available for adoption. Basically for proof of concept the owner needs a DApp which displays the entire process and every pet that is adopted has an ethereum address attached to it.Basically a smart contract is to be written which displays the front end logic, as the User Interface is provided in form of the website.[7].

1.3 Universal Logins

Universal Login is basically an architecture that helps you login into the dapps, web and native applications.Universal Logins utilizes some major concepts like personal multi-sig wallet, Meta-transactions, ENS names etc. Broadly we can classify Universal Logins under the UX Problems. Universal Logins is an Ethereum platform specific solution. In the conventional system for every new app the user creates a new private key, backup that seed phrase and transfer ethers(ETH) into it. This process is faster if you already have ETH, but if you don't it is again elongated as it usually requires credit card or an account in exchange which often requires official documents and wait for some days.Also the user may own multiple devices and they want their devices to be in sync with each other. The Generalized Process of Universal Logins works as:

- You create a context specific etherless account .
- You sign a message and forward it to the Identity contracts.
- Then you use Gas relay abstraction where the contract forward the message to the relayer which publishes the transaction to the blockchain.
- Also you may have certain easy recovery options from multiple devices in case you lost the device[6].

Some advantages of using this architecture are: User doesn't need Ethers to be attached with that particular account, User can pay transaction fees in whichever the token they like, also if the user's device is lost there are certain recovery methods they can follow, etc.

1.4 Perun Networks

Perun is an off-chain channel system that offers a new method for connecting channels that is more efficient than the existing technique of "routing transactions" over multiple channels. Perun introduces a technique called “Virtual Payment Channels” that avoids involvement of intermediary for each individual payment [4]. Let’s suppose Alice and Bob are both connected by a channel created over the blockchain with an intermediary payment hub Ingrid. Given these ledger channels, we can establish a virtual channel that establishes a direct (virtual) link between Alice and Bob, where the intermediary Ingrid does not need to get involved in each payment. Basically explaining in a single line only the summary of the transactions are uploaded to the blockchain and not he complete transactions. They are only performed between the peers.There is also a version control mechanism hence at the time of dispute the smart contracts can easily solve the issue using the latest version shown by the either user. Basically it helps in improve the performance of the conventional blockchain system.

1.5 Blockchain Enabled IoT devices

Blockchain is an disruptive technology bringing in the amplication and creating greater values in IoT networks. The major concerns creating new value convergence of blockchain and IoT are scalability and overhead computation cost for the communication. Hence to provide an infrastructure for the communication the hardware wallets play an ample role. The core idea behind it was to provide incentivization to the hardware nodes while they perform condition monitoring transactions. Basically the devices acts as a Hardware wallet. To perform the simulations and test specific requirements a Bosch specific hardware device name XDK was used. These are basically the programmable sensor devices which has many sensors like Temperature, pressure, Accelerometer and many more. Currently only three sensors like Temperature, Accelerometer and Humidity have been used. This particular concept can be better used in the Data Marketplace scenario. Currently the code works for connecting the two XDK devices to the Ethereum Network. Also there is a RESTApi for a general data market place scenario which requests the data based on the sensor parameters and can easily retrieve data from the devices in the network[12].

1.6 Hyperledger Avalon

It is a framework that enables privacy preserving blockchain transactional operations. It mainly enables moving the blockchain processing from the main chain to the dedicated resources. The task is to setup the examples of the Hyperledger Avalon and analyze it if its better for one or the other platform and If yes which parameters are better than the existing Hyperledger flavors. They have provied four examples in their repository namely Echo, EEA Token Execution, Heart Disease Evaluation and Generic Workload Client. Basically the task is to setup the example and evaluate the behavior[15].

Chapter 2

Literature Survey

2.1 Literature Summary

Paper Title	**Year**	**Type**	**Author**	**Summary**
Bitcoin: A Peer-to-Peer Electronic cash system [2]	2008	Paper	Satoshi Nakamoto	This Paper is where all the idea of blockchain technology got the boost. This allows electronic cash to go from one party to other without any intermediary participating between them. There is a hash based timestamp that is been used and a consensus that is PoW. Bitcoin is basically the first public blockchain where a User Initiates a transaction then using the consensus the transaction is mined and added to the blockchain and eventually the final value is updated.
A Next-Generation Smart Contract nd Decentralized Application Platform [3]	2014	Paper	Dr. Gavin Wood	This paper presents the platform which presents the blockchain paradigm and justifies the functionality. It is used to build the dapp's on the top of it. It provides functionality where different codes and states can talk to each other through a message passing framework. Ethereum is a project which attempts to build the generalized technology; technology on which all transaction based state machine concepts may be built.

Table 2.1: Literature summary

Paper Title	Year	Type	Author	Summary
Perun: Virtual Payment Channel Hubs over Cryptocurriencies [4]	2019	Paper	Stefan Dziembowski and Lisa Eckey and Sebastian Faust and Daniel Malinowski	This paper basically helps in solving the performance issues related to blockchain. It is generalized as the Layer 2 blockchain. Here a concept of Virtual channels is derived. These channels ae created between the nodes that want to transact and are not linked on-chain. They will somehow be connected to the main chain with the help of some intermediaries. So using them, a virtual channel is created and the rest of the transactions between those nodes are done off-chain. This helps in making the performance better.
AnyLedger: Embedded Wallet for Decentralized IoT [5]	2016	Paper	Bogdan Djukic, Lorenzo Pieri	This paper introduces the open source programmable embedded wallet. Every physical asset will be able to exchange value and interact with the smart contract. Once connected to a sensor or to an existing IoT device, the embedded wallet is able to communicate to the broker which acts as a bridge to a specific blockchain ecosystem. There is also a wallet fleet manager which is a vital feature to provide trust to the users.

Table 2.2: Literature summary

Chapter 3

Pet Shop Tutorial

3.1 Pet Shop DApp

The core idea behind this was to get some hands-on the Ethereum platform and working with the Smart Contracts. The problem statement of it was, there is a user who has some pets and has to display 16 pets at a time in a decentralized application. Basically the owner wants an Ethereum address to be associated with the pet that is to be adopted. The tasks that were covered during the exercise were[7]:

- Making the development environment up and running
- Using a Truffle box to create a truffle project
- Developing the smart contract
- Deploying the smart contract
- Testing the smart contract
- Develop a UI to interact with smart contract
- Testing the DApp in the browser

3.1.1 Making the development environment up and running

The technologies like truffle, Ganache, Node.js were used. There are already some dependencies that are present in the Truffle box which will be helpful in developing the environment. Truffle is basically the Test environment that is created and Ganache is an ethereum based blockchain that is basically used to develop and deploy the smart contracts, develop applications and to test the project in the ethereum based environment.

3.1.2 Using the Truffle box to create a truffle project

A Truffle box is already created in the project which includes all the dependencies related to the project, the complete project structure and the code for the user interface as well. The default Truffle directory structure contains the following:

- contracts directory: It contains all the smart contracts for the project and most importantly it has a smart contract named Migration.sol ‘
- migrations directory: These are the contracts which manages the changes occurring in the smart contract and also it checks and manages the compilation and migration process of the smart contract.
- test directory: It contains all the test code for our smart contracts, both in solidity as well as javascript.
- truffle-config.js file: It is the main configuration file.

3.1.3 Developing the Smart Contract

Basically there will be two functions that we will be adding in our contract. One will be for Adopting the pet and the other function will be for retrieving the adopters. For the Adoption function we will retrieve the pet-id and then check if it falls in the range and then the address of the user who called the smart contract will be retrieved using the msg.sender call. And for the retrieving function we will have to return the value of the adopters[3].

3.1.4 Deploying the Smart Contract

The deployment of the smart contract occurs in two phases one is the compilation process and other is the migration process. The compilation of the solidity code has a different aspect to it, It also generates the bytecode which is forwarded to the Ethereum Virtual Machine(EVM) for execution. Basically this translation means the conversion of human readable form of the language to machine readable form that is the one which a virtual machine understands. A migration process describes and changes every different states the application's contract passes through. Initially the state change is just for compiling and migrating the new code the code is replaced by the transition of data or a totally different contract. The format of the migrations is like, the migrations are succeeded by information related to each migration[7].

3.1.5 Testing the Smart Contract

The tests of the smart contract can be either written in solidity or in javascript, henc truffle is proved to be flexible in that way. So there will be various test cases that you can generate and then test the smart contract. Like retrieving a list of particular adopter or the list of all adopters.Basically maintaining a ledger of who adopted which dog.

3.1.6 Develop a UI to interact with smart contract

The basic front-end is completely available with the dependencies it is just that we will be adding the ethereum related dependencies and functions. Hence it is like a basic template which we edit with different functions on the basis of our requirement.

3.1.7 Testing the DApp in the browser

To test the smart contract and interact with the smart contract we neet the Application Binary Interface(ABI). So generally when the contract is compiled the compiler releases one the bytecode and the other the ABI. The ABI makes the application interact with the smart contract. We eventually pass the ABI object to the TruffleContract(),hence the instance of the contract with which we can interact with. After we instantiate out contract we call the web3 provider with the help of App.web3Provider. Eventually we call the markAdopted() function in the contract if there is any pet already adopted and that is separately encapsulated as after the function is called there are changes to be displayed on the user interface [7].

Chapter 4

Universal Logins

4.1 Introduction about Universal Logins

Universal Logins can be broadly classified into the UX problem. It is basically an SDK which you embed with certain part of your code and hence it can be used with any decentralized application. It is meant to ease th User's On-Boarding process. Currently for every new dapp the user creates a new prvate key, backup that seed phrase and transfer ETH into it. This process is faster if you already have ETH, but if you don't it is again elongated as it usually requires credit card or an account in exchange which often requires official documents and wait for some days.Also the user may own multiple devices and they want their devices to be in sync with each other. Currently there is minimal awareness in the users about ethers and private key being one of the reasons of its existence. Some other issues are Users Don't care about ether, Don't care about backing up private keys or seed phrases, Don't understand why they can't use standard two factor authentication, Don't want huge hex-strings, want a simple identifiable username, Don't understand why they can't use their credit card or appstore credit , would rather not download anything on the desktop, Owns multiple devices and switch between them constantly, etc[6].

Some of the core concepts used in Universal logins are:

- Personal multi-Sig Wallet: It is a smart contract used to store personal funds. A user gets his wallet created in a barely noticeable manner. The user then gets engaged incrementally to add authorization factors and recovery options.

- Meta-Transactions: that gives user ability to interact with the smart contract from multiple devices easily, without a need to store ether on each of those devices. Meta-transactions enable payments for execution with tokens.
- ENS Names: naming your wallet with easy-to-remember human-readable name
- Universal Login: a wallet name can be used to log in to dapps, web, and native applications

Similarly there are certain components those are used. They are:

- Contracts: smart contracts used by Universal Login, along with some helper functions
- Relayer: HTTP REST server that relays meta-transactions to Universal Login smart contracts
- SDK: javascript API, a thin communication layer that interacts with the Universal Login ecosystem, via both relayer and Ethereum node.
- React: typescript library, that contains Universal Login main components to use in react applications.

4.1.1 Key Ideas

Some of the features or the Ideas that will improve the on-boarding procss and those are used in the Universal Logins are:

- Context Specific Etherless Accounts: Every App has its own Private Key. User doesn't need to see it or back it up, keep it on the device as safely as possible.
- Identity Smart Contracts: Funds are stored in a proxy contract. The contract accepts the signed messages from these authorized keys, telling it to move funds or execute functions(meta-transactions). Contract is identified with a ENS name instead of the address[11].
- Gas Relay Abstration: They have built a separate relayer which helps the user create it's account without any ether and also initiates the transaction for the users. The amount of ether used for the transaction will be retrieved from the user later.Any system with some amount of ether can become relayer.

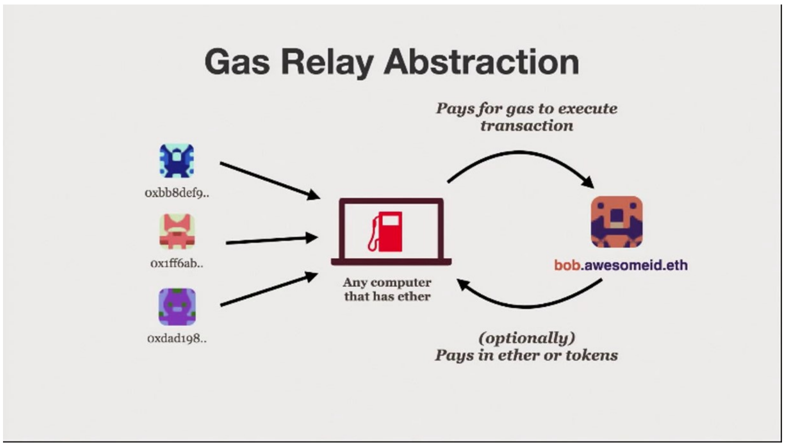


Figure 4.1: Gas Relay Abstraction

- Recovery Options: Backups are done via keys generated for the purpose that might be kept cold and can only be used under specific circumstances. Contract can allow more creative recovery solutions, like deadman's switches or social recoveries.

There is a bit of difference between the on-boarding process for the user's first device and the latter which is shown in below figures[11].

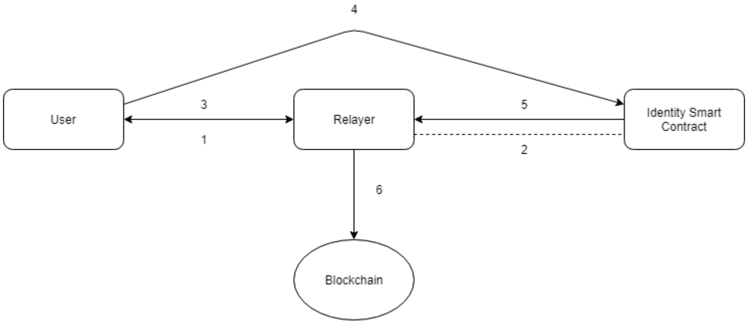


Figure 4.2: Universal Logins(For First Device)

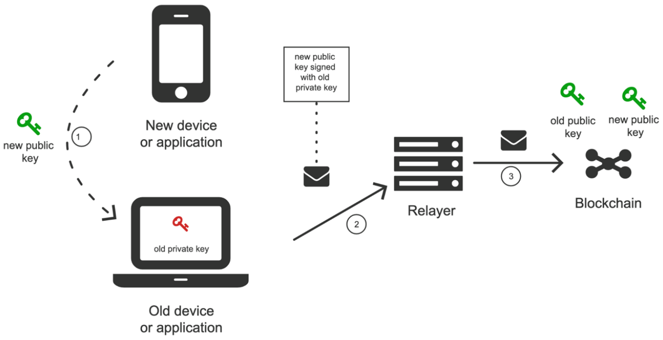

new public key
1
New device or application
new public key signed with old private key
old private key
Old device or application
2
Relayer
3
old public key
new public key
Blockchain

Figure 4.3: Universal Logins(For New Device)

Universal Logins will ease the user's on-boarding into the Ethereum dapp ecosystem.Universal Logins is an active project under Ethereum foundation.

Chapter 5

Perun Networks

It is a 'Layer 2' Protocol especially for financial transactions. This is developed for improving the performance of the current blockchain networks.They have introduced a term called Virtual Payment channels those are created between the users who are not connected through the chain directly or we can say that the two nodes are connected indirectly having some other node from the same network as an intermediary.

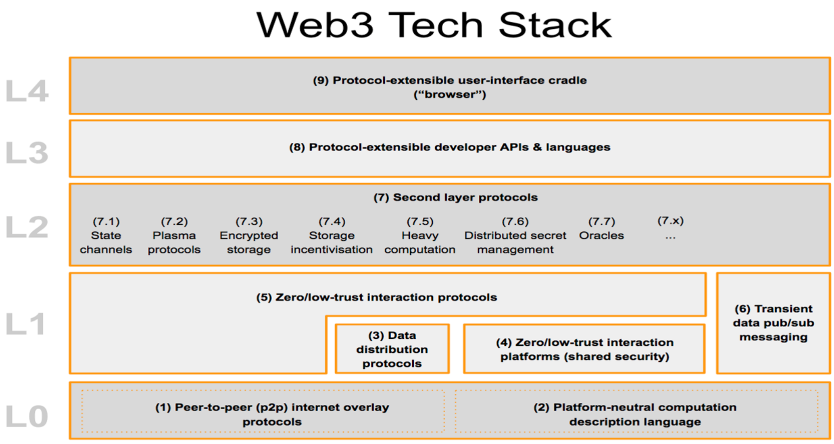

Web3 Tech Stack
L4
(9) Protocol-extensible user-interface cradle ("browser")
L3
(8) Protocol-extensible developer APIs & languages
L2
(7) Second layer protocols
(7.1) State channels
(7.2) Plasma protocols
(7.3) Encrypted storage
(7.4) Storage incentivisation
(7.5) Heavy computation
(7.6) Distributed secret management
(7.7) Oracles
(7.x) ...
L1
(5) Zero/low-trust interaction protocols
(3) Data distribution protocols
(4) Zero/low-trust interaction platforms (shared security)
(6) Transient data pub/sub messaging
L0
(1) Peer-to-peer (p2p) internet overlay protocols
(2) Platform-neutral computation description language

Figure 5.1: Web3-Stack

5.1 Introduction to Perun Networks

Perun is an off-chain channel system that offers a new method for connecting channels that is more efcient than the existing technique of "routing transactions" over multiple channels. Perun introduces a technique called "Virtual Payment Channels" that avoids involvement of intermediary for each individual payment. Let's suppose Alice and Bob are both connected by a channel created over the blockchain with an intermediary payment hub Ingrid. Given these ledger channels, we can establish a virtual channel that establishes a direct (virtual) link between Alice and Bob, where the intermediary Ingrid does not need to get involved in each payment. And the process of transaction goes like initially Alice and Bob tells the smart contract the amount of tokens they reserve for a particular blockchain.That is stored as the root version of the transactions and then with the help of the intermediary the channel between Alice and Bob is created. Hence the transactions will be done till both of them agrees to do or needs to do. In case of dispute both the parties have ample time to show their input to the smart contract in the form of versions and eventually the smart contacts decides the latest version as final and then the channel is closed [4].

5.1.1 Problem with today's blockchain

- Scalability: The system is stll unable to accommodate large-scale users at the same time.
- Security: The security still lacks in many ways and needs to be upgraded to a great extent.
- Privacy: A company revolving around privacy won't benefit from the public ledge system. The public ledger system may disrupt their privacy.
- Slow and Cumbersome: The transaction speed is too slow. If it doesn't speed up soon it may become obsolete.
- Lack of Adequate Skillset: Finding perfectly skilled pupil for developing a blockchain is too tricky. Many people aren't able to tackle the complexity of the network.
- Energy Consumption: Popular consensus mechanism such as POW requires a lot of energy to run smoothly.
- Cryptocurrencies / Digital token legal acceptance: Indian cryptocurrency regulation does not restrict the use of Bitcoin or other cryptocurrencies, but they are also not considered as legal tender.
- Standardization: Part of various working groups under the International Standards Organisation/Technical Committee 307 and working on defining the standards for DLT/blockchain along with many other member countries[8].

- Production Readiness: As technology is in the early stages, there are lots of challenges for the production level adoption. We have derived a framework for production adoption using which companies can adopt the DLT network and scale it for production scenarios.[8]

5.1.2 Performance of Current Blockchain Networks

Throughput of Bitcoin network is 3-7 transactions per second(tps), that of Ethereum Network is 13-15 tps, for quorum it is around 400 tps and for permissioned blockchain, it is around 1000 tps. Also, Performance of a modern blockchain with a more or less standard scheme and consensus may reach thousand's tx/sec under load in real projects (Bitshares, Steemit, EOS, Ethereum, PoA Network), not millions. Scalibility is the foremost issue when we talk about blockhchain and the most commonly discussed scaling challenge for blockchain is increasing transaction throughput. Energy consumption and resource usage is also a major issue with blockchain. A public blockchain consumes more energy as it requires a significant amount of electrical resources to function and achieve network consensus.About private blockchain it is obviously better than public blockchain in case of performance but it compromises the decentralization of the system.

Hence for enhancing the performance of the current blockchain networks the'Layer 2' comes in handy[10] [8].

Chapter 6

Publication

Our paper titled ”A Systematic Framework For State Channel Protocols Identication for Blockchain-based IoT Networks and Applications” is to be published in a conference, which in general provides a framework to choose a specific state channel protocol for the IoT network. Adoption of Blockchain for Internet of Things(IoT) has seen a steady increase of interest for overcoming some key challenges like security, privacy and decentralization. However, most blockchains are computationally expensive, have scalability bottlenecks and, if not adopted efciently may lead to higher transactional costs which are not suitable for most IoT network deployments. State Channel protocols for blockchain networks have been one of the solutions for improving the scalability and minimizing the computation overhead in the system[18]. In this paper, we analyse various state channel protocols and propose a systematic framework to decide upon choosing a specic protocol and apply them for IoT networks as per the needs and requirements of the enterprise. In this paper, we discussed the benets of using state channel protocols in terms of scalability, interoperability, higher throughput, security and privacy to mitigate the concerns using a systematic novel framework[17].

6.1 Proposed Model Architecture

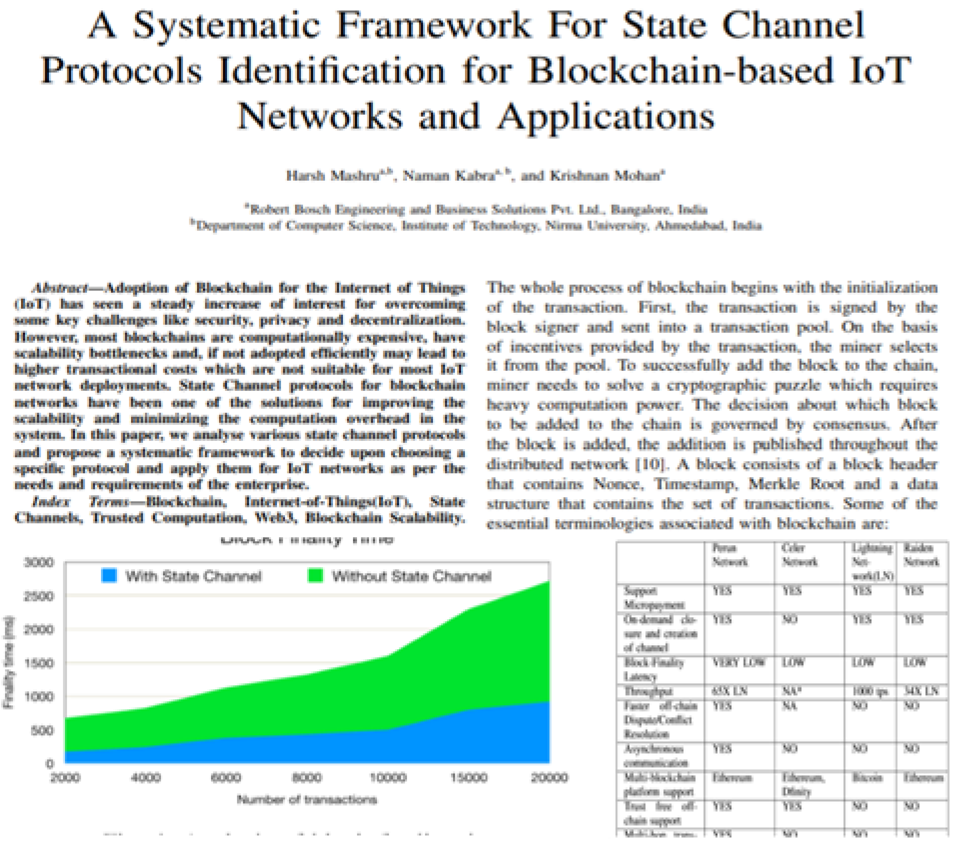
We have a Proposed Model Architecture of how the networks is and how it functions. There are several Edge Devices(EDs) which are capable of collecting and sensing the data from IoT sensors and pre-processing. We consider these edge devices as the mode of transactions between multiple entities involved in the network. The enterprise network consists of three EDs which are up and running in the network. Ledger channel denoted by LC shows that the involved nodes are directly connected over the ledger. ED1 and ED2 are connected through LC. On the other hand, ED1 and ED3 are not directly connected over the ledger and hence to communicate with each other to perform the transaction, we use the concept of Virtual Channel (VC) which implies that there exists a virtual connection amongst the participating node to perform financial transactions. Each edge devices would be governed by the programmable logic written in the general smart contract (GSC)[19]. GSC is responsible for the transactions flow and considering various factors such as privacy, access control mechanisms, transactions cost, abstraction of the data, authentication and validation of the addresses associated with each ED. We consider the consensus mechanism as formulated in the Perun network for governance in the network. GSC also governs the deciding mechanism to call the blockchain network or store the transactions state in the off-chain database. We have designed a generalized flowchart which helps the users to easily choose one best suited to their use-case from the General state channels and the Payment channels. This begins with the very fundamental question on the requirement of the Multi-Party transactions. This comes out to be an important question to consider the necessity of using the BIoT network. If use case demands for the BIoT network, the next question to address is whether the enterprise network can sustain the scalability bottleneck. The solutions to which is the L2 protocols. Finally, we categorise the L2 protocols into two state channels which are Payment channel suitable for economical transactions and General state channels for generic transactions.

6.2 Decision Flow for L2 Protocols Selection

As mentioned earlier we have proposed a framework to select the L2 state channel protocol for the IoT networks. After the decision is taken upon choosing payment or general state channel from the generic flow described earlier, the next question to address is whether the existing network supports state channels or not[14]. If the system does not support the state channels, the enterprise users can opt for sidechain and offchain computation to make the network scalable. If the focus of the enterprise user is not on the block finality latency, then lightning network is one of the suggested solution which claims to support more than 1000 transactions per second. If the primary choice is not throughput, then raiden network can be one of the suggested protocols. If there is a need for Multiblockchain support or interoperability, Celer network supports easy to build,operate and develop off-chain network, on the other hand along with pluggable codebase, Perun network supports asynchronous communication.

6.3 Results and Analysis

The results we provided can be basically divided in two parts one the flowchart and the other the comparison graph. The flowchart based on various requirements suggests whether the L2 Protocols are required for your network requirements or not. We provided some of the parameters based on which we can differentiate all the payment state channel protocols and also helped us to derive the flow. The parameters were selected on the basis of the important functionalities of a payment state channel protocol. Also we did some simulations and have provided the result in the form of the graph. Thus, from the graph we can infer that the BIoT networks with state channels are more effective when we consider large scale networks. In small scale networks, state channels are not preferable due to the larger transaction processing time.Though the complexity of the network increases when we use state channels along with the existing blockchain network.



A Systematic Framework For State Channel Protocols Identification for Blockchain-based IoT Networks and Applications

Harsh Mashru[a,b], Naman Kabra[a, b], and Krishnan Mohan[a]

[a]Robert Bosch Engineering and Business Solutions Pvt. Ltd., Bangalore, India
[b]Department of Computer Science, Institute of Technology, Nirma University, Ahmedabad, India

***Abstract*—Adoption of Blockchain for the Internet of Things (IoT) has seen a steady increase of interest for overcoming some key challenges like security, privacy and decentralization. However, most blockchains are computationally expensive, have scalability bottlenecks and, if not adopted efficiently may lead to higher transactional costs which are not suitable for most IoT network deployments. State Channel protocols for blockchain networks have been one of the solutions for improving the scalability and minimizing the computation overhead in the system. In this paper, we analyse various state channel protocols and propose a systematic framework to decide upon choosing a specific protocol and apply them for IoT networks as per the needs and requirements of the enterprise.**

***Index Terms*—Blockchain, Internet-of-Things(IoT), State Channels, Trusted Computation, Web3, Blockchain Scalability.**

The whole process of blockchain begins with the initialization of the transaction. First, the transaction is signed by the block signer and sent into a transaction pool. On the basis of incentives provided by the transaction, the miner selects it from the pool. To successfully add the block to the chain, miner needs to solve a cryptographic puzzle which requires heavy computation power. The decision about which block to be added to the chain is governed by consensus. After the block is added, the addition is published throughout the distributed network [10]. A block consists of a block header that contains Nonce, Timestamp, Merkle Root and a data structure that contains the set of transactions. Some of the essential terminologies associated with blockchain are:

	Perun Network	Celer Network	Lightning Network(LN)	Raiden Network
Support Micropayment	YES	YES	YES	YES
On-demand closure and creation of channel	YES	NO	YES	YES
Block-Finality Latency	VERY LOW	LOW	LOW	LOW
Throughput	65X LN	NA*	1000 tps	34X LN
Faster off-chain Dispute/Conflict Resolution	YES	NA	NO	NO
Asynchronous communication	YES	NO	NO	NO
Multi-blockchain platform support	Ethereum	Ethereum, Dfinity	Bitcoin	Ethereum
Trust free off-chain support	YES	YES	NO	NO
Multi-hop trans-	YES	NO	NO	NO

Figure 6.1: Snapshot of the Paper

Chapter 7

DLT Enabled IoT devices

The vision for the project is enabling IoT devices to have blockchain functions such as transaction signing and transaction verification. My work basically focuses on assessing the blockchain capalbilities that can run on IoT and Edge devices. According to a survey there will be more than 20 billion IoT devices being connected to the Internet. In todays enterprise deployement IoT devices are the major data sources[13]. The Increasing presence of IoT will have a great impact on our daily lives, but to unleash its full potential many challenges must be solved. Challenges are Data Integrity, Security, Privacy, Verification and Authenticity of data, Storage capabilities, Processing power, etc. Distributed Ledger Technology such as Blockchain provide Immutability, Decentralization, Privacy Preserving smart contracts which potentially addresses the above mentioned challenges. Additionally blockchain can also be used to manage the device identities in a large scale[12].

7.1 Use Case

The core idea is to provide incentivization for IoT devices while performing condition monitoring transactions.The Bosch specific sensor devices named XDK are used for the implementation purpose. Currently two XDK devices communicate with each other and store the transaction in the blockchain. Basically, two constraint embedded devices securely exchange encrypted sensor data against a payment. We will call the first edge device as the producer and the other edge device as the consumer[16].

The producer will sense the data like temperature, humidity and acceleration for an instance. And the consumer will request to nut that data for which there will be a financial transaction between them.The Meta mask wallet is used to monitor the financial transaction. Also it isnt necessary for a consumer to retrieve all the data that is recorded, it can get the data according to its need. The conditions of which are mentioned in a REST Api, can be helpful if different consumer requests for multiple data. Basically the complete flow of the request response for the data goes like: First the producer produces the data, then the consumer requests for the Smart contract address that is deployed with the help of producer and hence stored with it. This communication is done off-chain. Then the producer sends the contract address where the consumer stores its public key. Though the smart contract stores the public key as well as the address of the consumer. After the consumer recieves the transaction confirmation from the blockchain, i directly requests for the recorded data from the producer. The producer then reads the required information and encrypts the data locally with consumers public key.Furthermore, the Producer also stores the associated unique Ethereum account address and is therefore able to authenticate the Consumer. With this information locally available at the Producer, it removes the need to rewrite the Consumers RSA public key into the blockchain during a later communication cycle[16]. This means, after the public key is written once, the authenticated Consumer can now directly communicate with the Producer. So, the Consumer pays only once during the write public key transaction for the data until the Producer decides to delete the locally stored Consumer information. Finally the encrypted data is sent to the consumer which only the consumer can decrypt. For authentication the consumer calculates the data hash and compares it with the one that is stored in the smart contract by the consumer, hence it could be clear if there is any tamper of data in between. At the end there is a evauation system through voting, where voting is done by the consumer who has done the payment recently. Every other in the network is excluded from it. And the producer and consumers and incentivized on the basis of votes[16].

As mentioned earlier, eventually a REST Api is developed which helps the consumer to select what data it needs, in the sense only Temperture or Humidity or acceleration or any combined.

Chapter 8

Conclusion

Blockchain is a technology currently which is adapted at a great pace despite some of the flaws which are under research currently. Everyday there is something new that is invented or innovated in the field of blockchain. So here I have had my hands on Public blockchain and started with learning the technology and then some hands on in the UX problems and finally into the Layer 2 blockchain.Perun Networks or the Layer 2 blockchain can be said the core work from all the above mentioned. That focuses on the specific issue of the performance of the technology and helps to enhance it. Where as Universal Logins are equally helpful and beneficial for the technology but thy are ethereum specific solution and hence may be extended to public blockchain networks.State channels would help te IoT networks to be better and hence based on that is the paper we published which we inferred from our studies on Perun Networks. Eventually there is the need of the infrastructure for the hardware devices to communicate and hence we implemented the Blockhain Enabled IoT devices, Though state channels makes the networks complex but at the end it is more secure and reliable. Also currently enterprise blockchain is used when we take the market into consideration, hence our current and futue work is to evaluate the flavor of Hyperledger framework that is Hyperledger Avalon.

Bibliography

[1] Imran Bashir, MAstering Blockchain, Packt Publishing, 2018.

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, cryptography mailing list at metzdowd.com, 2008.

[3] Dr. Gavin Wood, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, North American Bitcoin Conference, 2014.

[4] Stefan Dziembowski and Lisa Eckey and Sebastian Faust and Daniel Malinowski,Perun: Virtual Payment Hubs over Cryptocurrencies, International Association for Cryptographic Research, 2018.

[5] AnyLedger: Embedded wallet for decentralized IoT
`file:///C:/Users/hmr9kor/Desktop/Perun-Pre/whitepaperAnyLedger.pdf`

[6] Universal Logins,
`https://universalloginsdk.readthedocs.io/en/latest/overview.htmlintroduction`

[7] Pet-Shop Tutorial,
`https://www.trufflesuite.com/tutorials/pet-shop`

[8] Layer 2 Review,
`https://hackernoon.com/`
`2019-blockchain-layer-2-solution-review-d0038514739`

[9] Challenges for blockchain to overcome,
`https://www.cnbc.com/2018/10/01/`
`five-crucial-challenges-for-blockchain-to-overcome-deloitte.html`

[10] Layer-2 Bockchain,
`https://www.coindesk.com/layer-2-blockchain-tech-even-bigger-deal-think`

[11] https://medium.com/limechain/part-two-second-layer-solutions-a-journey-into-meta-transactions-

[12] Blockchain Enabled Cyber-Physical Systems,
Rathore, Mohamed, Guizani,. (2020). A Survey of Blockchain Enabled Cyber-Physical Systems. Sensors. 20. 282. 10.3390/s20010282.

[13] Blockchain and IoT Integration,
Panarello, Alfonso Tapas, Nachiket Merlino, Giovanni Longo, Francesco Puliafito, Antonio. (2018). Blockchain and IoT Integration: A Systematic Survey. Sensors. 18. 2575. 10.3390/s18082575.

[14] Counterfactual,
Coleman, Jeff, Liam Horne, and Li Xuanji. "Counterfactual: Generalized state channels." (2018).

[15] Hyperledeger Avalon,
https://www.hyperledger.org/projects/avalon

[16] XDKonEthereum,
https://github.com/boschresearch/XDK_on_Ethereum

[17] FairSwap,
U: Peun Networks How to fairly exchange goods.pdf

[18] Lightning Network
https://lightning.network/lightning-network-paper.pdf

[19] Concurrency and Privacy with Payment-Channel Networks,
https://eprint.iacr.org/2017/820.pdf