ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 8, August 2018

Decentralized Public / Private Ledger Technology and It's Applications

Akshat Minesh Doshi[1]

School of Engineering and Applied Science, Ahmedabad University, Ahmedabad, India[1]

Abstract: Block Chain (BC), the technology behind the Bitcoin crypto-currency system. Blockchain helps Build Trusted, Powerful and Transparent Process with the potential to disrupt Intermediaries, Third parties & Expensive processes. Proof-of-Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), consensus algorithm plays a vital role in ensuring BC security by maintaining a digital ledger of transactions, which is considered to be incorruptible. Firstly, we explore top crypto currencies after that we will explore blockchain and mining concept. In further we will be exploring Ethereum blockchain solidity programming more and make DAPPs on Ethereum blockchain network.

Keywords: Crypto Currency, Block Chain, Ethereum, DAPPs

I. INTRODUCTION

Blockchain, the technology behind Bitcoin, seems to be the driving technology behind the next generation Internet, also referred to the Decentralized Web, or the Web3. The Blockchain is a novel solution to the age-old human problem of trust. It provides an architecture for so-called trustless trust. It allows us to trust the outputs of the system without trusting any actor within it. Blockchain is a shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls. It is a distributed database that maintains a continuously growing list of transaction data records, cryptographically secured from tampering and revision. A Blockchain protocol operates on top of the Internet, on a P2P Network of computers that all run the protocol and hold an identical copy of the ledger of transactions, enabling P2P value transactions without a middleman though machine consensus. Blockchain itself a file - a shared and public ledger of transactions that records all transactions from the genesis block (first block) until today. The ledger is built using a linked list, or chain of blocks, where each block contains a certain number of transactions that were validated by the network in a given time span. The crypto-economic rule sets of the Blockchain protocol (consensus layer) regulate the behavioral rule sets and incentive mechanism of all stakeholders in the network. This ledger runs on a Peer-to-Peer (P2P) network of computers. Distributed consensus based on economic incentive mechanisms combined with cryptography allows for secure P2P validation of transactions, thus bypassing the need for traditional trusted third parties. Instead of a single trusted third party validating transactions through their servers with authority (single vote), a peer-to-peer network of computers running the Blockchain protocol validates transactions by consensus (majority vote). The Blockchain protocol, therefore, formalizes pre-defined consensus rules for approving transactions on the P2P network, as hard-coded governance rules, managing and auto enforcing transactions of all participants in the network.

II. USE OF BLOCKCHAIN BEYOND CRYPTOCURRENCY

Although the Internet is a great tool to aid every sphere of the modern digital life, it is still highly flawed in terms of the lack of security and privacy, especially when it comes to Fintech, social media and E-commerce. Blockchain, the technology behind crypto-currency, brought forth a new revolution by providing a mechanism for Peer-to-Peer (P2P) transactions without the need for any intermediary body such as the existing commercial banks. BC validates all the transactions and preserves a permanent record of them while making sure that any identification related information of the users are kept incognito. Thus all the personal information of the users are sequestered while substantiating all the transactions. This is achieved by reconciling mass collaboration by cumulating all the transactions in a computer code based digital ledger. Thus, by applying Blockchain or similar crypto-currency techniques, the users neither need to trust each other nor do they need an intermediator; rather the trust is manifested within the decentralized network system itself. Blockchain thus appears to be the ideal "Trust Machine" paradigm. In fact, Bitcoin is just an exemplary use of the Blockchain. Blockchain is considered to be a novel revolution in the domain of computing enabling limitless applications such as storing and verifying legal documents including deeds and various certificates, healthcare data, IoT, Cloud and so forth. Tapscott rightly indicated Blockchain to be the "World Wide Ledger", enabling many new applications beyond verifying transactions such as in: smart deeds, decentralized and/or autonomous organizations/ government services etc.

DOI 10.17148/IJARCCE.2018.785

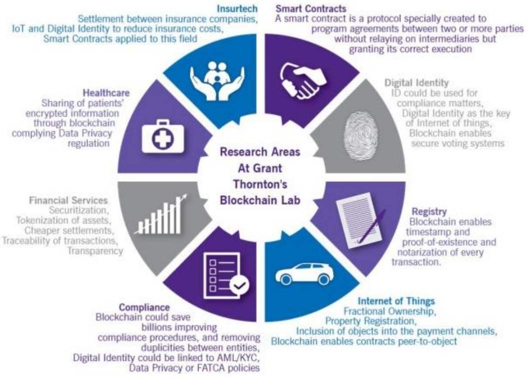

Insurtech
Settlement between insurance companies, IoT and Digital Identity to reduce insurance costs, Smart Contracts applied to this field
Smart Contracts
A smart contract is a protocol specially created to program agreements between two or more parties without relaying on intermediaries but granting its correct execution
Healthcare
Sharing of patients' encrypted information through blockchain complying Data Privacy regulation
Digital Identity
ID could be used for compliance matters, Digital Identity as the key of Internet of things, Blockchain enables secure voting systems
Research Areas At Grant Thornton's Blockchain Lab
Financial Services
Securitization, Tokenization of assets, Cheaper settlements, Traceability of transactions, Transparency
Registry
Blockchain enables timestamp and proof-of-existence and notarization of every transaction.
Compliance
Blockchain could save billions improving compliance procedures, and removing duplicities between entities, Digital Identity could be linked to AML/KYC, Data Privacy or FATCA policies
Internet of Things
Fractional Ownership, Property Registration, Inclusion of objects into the payment channels, Blockchain enables contracts peer-to-object

Fig 1: Blockchain Use Cases

III. TECHNOLOGY FUNDAMENTALS OF BLOCKCHAIN

This section briefly describes the fundamentals of the technology behind the Blockchain. A Blockchain comprises of two different components, as follows:

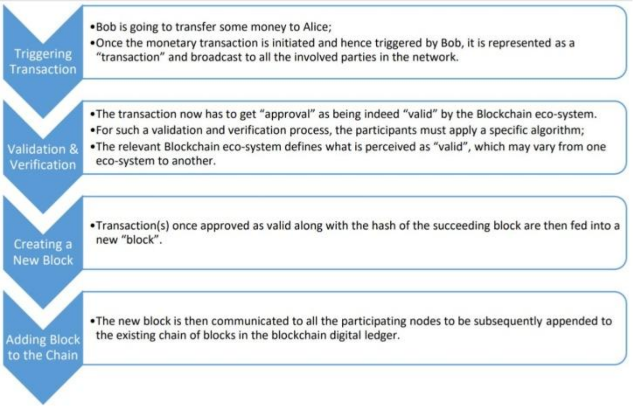
1. **Transaction**: A transaction, in a Blockchain, represents the action triggered by the participant.
2. **Block**: A block, in a Blockchain, is a collection of data recording the transaction and other associated details such as the correct sequence, timestamp of creation, etc.

The Blockchain can be either public or private, depending on the scope of its use. A public Blockchain enables all the users with read and write permissions such as in Bitcoin, access to it. However, some public Blockchain limit the access to only either to read or to write.

Another major advantage of the Blockchain technology is that it is decentralized. It is decentralized in the sense that:

- There is no single device that stores the data (transactions and associated blocks), rather they are distributed among the participants throughout the network supporting the Blockchain.
- The transactions are not subject to approval of any single authority or have to abide by a set of specific rules, thus involving substantial trust as to reach a consensus.
- The overall security of a Blockchain eco-system is another advantage. The system only allows new blocks to be appended. Since the previous blocks are public and distributed, they cannot be altered or revised.

For a new transaction to be added to the existing chain, it has to be validated by all the participants of the relevant Blockchain eco-system. For such a validation and verification process, the participants must apply a specific algorithm. The relevant Blockchain eco-system defines what is perceived as "valid", which may vary from one eco-system to another. A number of transactions, thus approved by the validation and verification process, are bundled together in a block. The newly prepared block is then communicated to all other participating nodes to be appended to the existing chain of blocks. Each succeeding block comprises a hash, a unique digital fingerprint, of the preceding one.


Triggering Transaction

- Bob is going to transfer some money to Alice;
- Once the monetary transaction is initiated and hence triggered by Bob, it is represented as a "transaction" and broadcast to all the involved parties in the network.

Validation & Verification

- The transaction now has to get "approval" as being indeed "valid" by the Blockchain eco-system.
- For such a validation and verification process, the participants must apply a specific algorithm;
- The relevant Blockchain eco-system defines what is perceived as "valid", which may vary from one eco-system to another.

Creating a New Block

- Transaction(s) once approved as valid along with the hash of the succeeding block are then fed into a new "block".

Adding Block to the Chain

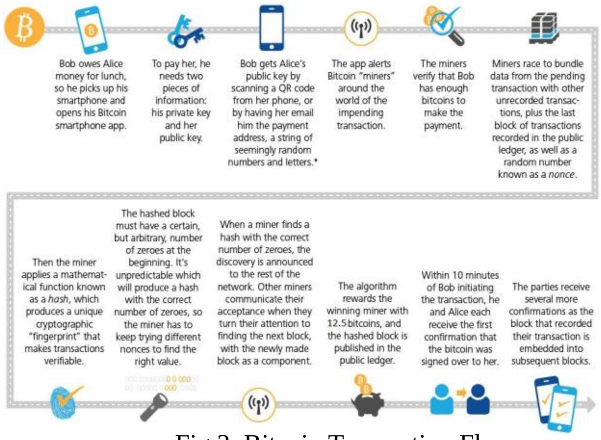
- The new block is then communicated to all the participating nodes to be subsequently appended to the existing chain of blocks in the blockchain digital ledger.

Fig 2: Transaction Flow

Below figures demonstrates how Blockchain transactions takes place, using a systematic example. Bob is going to transfer some money to Alice. Once the monetary transaction is initiated and hence triggered by Bob, it is represented as a "transaction" and broadcast to all the involved parties in the networks. The transaction now has to get "approval" as

DOI 10.17148/IJARCCE.2018.785

being indeed "valid" by the Blockchain eco-system. Transaction(s) once approved as valid along with the hash of the succeeding block are then fed into a new "block" and communicated to all the participating nodes to be subsequently appended to the existing chain of blocks in the Blockchain digital ledger.



Bob owes Alice money for lunch, so he picks up his smartphone and opens his Bitcoin smartphone app.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

The app alerts Bitcoin "miners" around the world of the impending transaction.

The miners verify that Bob has enough bitcoins to make the payment.

Miners race to bundle data from the pending transaction with other unrecorded transactions, plus the last block of transactions recorded in the public ledger, as well as a random number known as a *nonce*.

Then the miner applies a mathematical function known as a *hash*, which produces a unique cryptographic "fingerprint" that makes transactions verifiable.

The hashed block must have a certain, but arbitrary, number of zeroes at the beginning. It's unpredictable which will produce a hash with the correct number of zeroes, so the miner has to keep trying different nonces to find the right value.

When a miner finds a hash with the correct number of zeroes, the discovery is announced to the rest of the network. Other miners communicate their acceptance when they turn their attention to finding the next block, with the newly made block as a component.

The algorithm rewards the winning miner with 12.5 bitcoins, and the hashed block is published in the public ledger.

Within 10 minutes of Bob initiating the transaction, he and Alice each receive the first confirmation that the bitcoin was signed over to her.

The parties receive several more confirmations as the block that recorded their transaction is embedded into subsequent blocks.

Fig 3: Bitcoin Transaction Flow

IV. PERMISSIONLESS AND PERMISSIONED BLOCKCHAINS

There are various categorizations of Blockchain types, and for the purposes of this chapter we will focus on the different types of Blockchain according to whether authorization is required for network nodes which act as verifiers, and whether access to the Blockchain data itself is public or private For the first categorization we have:

- Permission less Blockchains, where anyone can participate in the verification process, i.e. no prior authorization is required and a user can contribute his/her computational power, usually in return for a monetary reward.
- Permissioned Blockchains, where verification nodes are preselected by a central authority or consortium.

For the second categorization we have:

- Public Blockchains, where anyone can read and submit transactions to the Blockchain.
- Private Blockchains, where this permission is restricted to users within an organization or group of organizations.

In reality, most permission less Blockchains feature public access, while the intention of most permissioned Blockchains is to restrict data access to the company or consortium of companies that operate the Blockchain. For this reason, we collapse the categorization into two types, permissioned and permission less Blockchains, and we elaborate the distinction between them in the following section.

V. COMPARISON OF DIFFERENT CRYPTOCURRENCIES AND BLOCKCHAIN IMPLEMENTATIONS

There are more than 10,000 of cryptocurrency available in the market but we will only focus on top cryptocurrencies like Bitcoin, Ethereum, Ripple, IoTA, SiaCoin, Dash, Neo, Hyperledger, Bitcoin Cash, Litecoin, Monero.

A. Bitcoin

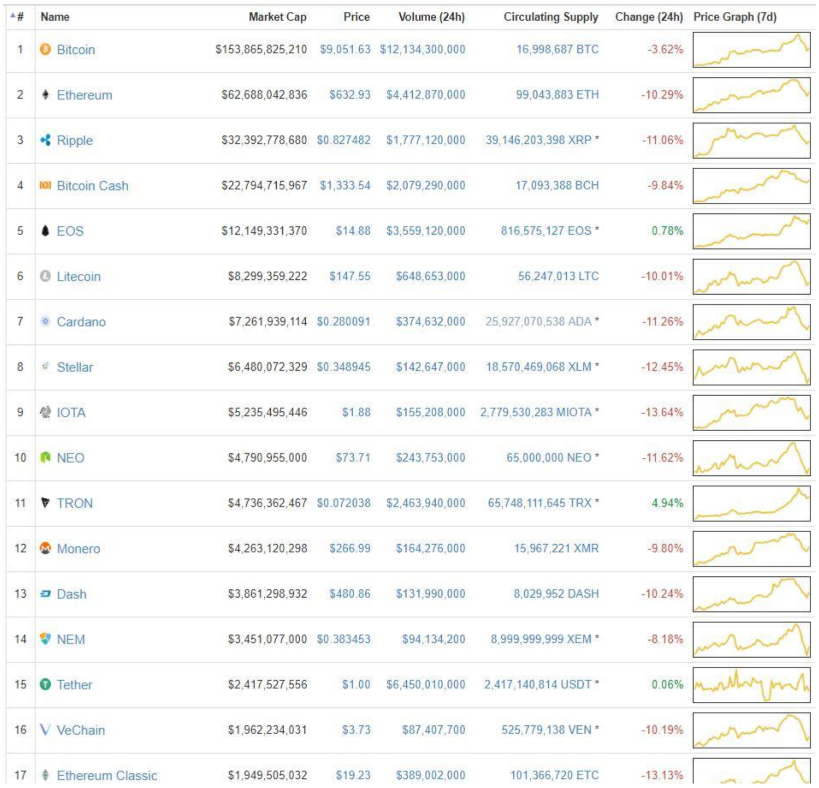
Bitcoin is a digital asset and payment system where users can perform transactions without any intermediary system. The original source code of Bitcoin includes an implementation of a Blockchain. The Bitcoin Blockchain stores data on transactions, which indicate the amount of currency that moved between two or more accounts.

New bitcoins are generated through a process called mining, and is performed by nodes called miners. First, a miner consolidates one or more transactions into a block. Next, they calculate a proof-of-work for that block so it can be approved by the network. This is done by creating a hash of the block. As long as the hash is not numerically less than the current difficulty target, the minor changes the nonce field in the block so the block's hash also changes. Once the hash is less than the target, the miner transmits the block across the Bitcoin network. Lastly, if the block is accepted by the entire network, the miner receives a reward in the form of newly generated bitcoin.

B. Ethereum

Ethereum is an open Blockchain platform that lets anyone build and use decentralized applications that run on Blockchain technology. Like Bitcoin no one controls or owns Ethereum. It is an open-source project build by many people around the world. Ethereum is adaptable and flexible unlike the Bitcoin protocol. The majority of token sales happen on the Ethereum platform, using the ERC-20 token standard.

Decentralized computing platform which features its own Turing-complete programming language. The Blockchain records scripts or contracts that are run and executed by every participating node, and are activated through payments with the native crypto currency 'ether'. Officially launched in 2015, Ethereum has attracted significant interest from many developers and institutional actors.



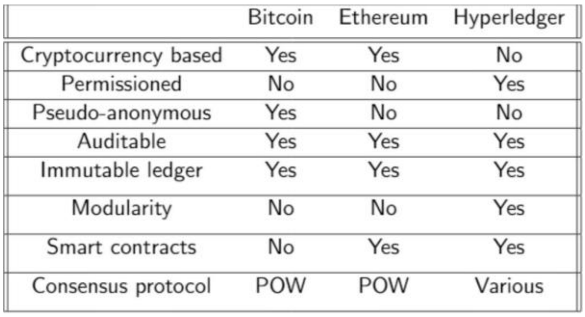
▲#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$153,865,825,210	$9,051.63	$12,134,300,000	16,998,687 BTC	-3.62%	
2	Ethereum	$62,688,042,836	$632.93	$4,412,870,000	99,043,883 ETH	-10.29%	
3	Ripple	$32,392,778,680	$0.827482	$1,777,120,000	39,146,203,398 XRP *	-11.06%	
4	Bitcoin Cash	$22,794,715,967	$1,333.54	$2,079,290,000	17,093,388 BCH	-9.84%	
5	EOS	$12,149,331,370	$14.88	$3,559,120,000	816,575,127 EOS *	0.78%	
6	Litecoin	$8,299,359,222	$147.55	$648,653,000	56,247,013 LTC	-10.01%	
7	Cardano	$7,261,939,114	$0.280091	$374,632,000	25,927,070,538 ADA *	-11.26%	
8	Stellar	$6,480,072,329	$0.348945	$142,647,000	18,570,469,068 XLM *	-12.45%	
9	IOTA	$5,235,495,446	$1.88	$155,208,000	2,779,530,283 MIOTA *	-13.64%	
10	NEO	$4,790,955,000	$73.71	$243,753,000	65,000,000 NEO *	-11.62%	
11	TRON	$4,736,362,467	$0.072038	$2,463,940,000	65,748,111,645 TRX *	4.94%	
12	Monero	$4,263,120,298	$266.99	$164,276,000	15,967,221 XMR	-9.80%	
13	Dash	$3,861,298,932	$480.86	$131,990,000	8,029,952 DASH	-10.24%	
14	NEM	$3,451,077,000	$0.383453	$94,134,200	8,999,999,999 XEM *	-8.18%	
15	Tether	$2,417,527,556	$1.00	$6,450,010,000	2,417,140,814 USDT *	0.06%	
16	VeChain	$1,962,234,031	$3.73	$87,407,700	525,779,138 VEN *	-10.19%	
17	Ethereum Classic	$1,949,505,032	$19.23	$389,002,000	101,366,720 ETC	-13.13%	

Fig 4: Top Crypto Currencies

C. Hyperledger

Many companies have come together to form Hyperledger, a Linux Foundation project whose goal is to advance Blockchain technology to benefit a variety of business use cases. There are many projects associated with Hyperledger. Subsequent sections of this document will describe three of the Hyperledger frameworks: Hyperledger Fabric, Hyperledger Sawtooth, and Hyperledger Iroha. These projects provide users with the tools to deploy their own Blockchains.

Hyperledger Fabric (HLF) likes to call its smart contracts 'chaincode'. HLF is an enterprise permissioned Blockchain, built with great flexibility, which makes it very useful for businesses as their business rules change after approximately 7 years. Most other Blockchains are not built considering flexibility.



	Bitcoin	Ethereum	Hyperledger
Cryptocurrency based	Yes	Yes	No
Permissioned	No	No	Yes
Pseudo-anonymous	Yes	No	No
Auditable	Yes	Yes	Yes
Immutable ledger	Yes	Yes	Yes
Modularity	No	No	Yes
Smart contracts	No	Yes	Yes
Consensus protocol	POW	POW	Various

Fig 5: Blockchain Comparison

D. Dash

Decentralized computing platform which features its own Turing-complete programming language. The Blockchain records scripts or contracts that are run and executed by every participating node, and are activated through payments with the native cryptocurrency 'ether'. Officially launched in 2015, Ethereum has attracted significant interest from many developers and institutional actors.

DOI 10.17148/IJARCCE.2018.785

E. Monero

Cryptocurrency system that aims to provide anonymous digital cash using ring signatures, confidential transactions and stealth addresses to obfuscate the origin, transaction amount and destination of transacted coins. Launched in 2014, it saw a substantial increase in market value in 2016.

F. Ripple

Only cryptocurrency in this list that does not have a Blockchain but instead uses a 'global consensus ledger'. The Ripple protocol is used by institutional actors such as large banks and money service businesses. A function of the native token XRP is to serve as a bridge currency between national currency pairs that are rarely traded, and to prevent spam attacks.

G. Litecoin

Litecoin was launched in 2011 and is considered to be the 'silver' to bitcoin's 'gold' due to its more plentiful total supply of 84 million LTC. It borrows the main concepts from bitcoin but has altered some key parameters (e.g., the mining algorithm is based on Script instead of bitcoin's SHA-265).

VI. SMART CONTRACTS

A smart contract is a computer code running on top of a Blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation. It is a mechanism involving digital assets and two or more parties, where some or all of the parties deposit assets into the smart contract and the assets automatically are redistributed among those parties according to a formula based on certain data, which is not known at the time of contract initiation. Smart Contracts, along with the Blockchain, are the basis of all Decentralized Applications. They are, like Blockchain, immutable and distributed, which means upgrading them will be a pain if they are already on the Ethereum Network.

The term smart contract is a bit unfortunate since a smart contract is neither smart nor are they to be confused with a legal contract:

- A smart contract can only be as smart as the people coding taking into account all available information at the time of coding.
- While smart contracts have the potential to become legal contracts if certain conditions are met, they should not be confused with legal contracts accepted by courts and or law enforcement. However, we will probably see a fusion of legal contracts and smart contracts emerge over the next few years as the technology becomes more mature and widespread and legal standards are adopted.

VII. TOKENS

Tokens are a representation of a particular asset or utility that usually resides on top of another Blockchain. Creating tokens is a much easier process as you do not have to modify the codes from a particular protocol or create a Blockchain from scratch. All you have to do is follow a standard template on the Blockchain – such as on the Ethereum or Waves platform – that allows you to create your own tokens. Tokens are created and distributed to the public through an Initial Coin Offering (ICO), which is a means of crowdfunding, through the release of a new cryptocurrency or token to fund project development. It is similar to an Initial Public Offering (IPO) for stocks. It is important to note that all coins or tokens are regarded as crypto currencies, even if most of the coins do not function as a currency or medium of exchange. The term cryptocurrency is a misnomer since a currency technically represents a unit of account, a store of value and a medium of exchange. The main difference between altcoins and tokens is in their structure; altcoins are separate currencies with their own separate Blockchain while tokens operate on top of a Blockchain that facilitates the creation of decentralized applications.

A. ERC20 Based Token Example

ERC stands for Ethereum Request for Comments. This is an official protocol for proposing improvements to the Ethereum network. '20' is the unique proposal ID number.

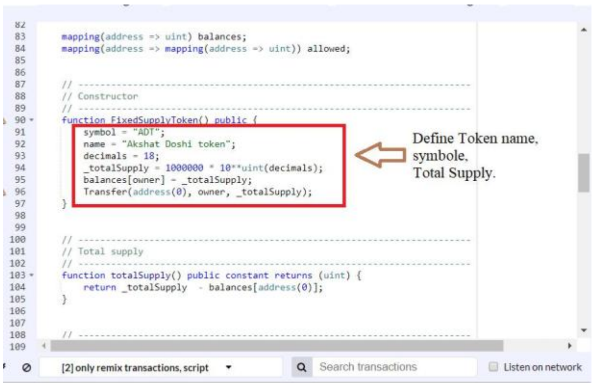
ERC20 defines a set of rules which need to be met in order for a token to be accepted and called an 'ERC20 Token'. The standard rules apply to all ERC20 Tokens since these rules are required to interact with each other on the Ethereum network. These tokens are Blockchain assets that can have value and can be sent and received, like Bitcoin, Litecoin, Ethereum, or any other cryptocurrency. We will understand and make ERC20 based token systematically.

DOI 10.17148/IJARCCE.2018.785

Step 1: Decide what you want your token to be.

In order to create an ERC20 token, you need the following:

- The Token's Name
- The Token's Symbol
- The Token's Decimal Places
- The Number of Tokens in Circulation



```
    mapping(address => uint) balances;
    mapping(address => mapping(address => uint)) allowed;


    // ------------------------------------------------------------------------
    // Constructor
    // ------------------------------------------------------------------------
    function FixedSupplyToken() public {
        symbol = "ADT";
        name = "Akshat Doshi token";
        decimals = 18;
        _totalSupply = 1000000 * 10**uint(decimals);
        balances[owner] = _totalSupply;
        Transfer(address(0), owner, _totalSupply);
    }


    // ------------------------------------------------------------------------
    // Total supply
    // ------------------------------------------------------------------------
    function totalSupply() public constant returns (uint) {
        return _totalSupply  - balances[address(0)];
    }


    // ------------------------------------------------------------------------
```

Fig 6: Defining Parameters

Step 2: Code the Contract

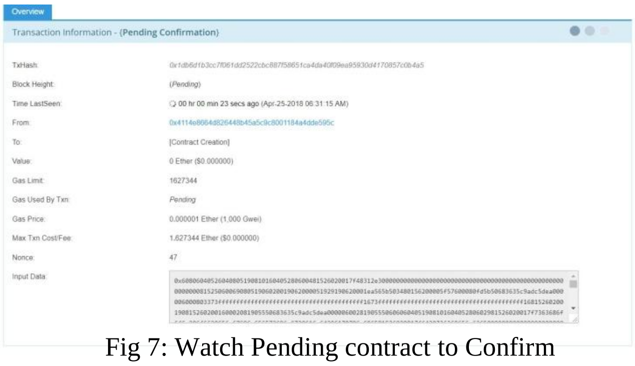
ERC20 contract sample code is available on their website (www.ethereum.org). We just need to change the code according to our requirements.

Step 3: Test The Token on The TestNet

Next we're going to deploy the contract to the Test Net to see if it works. It sucks to deploy a contract to the MainNet, pay for it, and then watch it fail. So we will first download Metamask for run our contract on the test network.

Step 4: Watch The Custom Token

Now you can actually send tokens that you have made on the test network using Metamask. You can also see the whole sending and receiving process live on etherscan.io.

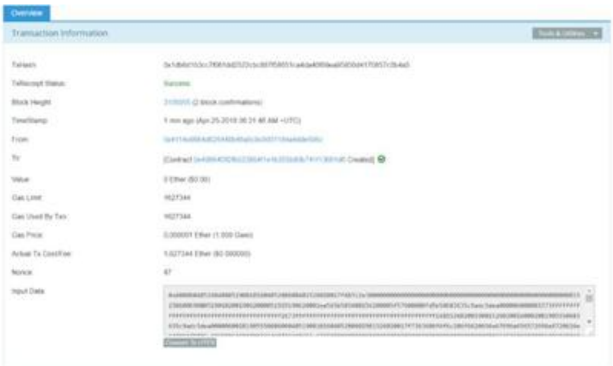


Transaction Information - (Pending Confirmation)

TxHash: 0x1db6d1b3cc7f061dd2522cbc887f58651ca4da40f09ea95930d4170857c0b4a5
Block Height: (Pending)
Time LastSeen: 00 hr 00 min 23 secs ago (Apr-25-2018 06:31:15 AM)
From: 0x4114e8664d826448b45a5c9c8001184a4dde595c
To: [Contract Creation]
Value: 0 Ether ($0.000000)
Gas Limit: 1627344
Gas Used By Txn: Pending
Gas Price: 0.000001 Ether (1,000 Gwei)
Max Txn Cost/Fee: 1.627344 Ether ($0.000000)
Nonce: 47
Input Data:

```
0x60806040526040805190810160405280600481526020017f48312e30000000000000000000000000000000000000000000000000
000000008152506006908051906020019062000051929190620001ea565b503480156200005f57600080fd5b50683635c9adc5dea000
006000803373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200
190815260200160002081905550683635c9adc5dea00000600281905550606060405190810160405280602981526020017f7363686f
```

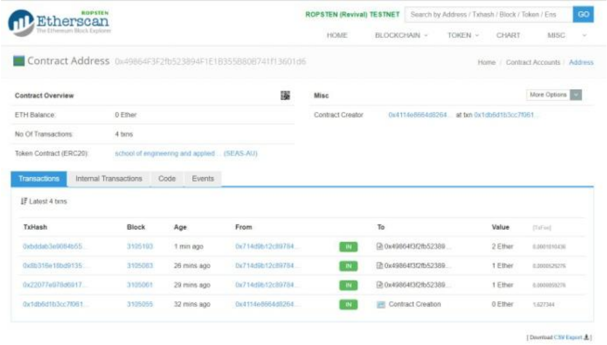
Fig 7: Watch Pending contract to Confirm



Transaction Information

TxHash: [illegible]
TxReceipt Status: Success
Block Height: [illegible] (2 block confirmations)
TimeStamp: 1 min ago (Apr-25-2018 06:31:48 AM +UTC)
From: [illegible]
To: [Contract [illegible] Created]
Value: 0 Ether ($0.00)
Gas Limit: 1627344
Gas Used By Txn: 1627344
Gas Price: 0.000001 Ether (1,000 Gwei)
Actual Tx Cost/Fee: 1.627344 Ether ($0.000000)
Nonce: 47
Input Data: [illegible]

Fig 8: Contract is Successfully Deployed on Ropsten Network


ROPSTEN Etherscan The Ethereum Block Explorer

ROPSTEN (Revival) TESTNET Search by Address / Txhash / Block / Token / Ens GO

HOME BLOCKCHAIN TOKEN CHART MISC

Contract Address 0x49864F3F2fb523894F1E1B355B808741f13601d6

Home / Contract Accounts / Address

Contract Overview

ETH Balance:	0 Ether
No Of Transactions:	4 txns
Token Contract (ERC20):	school of engineering and applied ... (SEAS-AU)

Misc

More Options

Contract Creator: 0x4114e8664d8264... at txn 0x1db6d1b3cc7f061...

Transactions | Internal Transactions | Code | Events

Latest 4 txns

TxHash	Block	Age	From		To	Value	[TxFee]
0xbddab3e9084b55...	3105193	1 min ago	0x714d9b12c89784...	IN	0x49864f3f2fb52389...	2 Ether	0.0001010436
0x8b316e18bd9135...	3105083	26 mins ago	0x714d9b12c89784...	IN	0x49864f3f2fb52389...	1 Ether	0.0000525276
0x22077e978d6917...	3105061	29 mins ago	0x714d9b12c89784...	IN	0x49864f3f2fb52389...	1 Ether	0.0000593276
0x1db6d1b3cc7f061...	3105055	32 mins ago	0x4114e8664d8264...	IN	Contract Creation	0 Ether	1.627344

[Download CSV Export]

Fig 9: Permanent contract deployed on Ethereum Blockchain

VIII. MINING

Cryptocurrency mining, or crypto mining, is a process in which transactions for various forms of cryptocurrency are verified and added to the Blockchain digital ledger. Also known as crypto coin mining, altcoin mining, or Bitcoin mining (for the most popular form of cryptocurrency, Bitcoin), cryptocurrency mining has increased both as a topic and activity as cryptocurrency usage itself has grown exponentially in the last few years.

There is mainly three type of mining happening nowadays:

- Solo Mining: Solo mining is the process of mining alone. In realistic timeframes, though pooled mining definitely is the better way if your hardware has only small hash rate. A wild guess here is that it would take more than several tens of TH/s (that is Terrahashes per second, which is 1000 GH/s) to get more out of solo mining than pooled mining.
- Pool Mining: In a mining pool, different users organize together in order to provide computing power for the bitcoin/altcoin network. If a Bitcoin block is newly created, each of the users in the mining pool receives its fair share proportionately to his mining power.
- Cloud Mining: Classical cryptocurrency mining requires huge investments in hardware and electricity. Cloud mining companies aim to make mining accessible to everybody. People just can log in to a website and invest money in the company that already has mining datacenters.

IX. ETHEREUM SMART CONTRACT

Smart contracts are account-holding objects on the Ethereum Blockchain. They contain code functions and can interact with other contracts, make decisions, store data, and send ether to others.
As part of my internship/training I had given tasks to build smart contracts using solidity on Ethereum Blockchain network.

This is the list of the smart contracts that I have made:

- Greeting Application
- Blog Application
- Voting Application
- Grade Distribution Application
- Auction Application
- Crowd Funding

I had done all of this above application in solidity. I had made frontend + smart contracts + api for only voting application. So we will only discuss voting application here.

A. Decentralized Voting Application

I have made decentralized voting application. User or voter can vote for their favorite candidate from this application. Main functionality of this DApp is that no one can hack this application and no one can give vote more than one time. Since a Blockchain is a permanent record of transactions (votes) that are distributed, every vote can irrefutably be traced back to exactly when and where it happened without revealing the voter's identity. In addition, past votes cannot be changed, while the present can't be hacked, because every transaction is verified by every single node in the network. And any outside or inside attacker must have control of 51 percent of the nodes to alter the record.

DOI 10.17148/IJARCCE.2018.785

Even if the attacker was able to achieve that while incorrectly entering user votes with their real IDs under the radar, end to end voting systems could allow voters to verify whether their vote was correctly entered in the system, making the system extremely safe.

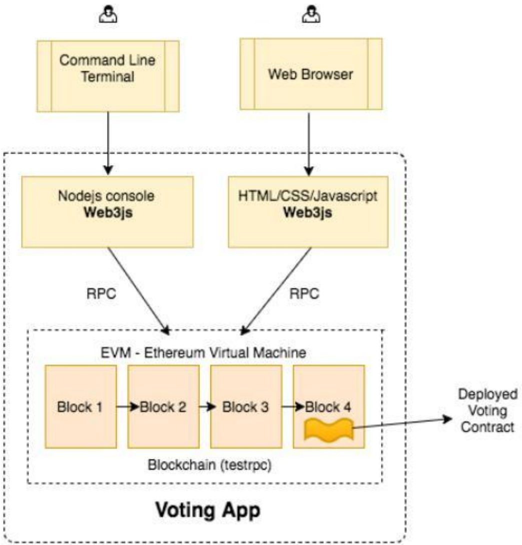
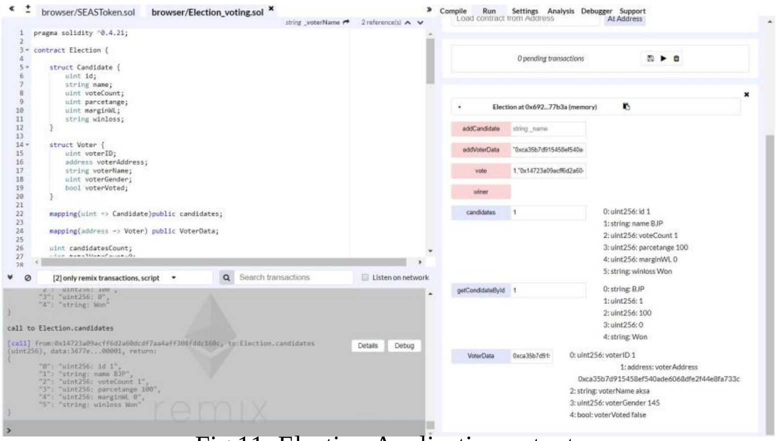


Fig 10: Flow of voting application



```
pragma solidity ^0.4.21;

contract Election {

    struct Candidate {
        uint id;
        string name;
        uint voteCount;
        uint parcetange;
        uint marginWL;
        string winloss;
    }

    struct Voter {
        uint voterID;
        address voterAddress;
        string voterName;
        uint voterGender;
        bool voterVoted;
    }

    mapping(uint => Candidate)public candidates;

    mapping(address => Voter) public VoterData;

    uint candidatesCount;
```

```
        "3": "uint256: 0",
        "4": "string: Won"
}

call to Election.candidates

[call] from:0x14723a09acff6d2a60dcdf7aa4aff308fddc160c, to:Election.candidates
(uint256), data:3477e...00001, return:
{
        "0": "uint256: id 1",
        "1": "string: name BJP",
        "2": "uint256: voteCount 1",
        "3": "uint256: parcetange 100",
        "4": "uint256: marginWL 0",
        "5": "string: winloss Won"
}
```

Election at 0x692...77b3a (memory)

addCandidate: string _name

addVoterData: "0xca35b7d915458ef540a

vote: 1,"0x14723a09acff6d2a60

winer

candidates: 1

```
0: uint256: id 1
1: string: name BJP
2: uint256: voteCount 1
3: uint256: parcetange 100
4: uint256: marginWL 0
5: string: winloss Won
```

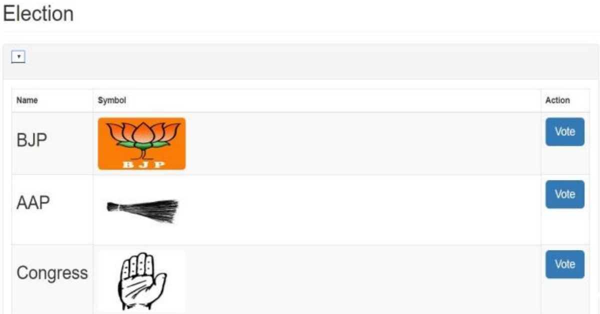
getCondidateById: 1

```
0: string: BJP
1: uint256: 1
2: uint256: 100
3: uint256: 0
4: string: Won
```

VoterData: 0xca35b7d91

```
0: uint256: voterID 1
            1: address: voterAddress
   0xca35b7d915458ef540ade6068dfe2f44e8fa733c
2: string: voterName aksa
3: uint256: voterGender 145
4: bool: voterVoted false
```

Fig 11: Election Application output



Election

Name	Symbol	Action
BJP	B J P	Vote
AAP		Vote
Congress		Vote

Fig 12: Permanent contract deployed on Ethereum Blockchain

We will code solidity coding in remix Ethereum Virtual Machine (EVM). For our voters Ethereum account we will use Metamask. Web3.ja is a Javascript API that allows you to interact with the Blockchain, including making transactions and calls to smart contracts. Truffle is a popular testing development framework for Ethereum. It includes a development blockchain, compilation and migration scripts to deploy your contract to the Blockchain, contract testing, and so on. Truffle contract is an abstraction on top of the Web3 Javascript API, allowing you to easily connect and interact with your Smart Contract.

DOI 10.17148/IJARCCE.2018.785

X. FUTURE WORK

I am going to explore Ethereum blockchain more and made Dapps on Ethereum blockchain in future. We will also make our own private blockchain using go, python language.

REFERENCES

[1]. Ethereum White paper and Crowd funding Code (www.ethereum.org)
[2]. http://remix.ethereum.org, www.etherscan.io
[3]. www.solidity.readthedocs.io
[4]. Applications of Blockchain Technology beyond Cryptocurrency, Mahdi H. Miraz, Maaruf Ali.
[5]. The Blockchain Technology: Some Theory and Applications, Nicola Dimitri.
[6]. Antonopoulos A., Mastering Bitcoin (2nd Ed), O'Reilly, (2017)
[7]. blockchain hub basic key words of blockchain technology
[8]. https://github.com/fivedogit/solidity-baby-steps/tree/master/contracts

DOI 10.17148/IJARCCE.2018.785