

Virtuoso Infotech Pvt. Ltd.



About Virtuoso Infotech

- Fastest growing IT firm; Offers the flexibility of a small firm and robustness of over 30 years experience collectively within the leadership team.
- Technology expertise & passionate team.
- Successful client engagements across India, USA, UK, Australia and Argentina.
- Handle enterprise solutions that involve **30,000 active users**, more than 20 servers, **data volume as big as 5 million entries per day.**

Ethereum



- **Bhargav Mehta**

Agenda

- Why Ethereum? Issues with the conventional implementations.
- Introduction to Ethereum
- Components of Ethereum
- Ether in Detail
- Transaction
- Contracts
- Merkle Trees
- Distributed apps (**DApps**)

Quick Recap

- What is a blockchain?
- What are cryptocurrency?
- Name a use case you can think of for blockchain.

The issues with conventional implementations

- Very specific use cases.
- Built for and around fixed protocols.
- Lacks flexibility.
- Focused more as a product and not as a platform.
- So effectively, for your each use case you will be creating your individual blockchains.
- Reinvent the wheel.

What we need as developers or creators ?

Introduction to Ethereum

What is **Ethereum**?

Introduction to Ethereum

It is a **Blockchain**.



Introduction to Ethereum

- It is more of a platform rather than a currency.
- It runs on a currency system termed as Ether, which is a Crypto-Fuel for the Ethereum network but also used as Crypto currency.
- The most prominent feature of Ethereum that makes it a unique platform is the feature of Smart Contracts and Distributed Apps.
- **Ethereum is a decentralized smart contracts platform that is powered by a cryptocurrency called Ether.**

Introduction to Ethereum

- Two accounts
 - User Accounts [Controlled by private keys]
 - Contracts [Controlled by code]
- It has a built in general purpose programming language support.
 - Solidity, Serpent, LLL and Mutan.
 - Viper for secure smart contracts. [Experimental]

State and History

- State has all the “current” information
 - Account balance
 - Nonces
 - Contract code [empty string for private-key accounts]
 - Contract storage [Storage trie root]
- History
 - Transactions
 - Receipts

Transaction

- **nonce** [Avoid replay attacks]
- **gasprice** [Amount of ether per unit of gas]
- **startgas** [Maximum gas consumable]
- **to** [Destination address]
- **value** [Amount of ether to send]
- **data** [Readable by contract code]
- **v, r, s** [Signature values]

Code Execution

- Every transaction specifies a “To” address.
- Code can:
 - Send ETH to other contracts
 - Read/Write Storage
 - Call other smart contracts [**Internal Transaction**]
- Every node on the blockchain processes every transaction and stores the entire state.
- Halting problem.

Gas [Fuel]

- To solve halting problem, a fee is charged per computational step.
- This fee is call “**Gas**”.
- Gas is not a currency, it is unit of effort for execution.
- There is also a special gas fee applied to operations that take up storage.
- Every transaction has to specify it’s **Gas Limit**. If the code exceeds the gas limit, transaction is reverted and returns with error. Sender still has to pay a fee.
- Gas Limit is like block size limit. Miner vote on the limit.
- Currently Global Gas Limit is at 6.7 million.

Ether in Detail

- Ether is a fuel for operating in the distributed application platform of Ethereum. Basically, ether is currency you can use to pay for Gas.
- Ether was just the incentive ensuring that developers write quality applications.
- Rise in popularity of Ethereum has sparked huge interest in trading of Ether as crypto currency.
- 5 ethers are awarded to the miner of the block (roughly 15 seconds).
- 2-3 ethers are sometimes sent to another miner if they were also able to find a solution but his block wasn't included (called uncle/aunt reward).
- Currently valued at #2 amongst all the cryptocurrencies. June 2018, market cap - \$47.47 Bn; June 21, 2018, closing - \$525.77.

Contracts in Detail

- A contract is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.
- Contract accounts pass messages between themselves as well as does the computation.
- Contracts live on the blockchain in a Ethereum-specific binary format called Ethereum Virtual Machine (EVM) bytecode

```
contract HelloWorld {  
    event Print(string out);  
    function() { Print("Hello, World!"); }  
}
```

- This contract will create a log entry on the blockchain of type Print with a parameter “Hello, World!” each time it is executed.
- Operating within the Ethereum environment, there is no obvious way of “outputting” a string. The closest we can do is to use a *log event* to place a string into the blockchain.

Ethereum Virtual Machine [EVM]

- Contains
 - Stack
 - Memory
 - Storage
 - Environment Variables
 - Logs
 - Sub-Calling
- High level languages used for programming are compiled to EVM byte code.

Merkle Trees

- Data structure for block in Ethereum.
- Allow for efficiently verifiable proof that a transaction is included in the block.
- State Tree maintained for all the states in Ethereum.
- Roots to block header.
- Very helpful for light clients.

Distributed apps (DApps)

- Dapp is a service that enables direct interaction between end users and providers.
- UI via an HTML/Javascript web application.
- They have their own suite of associated contracts on the blockchain which they use to encode business logic and allow persistent storage of their consensus-critical state script API to communicate with the blockchain.
- Covers a wide range of areas including finance, insurance, prediction markets, social networks, distributed computation and storage, gambling, marketplace, internet of things, governance, collaboration, development and games.

Mist

- This is the equivalent of a web browser, but for the Ethereum platform.
- It acts as a GUI to display the accounts and contracts that you interact with.
- It also allows you to create and interact with contracts in a graphical user interface without ever touching the command line.
- If you are not a developer and just want to store ether and interact with Ethereum contracts, then Mist is the program to use.

Conclusion

Thank You!

Virtuoso InfoTech Pvt. Ltd.
4th Floor, Victory Landmark, Opp. D-
Mart,
Behind Dominos Pizza, Baner, Pune.

+91 8087081318
support@virtuosoitech.com



www.virtuosoitech.com

