Ethereum Topic

Github Article (Whitepaper):

After a brief introduction to Bitcoin, and how it has sparked interested to a range of technologies behind it, the article sums ups some of the digital cryptocurrency history until 2009, and focused on the concept of "proof of work". In practice, it provided a "simple and moderately effective consensus algorithm" and allowing free entry into the consensus problem. The ledger contains the "state" of all bitcoins in transaction, or specifically the minted and unspent transaction outputs. Essentially the first half of a transaction in Bitcoin prevents spending coins that do not exists, the second half prevent spending other people`s coin. The major second step enforces the conservation of value. When activated in a transaction these steps are recorded into the decentralized ledger. The consensus is then that miners work on the longest chain with validated transactions and so that no attackers can apply a double-spending attack.

Each block contains a hash, being a 200-byte piece of information containing the timestamp, nonce, previous block hash, and the root hash of the data structure called Merkle tree. As transactions continue the chain grows at large, and so we see the rise of "simplified payment verification"nodes come along, allowing for lighter devices to compute only block headers, and "branches " that are relevant to them.

The article mentions that there are two ways of building a consensus protocol, either on top bitcoin or an independent network. Ethereum choose the latter.

Bitcoin also facilities the signature of not only a single private key, but also by design an option of "Two out of three", to sign an UTXO. It can also serve as a bounty script, only releasing the UTXO if a certain transaction or action has found place. Ethereum wanted to expand on this.

Bitcoin has a few limitations, and some of these are:

Lack of Turing-completeness: missing the ability of loops in the sript.

Value-blindness: UTXO lack the fine-grained control over the amount that can be withdrawn.

Lack of state: not possible with multi-stage contracts or scripts.

Blockchain-blindness: UTXO are blind to data such as the nonce, the timestamp and previous block hash, which are valuable sources of randomness data.

Building new blockchains require development time and bootstrapping efforts, using scripting is easy to implement and standardize, but is limited in its capabilities, and meta-protocols are easy to build, but suffer from faults in scalability.

Ethereum aims to be an alternative framework, ease development, light client properties, and allow for a shared economic environment and blockchains security.

Ethereum aims to be an alternative protocol for building decentralized applications, whether they are small and rarely used, and emphasis rapid development time. It`s blockchain contains a Turing-complete programming language, allowing for smart contracts with its own arbitrary rules for ownership, transaction formats and state transition functions.

Accounts are in the middle of this(Ethereum), containing four fields; the nonce, the ether balance, a contract code and the account storage. There are two types of accounts, externally owned and contract accounts. Their programming is described as "autonomous agents" that react when given a message or a transaction. The transaction itself is usually a signed data package that stores a message to be sent from an externally owned account. Two variables dictate the computational power, and limit accidental or hostile loops, called STARTGAS and GASPRICE.

In addition, messages can be sent through contracts. When transactions are sent, they either create a new account, deposit ether to another or contact a contract that executes code. This code is a custom-made high-level language referred to as EVM code. It consists of three types of spaces; the stack, the memory byte array

and a long-term storage – a key/value store. The EVM can encode any computation that can be conceivably carried out, including infinite loops. A contract cannot continue forever due to a set of computational steps allowed due to the amount of GAS given, and that it stops so that the computation is reverted but fees are paid.

There are a few categories of application mentioned that exist on top of Ethereum. The first being financial, the second being semi-financial applications, and the third being applications for online voting and decentralized governance that are not financial. Decentralized storages facilitation is a major innovation that also comes out to play. It also allows for what is essential voting and decentralized autonomous organizations. Other purposes mentioned in the whitepaper are savings wallets with multiple security features, crop insurance, decentralized data feed, smart multisignature options, cloud computing and verification, gambling, predictions markers and decentralized marketplaces.

GHOST Protocol: Takes into account ancestors but also stale descendants. Fees are regulated by two coded factors to avoid larger fee schemes.

In addition, Ethereum consists of a primary liquidity layer to allow for efficient exchange and paying of transaction fees. They are denominated, from smallest chronological order; wei, szabo, finney and finally, ether. At the beginning, Etherum was sold against BTC, and then the BTC was used to pay salaries and further development of the protocol. First came an endowment pool, before a steady release of funds provides for a growing linear supply.

The mining of these sees miners having to fetch random data from the state, compute some randomly selected transactions from the last N blocks in the blockchain and return the hash of the result. A verification protocol lives on the side, or is at least proposed, to verify transactions and cope with problems of scalability and 51% attack issues.

Wiki-article:

Ethereum itself was proposed by Vitalik Buterin, a young programmer and was funded by an online crowd sale. 11,9 millions coins were premined (13% of total supply). Due to a project collapse in 2016, there now exists Ethereum (ETH) and Ethereum Classic(ETC). The name was chosen due to its resemblance to ether, an invisible medium that allows light to travel. The token and development is now in the hands of a larger organization called Enterprise Ethereum Alliance (EEA).

The wiki article illustrates Ethereum as a open-source, public, blockhain-based computing platform, that implements a version of the Nakamoto consensus. It uses Ether as generated by the Ethereum platform. Gas is used as an internal pricing mechanism, and explained as used to mitigate spam and allocate resources on the network.

The protocol has undergone many planned changes, and will eventually plan to go from hardware (proof of work) mining to virtual mining (proof of stake). As a result of the previous split when the DAO project collapsed, the network chooses to split the blockchain to reallocate the lost funds that happened in the exploit. The chain has split two more times afterwards.

The currency is stored in a wallet that store the public and private keys also called addresses. Block time is significantly lower than bitcoins, where block time is 14 to 15 seconds.

Gas is usually measured in Gwei. A total of about 98 million ether is currently in supply.

The EVM is the virtual machine that allows for runtime environment and applies the contract and script-abilities the chain has. Programming abstractions and script can be written in Solidity (similar to C and Javascript), Serpent, LLL, and Mutan. Another language in development is Viper. This ability for languages allows for Ethereum biggest innovation, smart contracts. This also allows for many applications to be created on top, commonly referred to as DApps. Many enterprise projects are being tested.

The Ethereum blockchain uses Merkle trees for security, but also the ability to optimize transaction hashing. All smart contracts are publicly available on every node the blockchains, which aquires substantial costs, since they need to be calculated in real time every time a new block is added, or when running transactions.

The last part of the article argues that ponzi schemes are viable concepts on the chain, although infrequent among all the smart contracts created.

Understanding Ethereum – 5 takeaways from the original article (not accessible due to paywall)

1.Even though the platform was built for application and contracts between these, the market is still driven by exchanges, that only have 15% of the total transactions, but drive 50% of the volume.

DApps on the side, have about 6,39% of transactions, and roughly 12% of the total volume. It remains to see if these transactions are used to speculate or actually used for buying and preparing funds to use in smart contract applications.

2. Ether price could surge when accepted by Asian/Chinese Markets, that have been slow to adopt the Ether currency.

3. The DAO collapse remain a blemish on the reputation, where the hard fork is speculated to be initiated by the Ethereum foundation members, who also happened to be the largest stakeholders.

4. Application development in consolidating in four areas.

5. Ethereum platform is still very much a beta project, and remains to prove that is remains stable over time. It remains to see if the proof-of-stake concept will hold. Payment channels, plans to introduce sharding, and the language of Solidity.

Chapter 10.7

The chapter focuses on how the Turing-completeness of Ethereum is viable, in the form that the blockchains can apply to any application that a computer can come up with. With its Smart Contract Programming Model the programmable contract between you and a candy bar machine becomes possible. Anyone can upload a Ethereum contract to the chain, for a small fee. Written in bytecode and executed by the virtual machine. Once done, the contract will live on the blockchain. The contract then has its own fund, and can execute API calls and send/receive money. Wei is the smallest currency unit that is accepts. In addition to accepting different costs for an action, each contract should have a mean to withdraw or pass on funds, so they do not become stale.

The chapter argues that Ethereum uses the gas to throttle the problem of infinite loops, so that it cannot continue into infinity. The complete list of transactions (and their costs) is fixed, and will require a hard fork to fix or change. As of today, a unit of gas is defined as 50 Gigawei.

Every call specifies how much gas it will use, and if it runs out, the execution returns an error and halts. This also limited the system to “cheap” computations, not allowing for hardcore systems to be ran on Ethereum.

It also mentions the difference that Ethereum is, an account-based blockchain-model. It uses the Patricia tree, a prefix/radix tree. It contains the state of each address, including contract addresses. Each contract then has its own tree. It also uses an additional transaction counter.

The Ethereum is also ran by a non-profit foundation and has planned releases, compared to Bitcoin`s solemn existence. Updates are essentially hard forks, and updates often destroy contracts (not that this was expanded further on in the book..)

References:

https://github.com/ethereum/wiki/wiki/White-Paper

https://en.wikipedia.org/wiki/Ethereum

https://www.coindesk.com/5-takeaways-coindesks-understanding-ethereum-report/

Chapter 10.7