Maddie Tobolewski

DATA 470 Capstone Project - Background

An Analysis of the Ethereum Blockchain Network

Background

The intention of this project is to analyze the elements of popular cryptocurrency blockchains to better understand their network structures and operations. The primary focus of this study is the Ethereum blockchain network, while acknowledging the Bitcoin network consistently as a comparable blockchain application in which to compare the network structures. Ethereum and Bitcoin both use the Nakamoto consensus to regulate their blockchains' transaction serialization and are similar architecturally. Primary differences in the two cryptocurrencies include their APIs, abstractions, and wire protocol (Gencer, et al. 2018).

Blockchain technologies have been quickly extending their presence among a variety of industries, not the least of which includes the financial sector and cryptocurrency markets. This rapid expansion and implementation of blockchain has proven its potential to be altered and adopted by any company or organization seeking to more securely transfer, verify, and log data. In the writing, Blockchain Technology: Beyond Bitcoin, Crosby et al. describes blockchain as,

Essentially, a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. (Crosby, et al. 2016)

The creation of the cryptocurrency, Bitcoin, in 2009 and the creation of blockchain are synonymous, and in recent years the success of Bitcoin has inspired other companies and individuals to jump onto the blockchain bandwagon. Most of these other projects aim to build onto the foundation of the Bitcoin network itself to leverage the high value placed in the system and the vast amount of computation that goes into the consensus mechanism (Wood n.d.).

The Ethereum, a cryptocurrency introduced in 2015, is a decentralized virtual machine, which can execute programs – called contracts – written in a Turing-complete bytecode language, called Ethereum Virtual Machine (EVM) (Wood n.d.) (Bartoletti, Carta, et al. 2019). Every contract has a permanent storage where to keep data, and a set of functions which can be invoked either by users or by other contracts. Users and contracts can own a cryptocurrency (called ether, or ETH), and send/receive ether to/from users or other contracts (Bartoletti, Carta, et al. 2019). The Ethereum blockchain is similar in a variety of ways to the Bitcoin blockchain, although there are significant differences. The main difference between Ethereum and Bitcoin, in regard to the blockchain architecture, is that Ethereum blocks contain a copy of both the transaction list and the most recent state, while Bitcoin only blocks only contain a copy of the transaction list. Aside from that, two other values, the block number and the difficulty, are also stored in the block (Chinchilla 2019).

The first exploration into the concept of smart contracts was done in the late 1990s, and it showed clear potential to support the algorithmic enforcement of agreements. However, until very recently, in 2015, no specific system was proposed to create or implement such a system. Smart contracts are distributed programs that control the flow of the digital currency, Ether, and allow for expressing a broad spectrum of financial applications. No new concept goes unaffected by negative implications, as the significant semantic complexity increases the risk of programming errors (Grishchenko, Maffei and Schneidewind 2018).

In the research piece, Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact, by Bartoletti, Carta et al. explain the process in which transactions are initiated and executed, as well as how contracts are tied into the process. The process is broken down as follows:

Users can send transactions to the Ethereum network in order to: (i) create new contracts; (ii) invoke a function of a contract; (iii) transfer ether to contracts or to other users. All the transactions sent by users, called external transactions, are recorded on a public, append-only data structure — the blockchain. Upon receiving an external transaction, a contract can fire some internal transactions, which are not explicitly recorded on the blockchain, but still have effects on the balance of users and of other contracts. (Bartoletti, Carta, et al. 2019)

An understanding of the contract execution code and the heightened possibility for security risks is paramount to analyzing the Ethereum blockchain data. However, the analyzation of smart contracts is difficult for a few reasons. The first being that Ethereum smart contracts are developed in Solidity, a language which features transaction-oriented mechanisms and a number of non-standard semantic behaviors. Additionally, smart contracts are uploaded onto a blockchain in the form of EVM bytecode, a stack-based low-level code featuring dynamic code creation and execution, and, generally, minimal static information (Bartoletti, Carta, et al. 2019).

These concerns in mind, Ethereum is still particularly notable due to the varied potential of the smart contracts' functionality. The ability to be implemented many ways ranging from public cryptocurrency markets to permissioned consortium business-logic practices makes it even more vital to have insight into the process of smart contract execution and transaction information.

References

Bartoletti, Massimo, Salvatore Carta, Tiziana Cimoli, and Roberto Saia. 2019. "Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact." Future Generation Computer Systems (Dipartimento di Matematica e Informatica, Università degli Studi di Cagliari, Italy) 102 (2020): 259-277.

Bartoletti, Massimo, Stefano Lande, and Livio Pompianu . 2017. "A general framework for blockchain analytics." SERIAL'17: ScalablE and Resilient InfrAstructures for distributed Ledgers, December.

Chinchilla, Chris. 2019. "A Next-Generation Smart Contract and Decentralized Application Platform." GitHub. June. Accessed October 2019. https://github.com/ethereum/wiki/wiki/White-Paper (https://github.com/ethereum/wiki/wiki/White-Paper).

Crosby, Michael, Nachiappan, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. 2016. "BlockChain Technology: Beyond Bitcoin." AIR: Applied Innovation Review, June.

Gencer, Adam Efe, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gun Sirer. 2018. "Decentralization in Bitcoin and Ethereum Networks." Financial Cryptography and Data Security (FC) 2018 (Cryptovest).

Grishchenko, I., M. Maffei, and C. Schneidewind. 2018. "Foundations and Tools for the Static Analysis of Ethereum Smart Contracts." Computer Aided Verification, July 18: 51-78.

Tikhomirov, S., E. Voskresenskaya, I. Ivanitsky, R. Takhaviev, E. Marchenko, and Y. Alexandrov. 2018. "SmartCheck: Static Analysis of Ethereum Smart Contracts." IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), August 27: 9-16.

Wood, Gavin. n.d. "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER." Ethereum & Ethercore.