Developing Applications that Use the Blockchain

1 Introduction

In recent years, the emerging concepts of Blockchain and Smart Contract have been gaining sharply increasing attention. More and more researchers and engineers are contributing to this area to form fundamental theories and invent new algorithms. In addition, applications in real-world are also emerging with cryptocurrency as the most typical one. In this report, we are going to describe the basic principles, software tools, pros and cons, and impacts of Blockchain, focusing on the application and effect in software engineering.

2 Blockchain Overview

3 Blockchain Application Case Study

4 Libraries and Tools

This section focusing on more technical and practical aspects of Blockchain, that is, how to develop software using Blockchain. To be more specific, we are going to decribe, categorize and summarize libraries and tools for development of Blockchain-based software and integration into an applications.

The nature of decentralisation and verification of Blockchain makes it suitable for orgnisations and activities that require trust among participants. Furthermore, Smart Contract on Ethereum empowered Blockchain by the capability of executing codes in decentralised mannar on Ethereum Virtual Machine, which naturally results in the concept and practice of Decentralised Application(dApp).

Blockchain is an area far from maturity so it is fast evolving, and consequently different libraries and development tools are emerging. There are a few articles collect and describe such tools.(Blockgeeks, n.d.)(Dinita, 2019) These tools mainly focus on one of these aspects:

- Smart Contract development: language, compiler, libraries, IDEs
- dApp development: usually includes some Smart Contract development tools, but also integrates other tools such as decentralised storage or front-end frame work.
- Blockchain as a Service: usually provides Blockchain service in the form of APIs
- Decentralised data storage: store data on Blockchain network for security and lower cost
- Alternative Blockchain networks, platforms and development environments
- Testnet for testing Smart Contract and dApp before put into production

4.1 Smart Contract Development

- Geth: Go implementation of Ethereum protocol. With Geth, developer can run a full Ethereum node on there computer. With Geth, one can mine Ether, make transactions, and run and deploy their Smart Contract on Ethereum blockchain.
- Solidity and solc: Solidity is a programming language for development of smart contract on Ethereum. It syntax is JavaScript-like. `solc` is a Solidity compiler.
- EtherScripter: Visual smart-contract builder for Ethereum. Developer can drag and connect different components like building blocks to create a Smart Contract. Offical examples are available here.(EtherScripter - visual smart-contract builder for ethereum, n.d.)
- ethers.js: A JavaScript library completely implementing the Ethereum wallet. It enables interaction with the Ethereum Blockchain and its ecosystem. It is also fully TypeScript ready.

4.2 Decentralised App(dApp) IDE

dApp develoment tools usually integrate some Smart Contract develoment tools, but also includes other mondatory tools so that the developer can create, test, and deploy dApps in a single environment.

- Remix: A suite of tools for Blockchain development. It includes a debugger to debug transactions on Ethereum network, a unit test frame work for Solidity, and an IDE for Smart Contract and dApp development.(Remix - ethereum ide, n.d.)
- Metamask: It allows developers to run Ethereum dApps right in your browser without running a full Ethereum node.(MetaMask, n.d.)
- Embark: a JavaScript library for building and deploying dApps. Embark is not only a Smart Contract development environment, but also a complete development toolkit for dApps. It also integrates several parts for computation (EVM), storage (IPFS, Swarm), and communication (Whisper).(Frequently asked questions - embark, n.d.)
- Truffle Suite: a collection of dApp development tools, which includes:(Truffle suite, n.d.)
  - Truffle: a development environment and testing framework for dApps. It is based on EVM
  - Truffle Teams: a DevOps tool for dApp development. It provides features such as creating continuous integration(CI) pipeline, running and deploying contract, monitoring transactions and events.
  - Ganache: Is a tool to simulate an Ethereum network with which developers can deploy, run, and test Smart contracts and dApps. It has both a GUI for desktop application and a command-line interface, with the latter formerly known as the TestRPC.
  - Drizzle: a collection of a variety of front-end libraries aiming to make dApp front-ends development faster and more managable.

4.3 APIs or Blockchain as a Service (BaaS)

BaaS is a service, usually cloud-based, that enable developers build, deploy and host their Smart Contracts or dApps on blockchain network, while all operational and maintaining tasks are managed by cloud computing service provider and transparent to users.(Frankenfield, n.d.) Some typical BaaS solutions are:

- Azure Blockchain Service: Microsoft has created Azure to offer these services.(Azure blockchain service, 2018) It supports several Blockchain networks such as MultiChain, Eris, Storj, and Augur. It's also a develoment environment aimimg to develop dApps in a secure environment with less cost.
- Coinbase's API: Coinbase is a cryptocurrency exchange at San Francisco, which opens its APIs to allow developers to build new bitcoin apps and incorporate bitcoin functionality in their applications.
- Crypto APIs: an infrastructure layer making it easier and more managable to develop applications on any Blockchain and Crypto protocol. It provides services for more than 10 Blockchain protocols with a unified API layer.(Crypto API, n.d.)

4.4 Blockchain Data Storage

Blockchain can bring decentralised storage system into reality with robustness and safety to serve today's large-scale applications like Netflix or Facebook.(Saini, 2018)(Eterna Capital, n.d.) In this section, we will list and briefly describe some solution for decentralised storage or database.

- Tierion: Tierion is a collection of development tools and APIs to create, add data to and query from a verifiable database on the bitcoin network.
- BigchainDB: a blockchain database. It has characteristics of both database and blockchain, including decentralization, immutability, and native support for assets. Each BigchainDB node runs BigchainDB Server and various other software. It provides BigchainDB HTTP API and API wrapper libraries such as the BigchainDB Python Driver.(Terminology - bigchaindb docs, n.d.)
- FileCoin: a decentralized cloud storage platform on which users can provide their unused storage to fulfill storage request, and then earn FileCoin cryptocoins for hosting files.
- Storj(Tardigrade): a decentralised platform and suite for secure data storage. It is S3-compatible. Tardigrade is a production-ready version of Storj for enterprise use.(Introduction -storj, n.d.)

4.5 Alternative Blockchain Platforms

- Corda: an open-source blockchain platform. It enables to develop, deploy and run dApps known as Cordapps (Corda Distributed Applications).(R3 Limited, n.d.)
- Hyperledger: an open source collaborative effort created to advance cross-industry blockchain technologies hosted by The Linux Foundation.(Foundation, n.d.) It is a large collection of a range of tools and frameworks for blockchain and dApp development, including:
  - Hyperledger Burrow: provides a modular blockchain client with a permissioned smart contract interpreter partially developed to the specification of the Ethereum Virtual Machine (EVM).(The Linux Foundation, n.d.)

  - Hyperledger Sawtooth: a platform enabling development, deployment, and execution of distributed ledgers. It invents a novel consensus algorithm, Proof of Elapsed Time (PoET), targeting to significantly reduce the resource consumption for distributed validation.
  - Hyperledger Caliper: a blockchain benchmark of measurement of blockchain performance with a set of predefined use cases.

4.6 Blockchain Testnet

Before a project is released to the production Ethereum network, it is beneficial to make a test deployment to an Ethereum Test Network(testnet). Testnet is a copy of the Ethereum almost identical in every aspect to the mainnet except that their Ether values nothing. It enables a developer to test, debug and verify their codes before real assets are involved.(Hayes, 2018)

- Public Test: Public testnets are copies of Ethereum network which is publicly availabe. In contrast to the mainnet, writing to the testnet is free. Common public testnets includes Ropsten, Rinkeby, and Kovan.(Blockgeeks, n.d.)
- Private Test: Developers can deploy a personal Blockchain network on their own computers for the purpose of test, for example, with Geth. Another method is to emulate a Ethereum network, such as Ganache which is part of Truffle Suite.

5 Challenges and Shortcomings

The basic principles of blockchain appear to be simple, but when it comes to reality the implementation is facing a variety of challenges.(Reyna, Martín, Chen, Soler, & Díaz, 2018)

5.1 Scalability and Performance

The basic principle underpinning blockchain is the mechanism of consensus among the network for verification of transactions. Nodes communicate with each other and make decision following predifined rules. Transactions and blocks to be appended to the network requires confirmation from a certain number of nodes in the network. This approach brings about transpancy and trust in blockchain netwok, however, it also increases the time for processing and confirmation of a transaction, thus reduces the throughput (number of transactions per second) and increases the latency.

5.2 Storage Capacity

Storage capacity have been a significant challenge in blockchain for long. In main stream blockchain technology, the chain is always growing and each node in the network stores a complete copy of the whole chain with all transactions in them. For example, in Bitcoin there are approximately 1MB per block every 10 min. Although only full nodes (a node that can fully validate transactions and blocks) need to store the whole chain, enormous storage volume are required. (Reyna et al., 2018)

5.3 Security

Various vulnerabilities and security issues of Bitcoin protocol are found thanks to thorough analysis by engineers and researchers. The most well-known attack is the 51% attack or majority attack, which can happen if someone controlled at least 51% of nodes in the network because in this situation he/she took complete control of the consensus. In addition, some other attacks, such as double-spend attack, race attacks, and Denial of Service(DoS) are also discovered and investigated. Finally and interestingly, quantum computing could be seen as a dealy threat to blockchain such as Bitcoin because it unprecedented computing power can easily break the current cryptograhy algorithms underpinning blockchains.(Reyna et al., 2018)

5.4 Vulnerability of Smart Contract

Smart contract hugely expands the area of blockchain applications, but nothing comes without cost. The ability of executing abitrary code brings capability and flexibility but also more vulnerability to attack such as bugs, hacking, or viruses. Bugs in customer contract codes are particularly critical because of the system's irreversable and immutable nature. Therefore, it is essential to develop formal methods, mechanisms and tools to validate, verify and guarantee the correctnees of smart contracts before they are deployed to production network.(Reyna et al., 2018)

5.5 Consensus

Consensus mechanisms are fundamental for the transpancy, verification and trust without central authorisation in blockchain network. The most popular consensus is Proof of Work(PoW) which has been working successfully in Bitcoin. However, PoW has shortcomings such as low transaction rate and high latency as mentioned before, and furthermore, is highly computationally intensive and results in huge amount of energy consumption. Not suprisingly many alternatives and improved consensus mechanisms are proposed, such as Proof of Stake (PoS), Leased Proof of Stake (LPoS), Proof of Burn (PoB), Proof of Importance (PoI), activity test (PoA), Elapsed Time Test (PoET), and Proof of Capacity (PoC). However,consensus mechanisms have not been appropriately formally proved thus remain an open area.(Reyna et al., 2018)

6 A Research Paper

7 Impacts and Future Directions

Blockchain system was created with characteristics of decentralisation, immutability and transparency. It enables an infrastructure layer and a new paradigm for software development. Empowered by blockchain, developers can create secure and autonomous-running applications. Blockchain is seen as the next generation of internet.

7.1 Smart Contract and dApp

One of the most significant consequence of blockchain is dApps enabled by Smart Contract. Empowered by the verifiable and decentralised nature of blockchain, dApps is an innovative and promising software development paradigm. A increasing number of dApps are being created, including games, user-generated context (UGC) network, supply chain management. Blockchain and dApps are still in its early stage but some researchers believe we are at the start of a new era of decentralised computing which will eventually lead the internet service into next generation.(Cai et al., 2018)

7.2 Transparent, Decentralised File Storage & Database

The fundamental concepts of blockchain can also enables decentralised, transpancy and secure data storage on peer-to-peer networks. It will have lower data loss rate and lower costs. The decentralised data storage will benefit large-scale web applications.

7.3 Decentralised Software Engineering Tools

Blockchain technology not only brings about new software infrastructure and programming paradigm, but also could revolutionise software engineering itself. The key concepts in blockchain can bring about more trustable and efficient collaboration into software development and benefit many stages in software development lifecycle. For example, a decentralised continuous integration(CI) system and package manager were investigated.(Beller & Hejderup, 2019) Decentralised version control system such as Git can also be expected.

8 References

Azure blockchain service. (2018, May). Retrieved August 2, 2019, from https://azure.microsoft.com/en-us/services/blockchain-service

Beller, M., & Hejderup, J. (2019). *Blockchain-based software engineering*. *Proceedings of the 41st international conference on software engineering: New ideas and emerging results*, 53–56. https://doi.org/10.1109/ICSE-NIER.2019.00022

Blockgeeks. (n.d.). *15 of the best tools for blockchain development*. Retrieved August 2, 2019, from https://blockgeeks.com/guides/15-best-tools-blockchain-development

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). *Decentralized applications: The blockchain-empowered software system*. *IEEE Access*, *6*, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644

Crypto API. (n.d.). Retrieved August 2, 2019, from https://cryptoapis.io

Dinita, M. (2019, January). *4 of the best decentralized cloud storage solutions to use in 2019*. Retrieved August 2, 2019, from https://windowsreport.com/decentralized-cloud-storage

Eterna Capital. (n.d.). *Blockchain based decentralised cloud computing*. Retrieved August 2, 2019, from https://medium.com/@eternacapital/blockchain-based-decentralised-cloud-computing-277f307611e1

EtherScripter - visual smart-contract builder for ethereum. (n.d.). Retrieved August 2, 2019, from https://etherscripter.com

Foundation, T. L. (n.d.). *Hyperledger*. Retrieved August 2, 2019, from https://wiki.hyperledger.org

Frankenfield, J. (n.d.). *Blockchain-as-a-service (baas)*. Retrieved August 2, 2019, from https://www.investopedia.com/terms/b/blockchainasaservice-baas.asp

Frequently asked questions - embark. (n.d.). Retrieved August 2, 2019, from https://embark.status.im/docs/faq.html#Embark-in-one-sentence

Hayes, G. (2018, February). *The beginners guide to using an ethereum test network*. Retrieved August 2, 2019, from https://medium.com/compound-finance/the-beginners-guide-to-using-an-ethereum-test-network-95bbbc85fc1d

Introduction -storj. (n.d.). Retrieved August 2, 2019, from https://documentation.storj.io

MetaMask. (n.d.). Retrieved August 2, 2019, from https://metamask.io

R3 Limited. (n.d.). *What is a cordapp?* Retrieved August 2, 2019, from https://docs.corda.net/cordapp-overview.html

Remix - ethereum ide. (n.d.). Retrieved August 2, 2019, from https://remix.ethereum.org

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). *On blockchain and its integration with iot. Challenges and opportunities*. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/https://doi.org/10.1016/j.future.2018.05.046

Saini, V. (2018, August). *StoragePedia: An encyclopedia of 5 blockchain storage platforms*. Retrieved August 2, 2019, from https://hackernoon.com/storagepedia-an-encyclopedia-of-5-blockchain-storage-platform-8aa13c630ace

Terminology - bigchaindb docs. (n.d.). Retrieved August 2, 2019, from http://docs.bigchaindb.com/en/latest/terminology.html

The Linux Foundation. (n.d.). *Hyperledger burrow*. Retrieved August 2, 2019, from https://www.hyperledger.org/projects/hyperledger-burrow

Truffle suite: Sweet tools for smart contracts. (n.d.). Retrieved August 2, 2019, from https://www.trufflesuite.com