Deployment of Smart Wallet Contracts on Ethereum

Ms. Poonam Dhankhar

Dept. Of CSE
Assistant Professor, Maharaja Surajmal Institute of Technology, Delhi

Abstract: On the blockchain, cryptocurrencies play a role similar to cash, while cryptographic tokens are a universal tool for handling rights and assets. Software wallets interact with blockchains in general and with smart contracts (on-chain programs) in particular. Some wallets are realized (partly) as smart contracts with the intent to increase trust and security by being transparent and by offering features like daily limits, approvals, multiple signatures, and recovery mechanisms.
Ethereum is the most prominent platform for both, tokens and smart contracts, and thus also for wallet contracts. We discuss several methods for identifying wallet contracts in a semi-automatic manner by looking at the deployed bytecodes and their interaction patterns. Furthermore, we differentiate characteristics of wallets in use, and group them into six types.

Keywords: smart contracts, ethereun, blockchain, cryptocurrencies.

1. Introduction

Wallets keep valuables, credentials, and items for access rights (like cash, licenses, credit cards, key cards) in one place, for ease of access and use. On the blockchain, cryptocurrencies play a role similar to cash, while cryptographic tokens are a universal tool for handling rights and assets. Software wallets manage the cryptographic keys required for authorization and implement the protocols for interacting with blockchains in general and smart contracts (on-chain programs) in particular. On-chain wallets are smart contracts that hold cryptocurrencies and access to tokens and that may offer advanced methods for manipulating the assets. Simply by introducing the role of an 'owner' it becomes possible to transfer all assets of an on-chain wallet transparently and securely in a single transaction. More refined methods include multisignature wallets, which grant access only if sufficiently many owners sign. Regarding the number of transactions and public availability of data, Ethereum is the major platform for smart contracts, and thus also for tokens and on-chain wallets. This paper investigates the usage and purpose of on-chain wallets on the main chain of Ethereum qualitatively as well as quantitatively.
Methodologically, we start from the source code of wallets and determine characteristic functions. Then we search the deployed bytecode for variants of the wallets with the same profile. Some wallets can also be detected by their creation history or by the way they interact with other contracts. We group the wallets according to their functionality and collect creation and usage statistics from the blockchain data. Finally, we relate wallets to other frequently occurring contract types. Regarding their number, on-chain wallets form a substantial part of the smart contracts on the chain. This work thus contributes to a better understanding of what smart contracts on Ethereum are actually used for. Moreover, the collection of wallet features and blueprints may serve as a resource when designing further decentralized trading apps. Our methods for detecting wallets and analyzing their activities may help in assessing the liveliness of on-chain projects. E.g., a temporal view on the use of wallets is more informative than just the number of wallets initially deployed.

2. Literature Review

Sr no	Paper title	General idea	Advantages & limitations
1	Blockchain and Cryptocurrencies: Model, Techniques, and Applications [2018]	A survey of current cryptocurrencies to understand blockchain & its different types.	**Advantages:** Provides different incentive models, ecosystem & applications of the blockchain. Explains blockchain in a layered architecture. **Limitations:** Does not provide any solid architecture for its stated application.

2	A Brief Survey of Cryptocurrency Systems[2017]	It evaluates the strengths, weaknesses, and possible threats to all major mining strategy. It outlines how Cryptocurrencies mine, where they have comparable performance and assurance, and where they have unique threats and strengths.	**Advantages:** 1. Currently, major Cryptocurrencies use Proof of Work, Proof of Stake or a combination of the both for mining. 2. A combination of the both is found to be effective. 3. Typically memory-intensive hash functions have been found to be faster mining algorithms. **Limitations:** A majority of hash algorithms are CPU-intensive and the others are memory intensive. 2. While Proof of Work is resource intensive, Proof of Stake cannot act independently. 3. Cryptocurrencies are still experimenting with their mining protocols and algorithms to optimize their performance. No full proof algorithm has been found yet.
3	Blockchain: Future of Financial and Cyber Security[2016]	This paper explains the concept, characteristics, need for Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking.	**Advantages:** 1.The decrease in device cost 2.Increases computing power **Limitations:** 1. If an attack was done by an attacker then there will be a loss of all bitcoins, we can't recover it because the government is not involved in
4	Bitcoin: A Peer-to-Peer Electronic Cash System[2008]	A distributed peer to peer system working under the blockchain framework	**Advantages:** Cryptocurrency without any central authority. Successful POW mechanism. **Limitations:** The cost of POW consensus protocol will keep increasing as more people join the network.
5	Trust Your Wallet : a New Online Wallet Architecture for Bitcoin [2017]	It introduces a wallet which is highly secured by Multiple signatures.	**Advantages:** The scalability of disaster recovery center **Limitations:** If we lost one of the keys then we are not able to recover that key.
6	A survey on the security of blockchain systems [2017]	Detail survey of the security issues in current systems and existing solutions	**Advantages:** A careful comparison between bitcoin and ethereum. Different aspects of system vulnerability **Limitations:** Cryptocurrency will need more methods to achieve security and privacy.

Table 1.1: Literature review

The above table 1.1 describes the literature survey. The table describes about the details about the paper with the general idea of the paper with its advantages & limitations. It helps to understand the workings of the current system & the limitations of the system which are required to overcome for betterment of the system. The next section defines the solution for the limitations.

3. Scope of the work

Ethereum is also the cryptocurrency of the future because of its scope. The world is progressively moving to the digital platforms. Most industries and future companies will be based online. This means that a suitable infrastructure is needed to match the demand of future organizations.

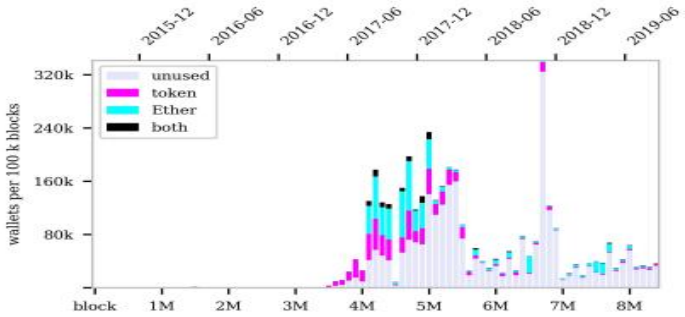

Fig. 1. Creation and usage of all wallets.

Figure 1 depicts the number of wallets created per 100 k blocks (about two weeks) as a stack plot over time. Of the Fig. 1. Creation and usage of all wallets. 3.9 M wallet contracts, 68 % have not been used so far (2.6 M, grey). The other wallets are either used for tokens (529 k, magenta) or for Ether (626 k, cyan), but only a few wallets are used for both (91 k, black). This means that wallet contracts are used either for tokens or for Ether, but rarely for both. Even though most wallets are designed for token management, only 16 % have so far received at least one token. Of the wallets holding tokens, 83 % hold just one type of tokens, 16.5 % hold 2–10 types, and only 0.5 % hold more than 10 different types.

Our contribution to understanding on-chain wallets may serve as a basis for further research in this direction, as wallets are a major application type.

To determine reliably what smart contracts actually implement, it is still indispensable to analyze byte code. Adequate tool support for a massive automated semantic code analysis would be helpful to obtain a comprehensive picture of the smart contract ecosystem.

4. Results and Discussions

1. Provided Transaction Facilities

1.1 Deposit Ether

1.2 Transfer Ether

1.3 Withdraw Ether

2. Created a Web Application for Ether Wallet

2.1 Deployed Coin using ERC20 -

ERC-20 is the technical standard for fungible tokens created using the Ethereum blockchain. A fungible token is one that is interchangeable with another token—where the well-known non-fungible tokens (NFTs) are not interchangeable. ERC-20 allows different smart-contract enabled tokens a way to be exchanged.

2.2 Wallet UI –

Ethereum wallets are applications that let you interact with your Ethereum account. Think of it like an internet banking app – without the bank.

2.3 Metamask Connection –

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

2.4 Smart Contract Integration –

Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met.

2.5 Functionalities- Get Token Balance

2.6 Transfer Token Functionality

2.7 Frontend Development –

Front-end web development is the development of the graphical user interface of a website, through the use of HTML, CSS, and JavaScript, so that users can view and interact with that website.

5. Conclusions

Thus, as we have already seen there is a need of a decentralized regulated transaction token or currency without a central point of failure. We have created a cryptocurrency from scratch which can be controlled using an e-wallet. We have also created a generalized blockchain API which can further be used to develop applications in the blockchain domain. This purpose can be other than a cryptocurrency as well. A new hashing function was implemented to create fixed length output needed. The cryptocurrency is fast, secure and readily available. It implements a hybrid consensus protocol, meaning it combines two proofs to verify and validate transactions in the blockchain system. Any transaction needs to be verified by miners like all the other prevalent cryptocurrencies. The difficulty of the function to be solved to verify transactions is set to be dynamic and is set such so that it does not cause either inflation or recession of the currency. The system is built as a peer-to-peer system, thus all the users depend on

each other for the proper functionality of the system. An efficient data cleanup and detection mechanism has been implemented to improve the execution efficiency of blockchain systems. An ewallet which is secure, fast and highly accessible has been implemented which can be used by the user to interact and control the cyrptocurrency. This e-wallet creates a public as well as private key bind to the user which can be used in various transactions over the currency.

Identification of wallets- The identification of wallets as recipients of tokens or Ether can be done automatically, but includes many contracts beyond proper wallets. Our method of identifying wallets by name, interface, and ancestry yields blueprints for wallets, which then are used to locate contracts with similar implementations or same deployers. This approach is only semi-automatic, but more reliable.

Blueprints for wallets- Since we manually verify the Solidity source code, our work yields a ground truth of wallets that can be used for evaluating automated tools.

Usage of Wallets. On-chain wallets are numerous, amounting to 7.3 M contracts (20 % of all contracts). However, most wallet contracts (68.4 %) are not in use yet. They may have been produced on stock for later use. Interestingly, the wallets are used either for tokens or for Ether, but rarely for both. Even though most wallets are designed for token management, only 1.1 M wallets (14.6 %) have so far received at least one token. Of the few wallets holding tokens, 79,5 % hold just one type of tokens, while 99.2 % hold at most 10 different types.

Landscape. Our assumption that wallets act as a cohesive in the graph of executed calls between contracts holds only for a very broad definition of wallets. To dissect the landscape of smart contracts effectively into applications, we may have to identify further contract groups that handle assets.

6. References

1. Y. Yuan, S. Member, and F. Wang, ―Blockchain and Cryptocurrencies: Model, Techniques, and Applications,‖ IEEE Trans. Syst. Man, Cybern. Syst., vol. PP, pp. 1–8, 2018.
2. U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, ―A Brief Survey of Cryptocurrency Systems.
3. S. Singh, ― Blockchain: Future of Financial and Cyber Security,‖ pp. 463–467, 2016.
4. S. Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System,‖ Www.Bitcoin.Org, p. 9,2008.
5. F. Zhu et al., ―Trust Your Wallet: a New Online Wallet Architecture for Bitcoin,‖ 2017.
6. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ―A survey on the security of blockchain systems,‖ Futur. Gener. Comput. Syst., 2017.
7. https://en.wikipedia.org/wiki/Cryptocurrency
8. https://trufflesuite.com/ganache/
9. https://en.wikipedia.org/wiki/Ethereum