Storage Assault on Crypto Wallet in Android

Mrs.Sahana D S
Assistant Professor
Department of Computer Science and Engineering
GITAM School of Technology, Bengaluru, Karnataka, India

Dr. Dayanand Lal N
Assistant Professor
Department of Computer Science and Engineering
GITAM School of Technology, Bengaluru, Karnataka, India

Dr. Brahmanand S H
Professor
Department of Computer Science and Engineering
GITAM School of Technology, Bengaluru, Karnataka, India

Mrs. Veena R C
Assistant Professor
Department of Computer Science and Engineering
GITAM School of Technology, Bengaluru, Karnataka, India

Abstract- Online payments have exploded dramatically in recent years, and a wide range of mobile apps offer money transfers. Such systems typically support scan-and-pay – a method that makes a customer to check the payment's destination address from the Client's mobile screen with ease. This technique is universal because it needs no special hardware, only the sensor, which is present on all modern smartphones. In this paper , illustration about how an Android can be used by attacker to utilize the sensitive information using Ethereum address and how attacker changed the address to spoil the privacy of transactions that make use of the scanning and pay technique have been shown with an example.

Keywords – Crypto Currency, Ethereum, Bitcoin, QR Code

I. INTRODUCTION

Mobile payments are quickly increasing, as they are extremely ubiquitous and countries are heading towards cashless currencies. A broad currency banning by the Indian government forced the citizens of India to turn to mobile wallets to pay for their daily commodities and services [1]. Paytm is one of India's most common wallet apps, with over 100 M downloads. The Paytm framework uses the scanning and paying technique in the same way as the Crypto currency wallet software . Crypto currencies are a new thought in the world's economy. The lifespan of this might be only about five years; even then they have already gained much publicity. They have experienced dramatic changes in their currency exchange especially since the year 2013. The crypto currencies are a part of the virtual currency group. Crypto currency can also be stated as a digital exchange medium, focused on its principles that allow safe, decentralized, and distributed business transactions to be performed [2].

There exists many categories of Crypto currency like Bitcoin, Ethereum, Litecoin , Ripple are the most used. Most of the people use Bitcoin and Ethereum. Where in Bitcoin [3**]** are a global payment system and a crypto-currency. This is the first digital decentralized currency, since the system functions without a banking system or a single director. The service is peer-to-peer and user-to-user transactions take place directly, without a middleman. Via Cryptography, these transactions are reviewed by network checkpoints and documented in a publicly distributed Blockchain. Bitcoin was developed under the name Satoshi Nakamoto by an anonymous person or group of people, and released in 2009 as Open Source Software. It can be traded for other assets, utilities, and goods. And Ethereum [4**]** is crypto currency is developed on the Ethereum blockchain, Ethereum is also called Ether. It is a shared forum of computing based on open source, block chain. It has an insightful facility for scripting. It operates with

transaction-based method of payment on updated version of Nakamoto's crypto currency. Vitalik Buterin[5], who was a computer programmer and crypto-currency academic, first launched Ethereum in 2013.

.

Figure 1: Simple Example illustrating Crypto Attack on Android

In this case the proposed work carried out the work on an Android phone. The specification for the crypto wallet application is undefined. We managed to change the address and research of the contact further if we could also modify the Ethereum, Bitcoin and other addresses of the crypto holders. By this the observation done and found that updating the address of owners is more problematic than fixing the address of contacts as typically the owner doesn't worry about their own address so it is important to re-check the address of the recipients. When compared to other operating systems IOS system is more difficult to jailbreak, which is a process of deleting the restrictions imposed by the software, as well as the amount of effective rooting is very small, which takes huge amount of time. This approach is transparent for an Android app and it doesn't take long to make it root. Hence, if you are using some crypto wallet, borrowing a friend's phone in 2-3 hours, or even losing your phone in during the time, is very risky which is illustrated as shown in figure 1 above. If we see the reason why it is dangerous, it is because of Ethereum [6], which is a big blockchain-based smart contract framework-transforming full programs performed in a decentralized network and typically manipulating digital value units. A network of peer-to-peer nodes that collectively oppose and maintain a common view of the global state, and runs code on demand. The defined one is maintained in a database, secured by an evidence-of-work agreement mechanism similar to Bitcoin's.

The Ethereum addresses consist of the prefix "0x," a standard hexadecimal identifier, combined with the ECDSA public key's rightmost 20 bytes of the Keccak-256 hash (big endian). 2 digits reflect a byte in hexadecimal, indicating that the addresses contain 40 hexadecimal digits. Examples include 0xb794F5eA0ba39494cE839613fffBA74279579268 [7].Taking an Ethereum address as an example above, 0xb794F5eA0ba39494cE839613 fffBA74279579268. Possibly we have to learn to remember it; likely regular users would pay only little attention to remember their own addresses. The address the application generates will be the address that they trust. Upon changing the address, the user displays their QR code created from the modified address (address of the attacker). If other people have checked the QR code nothing will stop it. [8]. In this paper we focus on the experiments on crypto wallet attack showing how dangerous if you lose your mobile phone that has a crypto wallet enabled, and also explaining the approaches to mitigate the attack by following the best practices in security and our field experience.

The rest of the paper is organized as follows. Related work explained in section II. Methodology is presented in section III. Concluding remarks are given in section IV.

II. RELATED WORK

According to Hayes[9], his work tries to classify the probable source of interest demonstrated on the marketplace by crypto currencies through cross-sectional scientific data. It has been calculated that a regression model leads to three key factors of crypto currency value: the coin mining difficulty; the unit output rate; and the crypto logical algorithm used. Comparative currencies called Bitcoin have been used, eliminating much of the price volatility associated with the dollar exchange rate. The corresponding model can be used to understand better the relative-value drivers observed in crypto currencies emerging region.

T. Moore and N. Christin[10] illustrated about Bitcoin , which has achieved Greater acceptance than any previous crypto-currency; but its success has also attracted the attention of frauds who have exploited organizational weakness and cumulative transaction effects. They concentrated on researching risks facing investors from Bitcoin exchanges that exchange between Bitcoins and local currency. Often it's to blame the frauds but not always. They considered the transaction volume of an exchange using a proportional hazards model which shows that it is likely to close or not.

Shuangyu He[11] et.al describes successful key management of crypto currency has always been a crucial criteria for traditional crypto currency. Though a vast body of crypto wallet-management schemes has been introduced, they are often designed for specific application contexts and sometimes suffer from poor protection. In this paper, they introduced a more reliable, functional, and protected crypto currency wallet-management framework based on semi-trusted social networks, thus enabling users to collaborate with the parties involved to achieve some powerful functions and recovery under certain conditions. Flexible Central Delegation, etc. The performance review reveals those requires less additional costs and have less time constraints, allowing them efficient enough for implementation in the real world.

According to Nikolaos A. Kyriazis[12] et. al Discover the nature of other crypto-currencies and how they should be influenced by the three largest digital capitalization currencies, namely Bitcoin, Ethereum, and Ripple. They used standard data representing the uncertainty market for the crypto currencies. The effect of these three cryptocurrencies 'decline on both the returns of the other virtual currencies is discussed with the family models of ARCH and GARCH and the DCC-GARCH. The study's key finding is that the largest of crypto currencies are similar to Bitcoin, Ethereum and Ripple and that there are no futures contracts capabilities among the largest digital currencies.

III. METHODOLOGY

Android uses the file system framework of Linux that has one root. Android uses the framework of the Linux file system and has a single root. It gives you with many choices for preserving your device files. The methodology you choose depends on your individual needs, such as whether you need space for your data, what kind of information you need to protect, and what information needs to be personal to your computer or available to other user and applications.

3.1 Crypto currencies used by people:

Cryptocurrency customers invest their money safely secured with private keys in online "wallets." For a trade, the transfer of money between the members of two digital wallets involves a record of the exchange to be entered in the national public national shared database. Individual computers gather data about every 10 minutes from the new Cryptocurrency or other bitcoin-currency [13**]** exchanges and transform it into a mathematical puzzle. There, proof of the payment-within-a-puzzle waits. Verification occurs only when individuals of another group of participants, called miners, separately resolve the complex mathematical puzzles that support the validity of the transaction, eventually resolving the transaction from one wallet's owner to another. A mine army usually works on the challenge at the same time in a contest to be the first with the puzzle proof authenticating the transaction.

The path several cryptocurrencies achieve its existence is via the "cryptocurrency mining" method , which is a reward, typically some amount of new cryptocoin, is given to the miner who first resolves the encrypted problem. This strategy was developed as an opportunity particularly for those who devote their computers time and computation power to sustain the network and generate new coins. While the difficulty of the puzzle calculations has increased significantly over time miners find that even high-PCs with a powerful processor could not profitably mine enough to cover the costs involved.

3.2 File Storage Structure of Android

The data storage in Android broadly categorized in to different types as illustrated in below figure 2-

(i) Internal storage of file: Stores the application file system apps and data which is a app-private files

(ii)External storage of file: Stores file information, i.e. a shared external file system, such as a micro sd card, typically used for shared user files, such as photographs.

(iii) Shared preferences: Store private primitive data in pair format that is in key-value format.

(iv)Databases: Store the data in a private database which is a structured data.

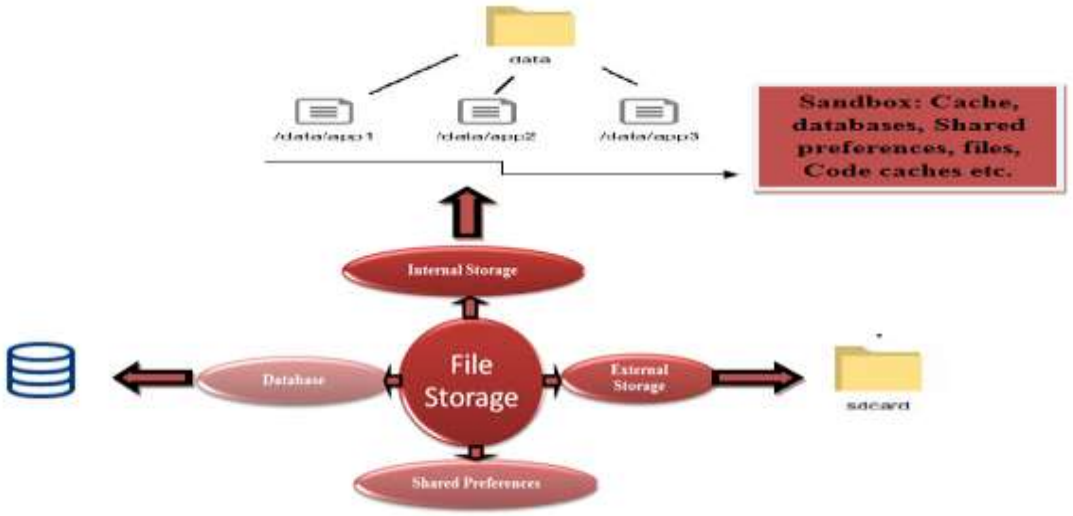

Figure 2: File storage Structure in Android

Each of these solutions is intended for app-private data except for certain types of files on external storage— the data is not necessarily available to other users. You can use the File Provider API if you want to transfer files with other devices [14]. By regular practice, data saved to your app's internal storage are private, and many other apps cannot access them unless users have root access. Such method makes internal storage a comfortable place inside the system for internal data that the user does not need to explicitly access. The application includes a private directory on the file system for each program where you can manage any files that your program needs. When the program is uninstalled individually, the files are erased from the internal storage. Because of this behavior, you cannot use the internal storage to save anything which the user expects to continue irrespective of your request.

3.3 Generating Ethereum and QR code

Download and install "unknown" application for the crypto wallet. After the installation Open the app and establish a new wallet, after successfully creating it, you will be receiving your Ethereum address as other crypto money like BTC. The Ethereum addresses are generated together with its QR code, as seen in the figure 3 below.

Figure 3: Ethereum Address with QR code of User

When you use another cell phone to check this QR you can get the Ethereum address in the plain text. When you are using the open-source QR library[15], be-alert of the vulnerability to QR code. Unanticipated errors might occur at any moment; a large amount of money may lose if the QR code produces a wrong character, keep in mind giving one wrong character in the address, and might loot your complete money. So make better use of

EIP55, which is check summed address which will really virtually guarantee that the Ethereum address is properly created. Thus in this case, the QR is created based on the app's Ethereum address. Any time the address is changed the QR code should also change. And if the attacker will change your Ethereum password, it's possible that your QR code will be made up to another one.

3.4 Example illustrating the Rooted Android Device attack

Consider attacker have stolen your android phone where you have installed you crypto wallet. They started changing your Ethereum address to their own Ethereum address. They start firing it from then. They have to go to the sandbox area to change the address, where regular users are limited. The rooting tool is the first step to enter the restricted area that they are required to do. Attacker starts to enable all necessary modes to get ADB, which is called as Android Debug Bridge. ADB is a powerful command-line tool that allows you to interact with your computer. The adb command supports a number of system behavior, such as installing, updating and debugging programs, and offers connections to a UNIX shell that you can use to execute a number of commands on a system that works.

There are four locations where the attacker must pay close attention: those 4 locations are files, cache, databases, and shared prefs. Attacker now begins checking for the document where the Ethereum address stays, the Ethereum address can be found directly by using any grep command or other Linux command lines. Sandbox information is collected in a number of ways, might be plaintext in an xml file, a sqlite3 database with encrypted data / plaintext / binary file. So finding the exact location where actually the address of the holders stored takes some time. Attacker might use grep command to get the Ethereum address to find and examine and to ensure it comes from the Ethereum address of the owner. After getting the Ethereum address by using grep command and analysing it, the data gives the attacker some information.

Example 1: With Plain Text as shown in figure 4

Users Ethereum address:
Ethereum Address &quot : “ 0xaC04fAc67fd509d2dCD380edb5A3B784ca03d9C2 &quot”;

Figure 4: Users Ethereum address in Plain Text

The attackers’ address:
“ 0x587Ecf600d304F831201c30ea0845118dD57516e”

Therefore, the attacker simply has to modify Ethereum address with his Ethereum address. It is not efficient to adjust the data within the sandbox, this could break the files system and trigger "unknown wallet stopped, submit bug report to...." To prevent this, the attacker transfers the file to sdcard which is external storage , instead uses

ADB transfer to their own local machine and modify the document without any constraints. This can be done using the commands shown in below figure 5.

```
$ cp wallet_info_sp.xml /mnt/sdcard/
```

On their local computer terminal

```
$ adb pull /mnt/sdcard/wallet_info_sp.xml /home/attacker/unknown/
```

Figure 5: Use of Copy command and ADB command to transfer data to local machine

After transferring the data to the attacker's machine , now he is able to change their file as they want (using Ethereum address). Users Ethereum address is shown in figure 5 above and Hackers Ethereum address are shown in below figure 6, upon changing the user's address, he / she simply has to move it back to the sdcard and then copy it to the shared prefs.

```
$ cp /mnt/sdcard/wallet_info_sp.xml /data/data/unknown/shared_prefs
```

Figure 6: Changed address of User to Attacker's Address

To guarantee the application runs as intended, the permissions for the wallet info sp.xml file as well as the user, groups, etc are set correctly. Otherwise the program fails and the error shows up. After efficiently editing the Ethereum address, open the software and you can observe that the attacker's Ethereum address will be updated as shown in below figure 7.

Figure 7: Ethereum Address with QR code of Attacker

Another QR code reader program is used by the attacker to test if the QR code on the wallet has been changed along with their address. And the attacker whom we have considered in this work got the correct match for it as shown in figure 8.

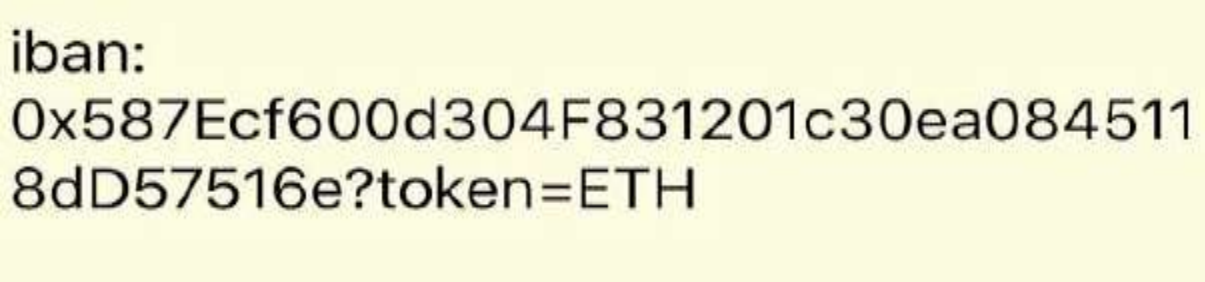

Figure 8: QR code reader program sample used by Attacker

Example 2: With Binary File

Even if we save the data in database also the attackers tries to steal the data. Below figure 9 shows the example of how data stored in binary format and figure 10 shows how it gets converted to string format using the string command.

Case 1: Binary file format

Figure 9: Binary File stored as default. Realm

Case 2:

(i) In order to read the data stored in binary file format which is a plain data, “String” Command is used.

```
U2FsdGVkX19h6NfyxszFHabvzb6hd1siTOWJu1dMXSSPnZrQX4+J7qfONe7MjQxoSE6ivfuiUcR2mWdBQJws0yl3XY0f+z9uaUU4g9ZySje1R/YUGl/
TfAkt5LVC34mp
AAAAE
AAAAE
/ /AAAAe
fgik3tJmGp2jqpaJJyGh8j7c2abRngZxEBP/lQ9W7L0KC7Bx79FiGA
U2FsdGVkX19h6NfyxszFHabvzb6hd1siTOWJu1dMXSSPnZrQX4+J7qfONe7MjQxoSE6ivfuiUcR2mWdBQJws0yl3XY0f+z9uaUU4g9ZySje1R/YUGl/
TfAkt5LVC34mp
AAAA
U2FsdGVkX19h6NfyxszFHabvzb6hd1siTOWJu1dMXSSPnZrQX4+J7qfONe7MjQxoSE6ivfuiUcR2mWdBQJws0yl3XY0f+z9uaUU4g9ZySje1R/YUGl/
TfAkt5LVC34mp
AAAAE
AAAA
*0x69759fed0a72cc6ed579352f2da517c1fdfbce4d
U2FsdGVkX1+36ApmrFSCTuOf0Gd5zxtqYcKOPAMIjde0ioZA/fG99nDRZaD9HqA1za0H3tVfDCigik3tJmGp2jqpaJJyGh8j7c2abRngZxEBP/lQ9W7
L0KC7Bx79FiGA
U2FsdGVkX19h6NfyxszFHabvzb6hd1siTOWJu1dMXSSPnZrQX4+J7qfONe7MjQxoSE6ivfuiUcR2mWdBQJws0yl3XY0f+z9uaUU4g9ZySje1R/YUGl/
TfAkt5LVC34mp
```

Figure 10 : Conversion from Binary to string using string command

(ii) The attacker is able to get the Ethereum address by combining with strings using the grep command once after getting the user address in plain text format as shown in figure 11.

```
trings default.realm| grep -i "69759"
+0x69759fed0a72cc6ed579352f2da517c1fdfbce4d
```

Figure 11 : Combining with grep command to get Ethereum Address

Use of any text editors, the attacker cannot modify the data in plaintext because the binary file does not allow todo so, or even if necessary, the file will be broken down. They make use of command "hexdump", which is a command-line tool that is used to demonstrate the raw bytes of a document in different ways such as hexadecimal, viable on Linux, FreeBDS, OS X, and other platforms. [16]

```
$ hexdump -C default.realm | less
```

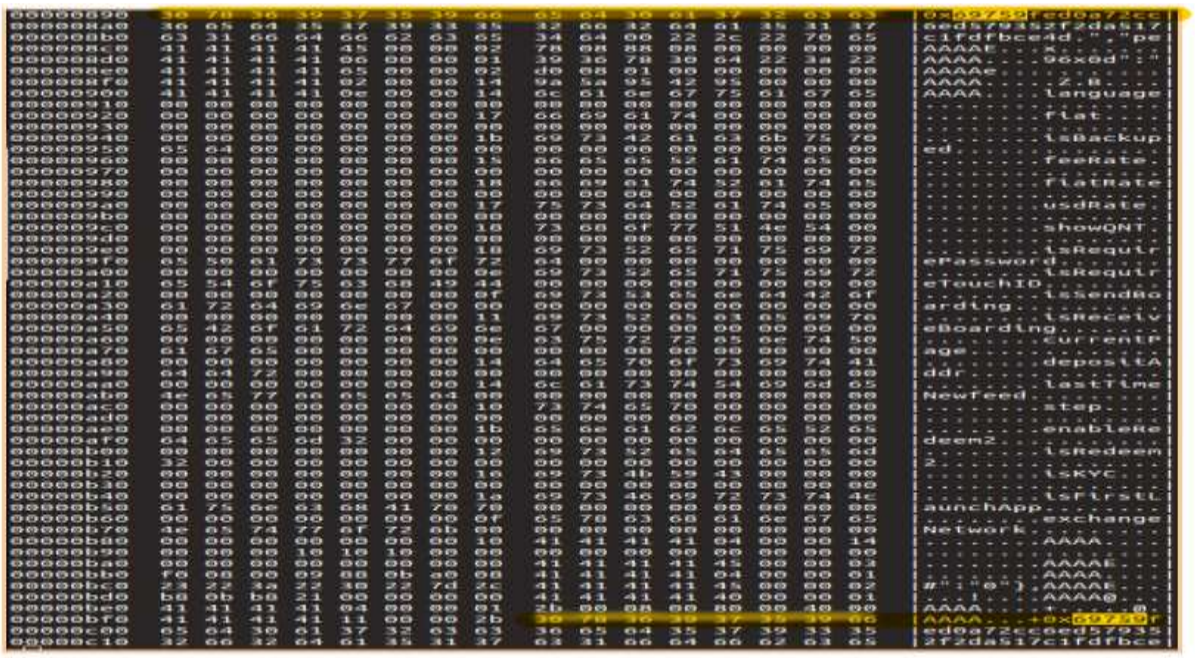

Figure 12: Usage of Hexdump command to display raw bytes of document

When u give the hexdump command, the attacker now get a chance to view the Ethereum address of a user which is shown in the format of binary. The attacker will now evaluate the Ethereum address encoded in binary, by using the hexdump command as shown in figure 12.

(i) Original Ethereum address :

0x697**59f**ed0a72cc6ed579352f2da517c1fdfbce4d

(ii) Attacker attempting to change Ethereum address as

0x69759f to 0x69789a

(iii) Binary format of 0x69759f

30 78 36 39 37 35 39 66

(iv) Attackers changed Ethereum address Binary format

30 7836 39 37 38 39 61

(v) Then finally using **sed-i** command we can replace the text as shown below

```
$ sed -i "s/\x30\x78\x36\x39\x37\x35\x39\x66/\x30\x78\x36\x39\x37\x38\x39\x61/g"
default.realm
```

(vi) Then if you run the command of **hexdump** , we can observe that Ethereum address will be changed to attackers address as shown below-

```
hexdump -C default.realm | grep -i "789a"
00000890  30 78 36 39 37 38 39 61  65 64 30 61 37 32 63 63  |0x69789aed0a72cc
00000bf0  41 41 41 41 11 00 00 2b  30 78 36 39 37 38 39 61  |AAAA...+0x69789a
```

IV.CONCLUSION

In addition, there are several ways in which situations can be utilized by the attacker to figure out where actually the address of user stored, it might be internal or external storage. A clearest example we can consider is changing the email address of friends. Losing the trust between the user and the application, as well as the long string of crypto addresses, is related to the fact that the normal users hardly see their own address, particularly when they display their QR code to their friends or outside world.

REFERENCES

[1] M. Mohamadi and T. Ranjbaran, "Effective factors on the success or failure of the online payment systems, focusing on human factors," 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, Kish Island, 2013, pp. 1-12.

[2]A. Greenberg, “Crypto currency”, 2011. [online], Forbes, 20-4-2011, Available at: http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html.

[3]S. Jain, U. Rastogi, N. Bansal and G. Kaur, "Blockchain Based Cryptocurrency for IOT," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 744-749

[4] D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, 2018, pp. 1-6.

[5] https://en.wikipedia.org/wiki/Vitalik_Buterin

[6] Sven Bugiel, Alexander Dmitrienko, Kari Kostiainen, Ahmad-Reza Sadeghi,Marcel Winandy, "TruWalletM : Secure Web Authentication on Mobile Platforms"

[7] https://en.wikipedia.org/wiki/Ethereum#Addresses

[8]_ Dr. Gavin Wood Founder, " Ethereum: A Secure Decentralised Generalised Transaction Ledger ".

[9] Dejan Vujičić, Dijana Jagodić, Siniša Ranđić "Blockchain technology, bitcoin, and Ethereum: A brief overview".
[10] HAYES, A. 2015. "What Factors Give Cryptocurrencies Their Value: An Empirical Analysis, In: Social Science Research Network", The New School for Social Research, New York, http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2579445

[11]T. Moore and N. Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk", 2013. Financial Cryptography and Data Security Lecture Notes in Computer Science, Volume 7859, pp. 25-33]

[12] SHUANGYU HE , QIANHONG WU, XIZHAO LUO , ZHI LIANG , DAWEI LI , HANWEN FENG , HAIBIN ZHENG, "A SOCIAL-NETWORK-BASED CRYPTOCURRENCY WALLET-MANAGEMENT SCHEME".

[13] Nikolaos A. Kyriazis *, Kalliopi Daskalou, Marios Arampatzis, Paraskevi Prassa, Evangelia Papaioannou,"Estimating the volatility of cryptocurrencies during bearish markets by employing GARCH models"

[14] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," 2015 IEEE Symposium on Security and Privacy, San Jose, CA, 2015, pp. 104-121

[15] https://developer.android.com/training/data-storage

[16] Enis Ulqinaku, Julinda Stefa, Alessandro Mei, "Scan-and-Pay on Android is Dangerous".