some other countermeasures that can reduce the merchant's likelihood of being deceived by an attacker, which are: requiring the merchant to be connected to a large random sample of nodes of the network and not accepting incoming connections. Therefore, the attacker cannot send transactions directly to the merchant neither identify the merchant's neighbours.

Other research studies have indeed demonstrated that this kind of attacks were possible, and not only was the attacker able to identify the merchant's neighbors but also forced them to be a set of nodes controlled by the attacker [15, 16, 68].

P2P networks, we review how each of the security problems may affect the Bitcoin network and, from those which affect it, we explain the specific countermeasures Bitcoin provides in order to defend from them.

The list of reviewed attacks goes over the most typical types of attacks and security flaws found in common P2P networks. It is clear that specific networks and applications might present specialized attacks but in most cases they can be seen as an specification of the attacks presented here.

So as to provide a clear picture of how common P2P attacks affect Bitcoin, we first review the three attacks that have been shown to be clearly applicable to Bitcoin. After that, we include a list of attacks identified for common P2P networks but that do not have such a high impact on Bitcoin, reviewing why the attacks do not apply to the specific Bitcoin network and detailing the particular cases where those attacks (or some variation) may somehow relate to Bitcoin.

In favor of a clear and concise presentation, we have not explicitly covered some recent attacks, such as [24], which do not directly affect or involve the Bitcoin network. Network related attacks such as [4] are also out of the scope of the study, since they rely on BGP hijacking.

### 3.3.1 DoS Flooding

Denial of service (DoS) attacks are possible in most P2P scenarios and are especially relevant, for example, in P2P streaming applications [23, 97, 111]. Given their dynamic nature, P2P networks are usually more resilient against generic DoS attacks than more static networks. Targeted DoS attacks to specific parts of the P2P network (a given node) or services are usually more important.

There exist several potential DoS flooding attacks in Bitcoin, but the system has countermeasures in place. *Transaction flooding* is prevented by not relaying invalid transactions and imposing fees to valid transactions. On the one hand, transactions are signed by the senders in order to prove they are authorized to transfer those bitcoins. If the signatures of a transaction are not correct, the transaction is considered invalid and it is not relayed to the network. On

CHAPTER 8

# CONCLUSIONS

This final chapter summarizes the results of the thesis and concludes with some guidelines for future work.

## 8.1 Conclusions

In the first part of the thesis we have analysed some of the foundations of Bitcoin in order to identify potential flaws, as well as to gain further knowledge about the system to design several solution. Some of those solutions are presented in the last part of the thesis.

In Chapter 3 we have given a network characterization of Bitcoin focusing especially in its security. We reviewed the most harmful attacks to P2P networks and we have seen how Bitcoin has built-in countermeasures to deal with them. Some clear examples are liveness of the system via massive data replication, protection against DoS attacks both at high level (through digital signatures in case of transactions and trough mining and PoW in case of blocks), and low

### 2.2.1 The Bitcoin scripting language

Bitcoin uses a stack based non-Turing-complete scripting language with no loops known as **Script** to encode both input and output scripts. Two different clauses can be found in Script, operation codes (**opcodes**) that define some functionality, such as addition, subtraction, signature validation, etc, and regular data, that is used as input of the aforementioned opcodes. Scripts work in pairs, when an output script is created certain locking conditions are specified in the `scriptPubKey` field. Such conditions state how the output can be redeemed. When a new transaction is created each input must provide proof of fulfilment of the conditions in the form of a script, placed in the `scriptSig` field, and pass a correctness validation. The correctness of a script is validated by evaluating both parts of the script, namely the `scriptPubKey` of the UTXO and the `scriptSig` of the input, one after the other, and analysing the final result. To do so both scripts are pushed into the stack starting from the `scriptPubKey`. If the script evaluates to true, the correctness is verified, otherwise the script is invalid making the transaction also invalid. At the time of writing, five type of standard scripts can be found within Bitcoin[1].

**Pay-to-PubKey (P2PK)** is a fairly simple type of script that allows to send coins to a given public key. The input script for P2PK scripts contains only a signature, whereas the output script contains a public key and an opcode to validate signatures.

```
ScriptPubKey: <pubKey> OP_CHECKSIG
ScriptSig:    <sig>
```

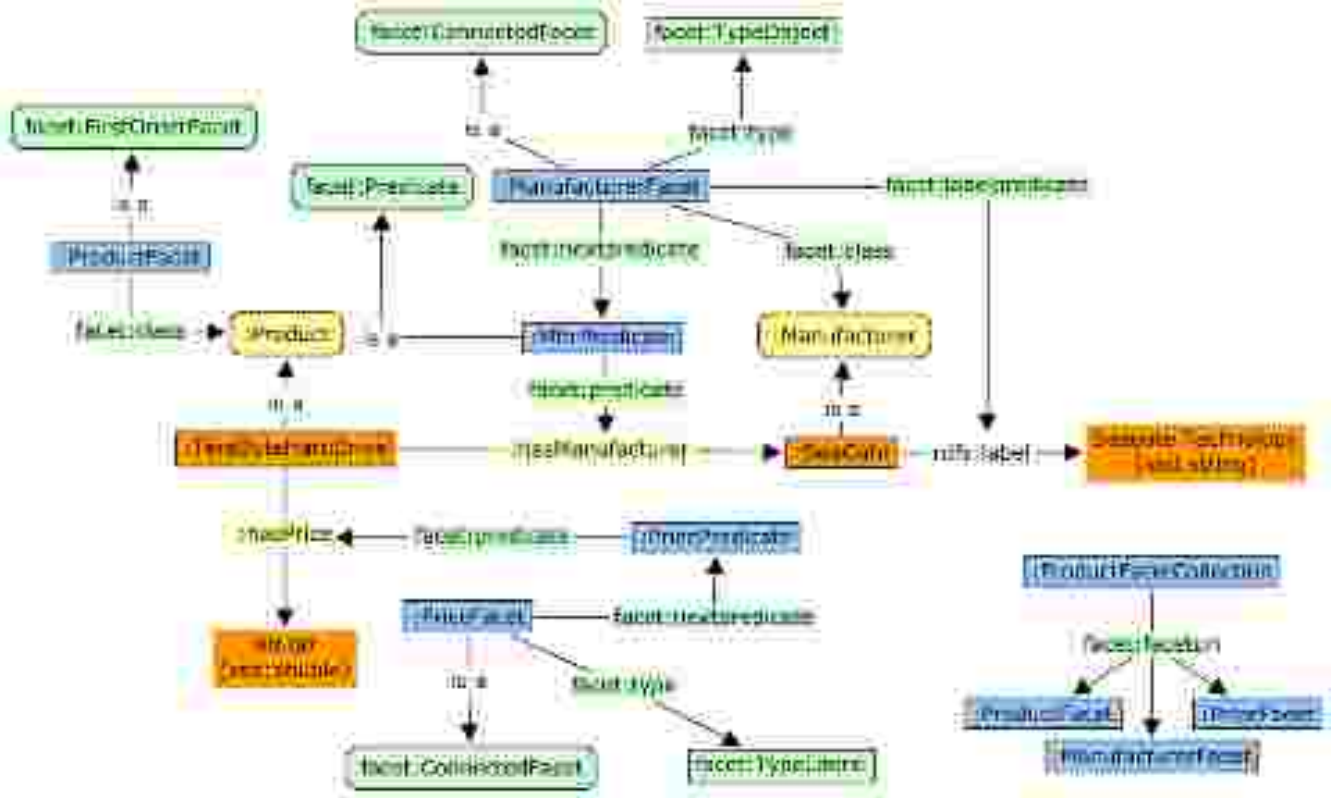
When both scripts are put together `OP_CHECKSIG` validates if the provided public key can validate the provided signature. If the validation succeeds, the script is valid, otherwise it fails. P2PK scripts where broadly used during the

[1] Excluding the recently defined SegWit scripts.

str = [chr(el) if chr(el).isprintable() else "." for el in block]
Abdel Fattah el–Sisi into power.
From August to September, the Bitcoin wallet Electrum was phished twice by hackers. According to statistics from various parties, the phishing attacks forged Electrum upgrade notifications have stolen at least 1,450 BTC worth $11.6 million.
A new repo qtum–electrum–new has been built to add qtum–related features to the latest code for Bitcoin electrum.
A new repo qtum–electrum–new was built to add qtum–related features to the latest code for Bitcoin electrum.
The Electrum development team also warned them that they had nothing to do with a project called Electrum Dark: they used our name without our permission. Be careful with the altcoin version of Electrum, as they are sometimes used as vectors to install malware against your real Bitcoin wallet.
According to Reddit user u/normal_rc, electrum's wallet was hacked and nearly 250 bitcoins (243.6 BTCs, nearly $1 million) were maliciously stolen, according to coinelegraph. Electrum then confirmed that the attack included creating a fake version of the wallet to trick users into providing password information. Electrum responded on Twitter that "this is a persistent phishing attack on Electrum users" and warned users not to download Electrum from any source other than the official website.
JoinMarket can interact with a Bitcoin Core full node to get the history of your wallet in a private way. You can also choose how to use the Electrum server, but you do not encourage regular users to use it. There are also plans to replace the Electrum interface with one that uses client bl

ock filtering.
Bitcoin desktop wallet client Electrum has released a 4.0 beta version, adding several important updates, including support for the Lightning network, nearly a year after the previous version of Electrum, 3.3.8 (last July). In the 4.0 beta version, Electrum mainly added features such as PSBT (partially signed Bitcoin transactions), Lightning Network, watchtowers ( watchtowers) and Submarineswaps (subliminal switching). (Github)
According to the Dimensionality Reduction Security Lab, users of Bitcoin wallet Electrum are currently facing phishing attacks. The hacker broadcasts a message to the Electrum client through a malicious server, prompting the user to update to v4.0.0. If the user installs this "backdoor client" as prompted, the private key will be stolen and all digital assets will be stolen
When Electrum wallets are synchronized with malicious servers, they are instructed to "update" clients provided by hackers, resulting in the loss of assets contained in older versions. Previously, in December 2018, Electrum.
In a recent announcement on Twitter, Electrum advised users to disable the automatic connection option and manually select a server, while the company is developing a more powerful Electrum.
Dash releases Dash Electrum 3.3.8.4 version
Then, on top of another computer, install the electrum. Create a new wallet and select Import Bitcoin Address or Private Key
Dynamic . . . Electrum and MyEtherWalle users face phishing attacks.
Electrum is a well–known light wallet for Bitcoin that adds new features such as server authentication using SSL to prevent MITM attacks. So unlike other Bitcoin light

**wallets, Electrum cannot communicate directly with different versions of Bitcoin full nodes, and each startup connects to electrumserver to communicate, and electrum.**
**In a forum post on Bitcointalk, website administrator Theymos explained: "If at any time in the past you've logged in to Electrum without a wallet password and opened a web page, your wallet might have been stolen." Particularly paranoid people may want to send all bitcoins (BTCs) from their old Electrum wallets to the newly generated Electrum wallet. "**
**According to the slow fog zone, the Phishing attack by Electrum forged upgrade tips has stolen at least 200 BTCs, and this attack cannot be avoided by upgrading Electrum alone, requiring the entire ecological service to make corresponding changes (because Electrum is not a full node, and then on the transaction broadcast and the corresponding server has a message communication, the attacker can also deploy a malicious server)**
**According to The Next Web, the attackers even implemented their own Electrum servers, which hosted the attacked Electrum.**
**hex = ["%.2x" % el for el in block]**
**The fact that not many people know is that Esplora is bundled with a based and optimized Electrum server. This Electrum server is derived from Electrs and is now maintained separately by the Blockstream engineering team. Over the past two years, Esplora has become one of the fastest and most scalable Electrum server solutions available for Bitcoin due to continuous updates and performance optimization. Esplora is also the only Electrum server that supports liquid networks.**
**Qtum Electrum synchronously updates electrum–related code.**



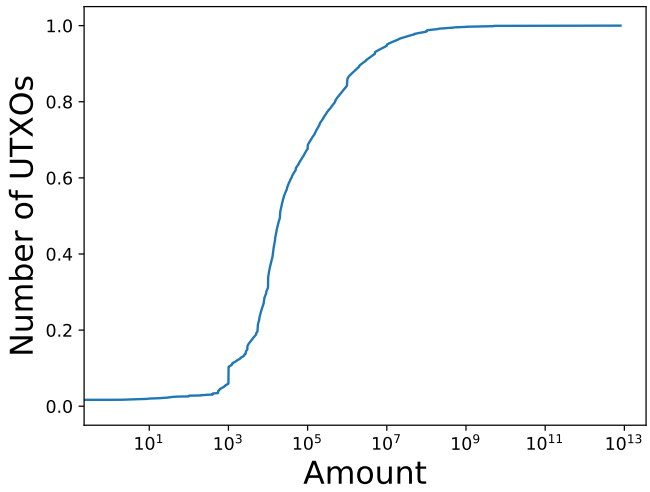



Figure 4.2: Amount of bitcoins per UTXO (in satoshis).

on two factors: the fee-per-byte rate that the network is expecting at the time of creating the transaction and the size of the transaction. The fee-per-byte rate, measured in satoshi, is a highly variable factor that depends on the transaction backlog (i.e. how many transactions are pending to be included in new blocks).

Since fees depend on the transaction size, in order to label the outputs in the UTXO set as a dust or unprofitable, we need an estimation of the size of data needed to spend such output. In order to identify the minimum information needed, we can consider an already standard transaction with its inputs and its outputs and enough fees to be relayed. Then, we define the **minimum-input of a UTXO** as the smallest size input that spends such UTXO. The size of such minimum-input, along with the value held in the output and the fee rate, will determine whether a UTXO may be included in the dust or unprofitable categories.

In order to measure the size of such minimum-input, we need to have in mind

provide this type of data, since regular nodes only keep track of transactions bounded to their addresses.

### 3.2.4 System parameters

Different P2P network overlays require a set of system parameters for the overlay system to operate. For instance, structured P2P networks require to store information on the distribution of peers in the network in order to improve routing performance. However, the Bitcoin P2P network, in line with other unstructured P2P overlays, does not require any special system parameters for the normal behaviour of the network. Every single node can join the network with no prior knowledge of it. Apart from that, some default parameters are used by nodes, such as the maximum connection limit set to 125, the minimum relay fee for transactions set to 1 sat/byte, or whether the node will relay non-standard transaction or not, among others. However such values are not a restriction and each node can set them to match their needs.

### 3.2.5 Routing performance

Differing from traditional P2P networks, Bitcoin does not follow a multi-hop routing scheme. Peers in the network store a replica of all the information that has been flowing through the system up to the date, namely the blockchain. In that way, no queries are forwarded between peers, since all information should be found at one hop. Therefore, data is guaranteed to be located if the network is synchronized, and no routing protocol is needed nor used, apart from the synchronization protocol.

### 3.2.6 Routing state

Despite being a content distribution network, the routing state of Bitcoin cannot be directly defined due to the randomness and dynamism of its topology, and to the fact that it is not known. Moreover, as we have pointed out before, no multi-hop routing is performed since data can be found at one hop at most.

# ACKNOWLEDGEMENTS

En primer lloc vull donar les gràcies als meus directors, en Jordi Herrera i en Guillermo Navarro, per confiar en mi i donar-me l'oportunitat de realitzar aquesta tesi, pel seu suport incondicional, i per tot el que m'han ensenyat durant aquests tres anys de tesi. M'agradaria estendre aquest agraïment a la meva companya Cristina Pérez, amb qui he estat treballant els darrers dos anys, i sense qui aquesta tesi tampoc hagués estat possible.

I would also like to express my most sincere gratitude to Andrew Miller for accepting me as a visiting scholar at the UIUC and for providing me guidance throughout the months I stayed there. It has been a pleasure having the opportunity to work with him. I would also like to thank the guys at UIUC: Surya, Kevin, Hanyun, Tom, Deepak, Riccardo and Zane, you really made me enjoy my stay in Illinois.

A tots els membres del grup de recerca SeNDA, i a la resta de docents del departament, que m'heu guiat des del meu pas com a estudiant fins a la finalització de la tesi.

Als meus companys de *penúries*, a en Carlos, la Sara, l'Iván, en Roger i a la resta dels anomenats *pifos*, per tots el grans moments viscuts durant aquests anys, pel suport moral, i per la quantitat de problemes resolts entre pissarres i dinars.

Al Jose i l'Andreu, per ser-hi, sempre, i per fer aquest camí infinitament més divertit. A la Clàudia i a la Núria, perquè amb vosaltres vaig poder tornar a gaudir de la muntanya que tant m'estimo, i que m'ha permès desconnectar més m'ha fet falta.

Als de casa, en especial al meus pares, per ensenyar-me a buscar la millor versió de mi, i per recolzar-me de forma incondicional. I finalment a la Laia, per acompanyar-me durant el camí, per ser al meu costat i ajudar-me, per aguantar les meves xerrades sobre temes inintel·ligibles, per tot.

**Gràcies.**