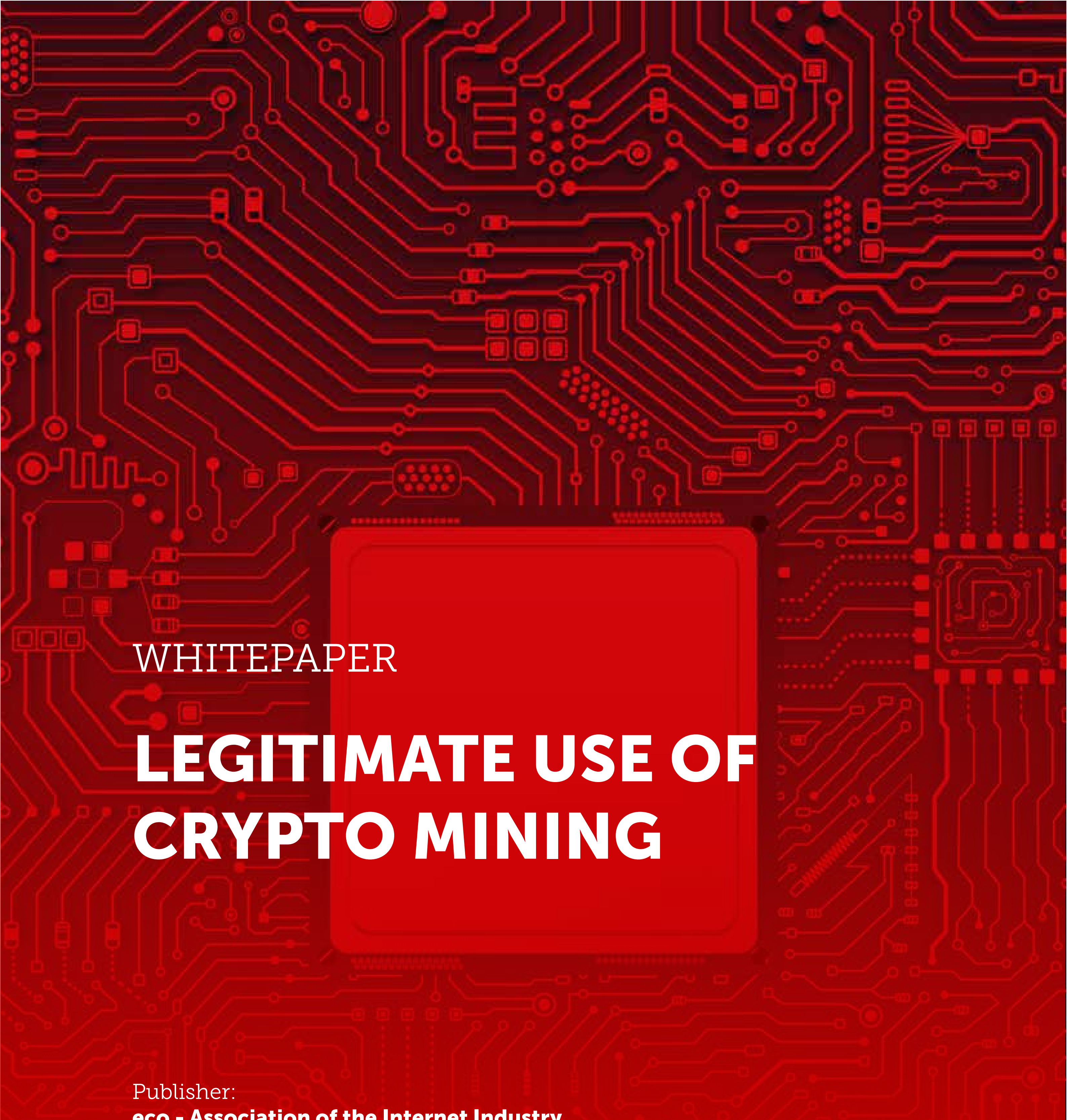

WHITEPAPER

LEGITIMATE USE OF CRYPTO MINING

Publisher:
eco - Association of the Internet Industry

Authors:
Ralf Benzmüller (G DATA), Michael Hausding (SWITCH), Patrick Koetter (sys4 AG), Peter Meyer (eyeo)

eco
ASSOCIATION OF THE
INTERNET INDUSTRY

INTRODUCTION

Crypto mining has the potential to establish itself as a new, alternative business model for the financing of online services in the Internet. Unfortunately, crypto mining has fallen into disrepute due to frequent criminal abuse of the process. The goal of this whitepaper is to make recommendations for the future legitimate use of crypto mining on websites and in (mobile) apps. These recommendations on the one hand harmonize with the interests of Internet users, and on the other hand take into account the interests of commercial providers.

Crypto mining occurs on the computers or smartphones of users. It offers website operators a way of earning money, as an alternative to or alongside online advertising. Through this new technology, app developers thus gain an additional possibility for financing the development and provision of their services.

The use is permissible, as long as it is done with the consent of the user. However, when computers are used to mine for crypto currencies without consent from the respective owner, this becomes an abuse of an external resource. This unwanted and abusive use currently outweighs the legal use to such an extent that many crypto mining services are universally blocked. Operators of app stores have therefore already adapted their policies, and banished mining apps from their stores.

CRYPTO MINING VS. CRYPTO JACKING

Crypto currencies like Bitcoin, Ethereum, Monero, and Dash are based on the concept that participants allow their devices to perform complicated calculations (the calculation of a blockchain). In exchange for this, participants receive a reward, mostly in the form of coins in the respective currency. This process is known as "mining". This can be undertaken with any computer or smartphone/tablet. Crypto mining costs money, because the calculations use the device's processors, which in turn consume additional power. For the established crypto currencies like Bitcoin or Ethereum, the calculations are unprofitable using normal PCs, as a result of the processing power required and the comparatively low remuneration. To still earn money with crypto mining, professional miners perform the required calculations in large data centers with specialized hardware, in regions with inexpensive power. In this way income can be generated that covers high power costs and returns a profit. Other crypto currencies, such as Monero, allow effective mining with standard, commercially available computers, notebooks, and even smartphones. But also in this case, power costs reduce the projected profits considerably. The power costs are eliminated if the calculations are performed by external devices, such as those of website visitors or the users of software and apps. In this case, the owners of the devices bear the power costs. If this occurs with the knowledge and consent of the users, it is legitimate. This approach has the potential to finance not only Internet offers, but also apps, primarily through the use of smartphones.

Cyber criminals have also become aware of the considerable income potential of the use of external devices for crypto mining. They make use of malware and hidden executable scripts, unbeknownst to the users, to mobilize computers for mining crypto money. They distribute their malicious software and scripts via websites and/or app stores. They abuse infected smartphones and – on a large scale – hijacked computers, computer networks, Wi-Fi hotspots, and even data centers for the purposes of mining. The revenues earned in this manner flow into the pockets of the cyber criminals. This type of crypto mining is known as "crypto jacking". Crypto jacking stands for the illegal, abusive use of mining scripts, whereas crypto mining refers to the legitimate use of mining scripts. Mining can be performed in many ways. In this document, crypto mining refers to the use cases for crypto mining on a website, and as an additional functionality of a (mobile) app.

HOW DOES CRYPTO MINING WORK?

JavaScript on a website

JavaScript is a programming language which can be executed on a user's device. Website owners can integrate a script written in JavaScript into their website. The browser loads it on the website and it is executed on the website visitor's device. Because of this functionality, crypto mining service providers like Coinhive, CoinImp, or Crypto-Loot offer mining scripts written in JavaScript. These are distributed via websites to the devices of website visitors. In the browser, the delivered script starts the calculation operations necessary for the mining of crypto money, and delivers the results back to the operator. The profits gained flow on to the registered customer of the crypto mining service providers – minus a commission for the service provider. The customer can be the legal operator of a website, who finances the Internet offer on this basis. On the other hand, it could also be a criminal who has gained illegal access to the webserver and is now using the website for nefarious purposes. Unfortunately, abusive usage is considerably more common.

Apps on the PC and smartphone

The crypto mining functions can also be integrated directly into the respective app, and are executed in the background during the use of the app. In many cases, the apps spread to other computers in the network.

CRYPTO MINING FROM THE PERSPECTIVE OF THE USER

Crypto mining or crypto jacking frequently occurs without the consent or knowledge of the user.

In the first place, this generates costs, through the additional power consumption, and it also frequently reduces the processing speed of a device. This sometimes goes so far that the device affected by crypto jacking is either limited in its usability, or it cannot be used at all.

On mobile devices, crypto mining significantly reduces the battery life. In some cases it leads to overheating or irreparable damage to the device. Crypto mining also may infringe software rights, and potentially opens backdoors for the transferal of malware.

Crypto mining is also problematic on external devices in, for example, company networks, if it is not the staff member's personal resources that are being used, but the resources of a third party – without their consent. The visit to a website or the use of an app with crypto mining may infringe company rules.

As a result of these consequences, some of which are severe, it is necessary that users are informed about the legitimate and legal use of crypto mining, and that the possible consequences are made clear.

CRYPTO MINING FROM THE PERSPECTIVE OF A WEBSITE OPERATOR OR APP PRODUCER

The use of crypto mining on a website or as part of an app also has associated risks for the operator.

The use can quickly lead to the website being blocked by browsers, protection software, and adblockers. Apps with mining functions are removed from the standard app stores. In the worst case, the entire range from one producer may be banished from the app store. Something similar can also happen to a website operator. In both cases, the operators face the threat of reduced revenues, given that their offer is no longer reachable or available.

For this reason, it is necessary for the operator to ensure a clean implementation, in order to avoid being listed on a blacklist or having their offer removed from stores. Therefore, there should be rules of play for the legitimate use of crypto mining.

RECOMMENDATIONS FOR THE LEGITIMATE USE OF CRYPTO MINING

1. The operator of a website or producer of an app must explicitly inform the user that the website or the app carries out crypto mining, and in doing so accesses the resources of the user.
2. The user must explicitly give their consent via opt-in for the use of crypto mining.
3. The user must be able to put an end to the crypto mining process at any time.
4. The information regarding crypto mining, the consent declaration, and how to end crypto mining must be clearly visible for the user ("Accessibility Guidelines") and must be unambiguous in terms of their use.
5. The provision of information regarding crypto mining, the consent declaration, and how to end crypto mining must be carried out using established interface standards.
6. The risk of a transferal of malware must be minimized as far as possible. For this, the code used should not deviate from the standard configuration of the crypto mining tool used, in order to exclude the possibility of concealed malware. For apps, the standards for software development provided by the German Federal Office for Information Security (BSI) can function as a basis.
7. The code used must exclusively be used for crypto mining. A further function – for example, as a bundle with functions like advertising or tracking – must be explicitly excluded.
8. The code used must be machine-readable at any time. The obfuscation of URLs and JavaScript code should not be attempted.
9. For the use of crypto mining, it must be ensured that the resources of the device being used are not overstrained. The regular use of the device by the user must not be impaired and the device must not suffer any physical damage as a result of the mining. Ideally, a user can limit the maximum CPU load.
10. The operator of a website must ensure that the use of crypto mining is carried out in a manner that is transparent for website visitors and must make available all relevant information pertaining to data protection.

CONCLUSION

Crypto mining may become established in the future as an alternative possibility for the financing of websites. Alongside online advertising, this would offer the operators of Internet presences a further possibility for financing high-quality content or other online offers.

With this document, the authors suggest framework conditions that should function as the basis for the fair use of crypto mining. They have also attempted to take into account the interests of all stakeholders – both from the perspective of the operator of web presences and those of website visitors. Through this, the rules of the game should be developed so that crypto mining can establish itself as a business model for website operators and app developers.

The authors recommend that international bodies or organizations define technical standards for crypto mining on the basis of the suggestions in this document.

ABOUT THE AUTHORS

Ralf Benzmüller

Under the leadership of Ralf Benzmueller, G DATA SecurityLabs was established in Bochum in 2004. There, he was responsible for the development of efficient analytical procedures and the integration of proactive protection technologies against malware threats. Ralf Benzmueller is the author of many specialist articles on online threats. He acts, among other roles, as a member of the BSI Expert Circle for Cyber Security and of the eco Competence Group Security, and teaches at several tertiary institutions.

Michael Hausding

Michael Hausding is the Competence Lead DNS & Domain Abuse at SWITCH, the registry for .ch and .li domain names. He is also an incident handler at SWITCH-CERT and a trainer for Incident Response at FIRST, the worldwide Forum of Incident Response and Security Teams. He is also a member of the board for the ISOC Switzerland chapter and is active in the Swiss Internet Security Alliance. Michael Hausding studied computer science at the Technical University Darmstadt, and gained a MAS in management, technology, and economics from the ETH Zurich.

Patrick Koetter

Expert for email security Patrick Koetter is the CEO of sys4 AG and Leader of the eco Competence Groups Anti-Abuse and Email. He advises public authorities and companies on the planning, set-up, and operation of secure email platforms. He is active in the Internet standards body the IETF, collaborating on the creation of new security technologies for email and other services.

Peter Meyer

Peter Meyer is Project Manager for IT Security at eyeo GmbH. He speaks regularly at conferences and is the author of many publications focussing on IT Security Awareness (Phishing, Botnets, Malvertising, and Online Fraud). He is also a member of the Expert Board for the EU project Cyberwiser.eu and the Cologne-based Security Startup SoSafe. He is also active in the eco Competence Groups Anti-Abuse and Security, where he led the projects Botfrei, SIWECOS, and the EU-funded ACDC project.