Diss. ETH No. 24057

On the Security, Performance and Privacy of Proof of Work Blockchains

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

Arthur Gervais

Diplôme d'Ingénieur, INSA de Lyon
Master of Science, KTH Stockholm
Master of Science, Aalto University
born 29.03.1987
citizen of France and Germany

accepted on the recommendation of

Prof. Dr. Srdjan Čapkun, examiner
Prof. Dr. Bryan Ford, coexaminer
Prof. Dr. Sarah Meiklejohn, coexaminer
Prof. Dr. Roger Wattenhofer, coexaminer

2016

Abstract

In this thesis, we examine the security, performance, and privacy of Proof of Work-based (PoW) blockchains and digital currencies such as Bitcoin. The decentralized characteristics of blockchains have the benefit of removing trusted third parties; however, they create new challenges for security, performance, scalability, and privacy, which we investigate. The blockchain's security, for example, affects the ability of participants to exchange monetary value or participate in the network communication and the consensus process.

In our first contribution, we observe the decentralized nature of Bitcoin and show that few individuals typically control vital operations in the Bitcoin ecosystem. Moreover, we show that a third party can unilaterally affect the fungibility of individual Bitcoins. Our second contribution provides a quantitative framework to objectively compare the security and performance characteristics of Proof of Work-based blockchains under adversaries with optimal strategies. Our work allows us to increase Bitcoin's transaction throughput by a factor of ten, given only one parameter change and without deteriorating the security of the underlying blockchain. In our third contribution, we highlight previously unconsidered impacts of the PoW blockchain's scalability on its security and propose design modifications that are now implemented in the primary Bitcoin client. In our fourth contribution, we investigate the privacy of lightweight Bitcoin clients, those that are the most critical to Bitcoin's mainstream adoption. Similarly, we propose appropriate design modifications that are being implemented to protect the user's privacy. Orthogonally, in our fifth contribution, we analyze the location privacy implications of public transaction prices. Surprisingly, we show that, given only a few prices from a consumer, we can accurately position the purchase location.

Zusammenfassung

In dieser Arbeit untersuchen wir die Sicherheit, Leistungsfähigkeit und Privatsphäre von Proof of Work-basierten (PoW) Blockchains und digitalen Währungen wie Bitcoin. Die dezentralen Merkmale von Blockchains haben den Vorteil, trusted third parties zu entfernen; jedoch schaffen sie neue Herausforderungen für Sicherheit, Leistungsfähigkeit, Skalierbarkeit und Privatsphäre, die wir untersuchen. Die Sicherheit der Blockchain beeinflusst beispielsweise die Fähigkeit der Teilnehmer, Geldwerte auszutauschen oder an der Kommunikation im Netzwerk und dem Konsensus Prozess teilzunehmen.

In unserem ersten Beitrag beobachten wir die dezentrale Natur von Bitcoin und zeigen, dass wenige Individuen in der Regel lebenswichtige Operationen im Bitcoin-Ökosystem kontrollieren. Darüber hinaus zeigen wir, dass ein Dritter die Fungibilität einzelner Bitcoins einseitig beeinflussen kann. Unser zweiter Beitrag liefert eine quantitative Methode, um die Sicherheits- und Leistungsmerkmale von Proof of Work-basierten Blockchains unter Gegnern mit optimalen Strategien zu vergleichen. Unsere Arbeit ermöglicht es uns, den Transaktionsdurchsatz von Bitcoin um den Faktor zehn zu erhöhen, mithilfe nur einer Parameteränderung und ohne die Sicherheit der zugrundeliegenden Blockchain zu verschlechtern. In unserem dritten Beitrag heben wir die bisher unberücksichtigten Auswirkungen der Skalierbarkeit der PoW-Blockchain auf ihre Sicherheit hervor und schlagen Konstruktionsänderungen vor, die nun im primären Bitcoin Klienten implementiert sind. In unserem vierten Beitrag untersuchen wir die Privatsphäre von ressourcenschonenden Bitcoin Implementationen, die für die Mainstream-Adoption von Bitcoin am wichtigsten sind. Ebenso schlagen wir geeignete Designänderungen vor, die implementiert werden, um die Privatsphäre der Benutzer zu schützen. Parallel hierzu, analysieren wir in unserem fünften Beitrag, die Implikationen von öffentlichen Transaktionspreise

auf die Privatsphäre der Käufer. Überraschenderweise zeigen wir, dass wir mit nur wenigen Kaufpreisen eines Konsumenten, die Position des Einkaufsortes genau positionieren können.

Resumé

Dans cette thèse, nous examinons la sécurité, performance et vie privée de blockchains basé sur le Proof of Work (PoW) comme par exemple la monnaie digitale Bitcoin. Les caractéristiques décentralisées de blockchains ont l'avantage d'enlever des tiers de confiance ; ils créent néanmoins de nouvelles défis concernant la sécurité, performance, évolutivité, et vie privée que nous étudions. La sécurité de la blockchain par exemple influence la possibilité des participants à échanger de la valeur monétaire ou généralement à participer à la communication réseau et au processus d'atteindre un consensus.

Dans notre première contribution, nous observons la nature décentralisée de Bitcoin et montrons que quelques individus contrôlent généralement les opérations vitales dans l'écosystème Bitcoin. De plus, nous montrons qu'une partie tierce peut unilatéralement affecter la fongibilité de Bitcoins individuels. Notre deuxième contribution fournit une méthodologie quantitative pour comparer objectivement les caractéristiques de sécurité et de performance de blockchains basé sur le Proof of Work en tenant compte d'adversaires avec des stratégies optimales. Notre travail nous permet d'augmenter le débit de transaction de Bitcoin par un facteur de dix, avec qu'un seul changement de paramètre et sans détérioration de la sécurité de la blockchain sous-jacent. Dans notre troisième contribution, nous mettons en évidence les impacts précédemment inconsidérés de l'évolutivité de PoW blockchain sur sa sécurité et nous proposons des modifications de conception qui sont maintenant mises en œuvre dans le client Bitcoin primaire. Dans notre quatrième contribution, nous étudions la vie privée des clients Bitcoin légers, ceux qui sont les plus critiques à l'adoption générale de Bitcoin. De même, nous proposons des modifications de conception appropriées qui sont mises en œuvre pour protéger la vie privée des l'utilisateurs. En parallèle, dans notre cinquième contribution, nous analysons les impli-

cations des prix de transaction publics concernant la confidentialité de la localisation. Étonnamment, nous montrons que, étant donné que quelques prix d'un consommateur, nous pouvons positionner avec précision l'emplacement d'achat.