VRG18-002 - COnFIDE - Cryptographic Foundations of Privacy in Distributed Ledgers

Abstract

We are observing a trend towards decentralization to avoid single points of failure and trust in a single actor. Its epitome is the blockchain, a distributed ledger that ensures consistency of its entries and was introduced by Bitcoin, a currency with no central authority. Banks are also using distributed ledgers, in the form of Ripple, a distributed settlement network, but applications are now spreading far beyond currencies. Blockchains enabled smart contracts, which promise community-based applications that forgo reliance on centralized, typically commercial, actors. Central to all such systems is their transparency; anyone can view and check consistency of Bitcoin transactions. While public verifiability is a prerequisite for consensus in distributed ledgers, this openness conflicts with an increasing awareness (cf. the EU's recent GDPR) of the importance of privacy in a world where more and more user data is amassed and leaked in frequent security breaches. At the same time the civic freedom of making payments anonymously is disappearing together with cash, forcing citizens to submit to surveillance by payment providers and secret services. While cryptocurrencies may seem like an alternative, contrary to popular belief they often offer only very little privacy. Transactions can be traced, systems lack rigorous guarantees, make strong assumptions or they are not practically efficient. Traceability of coins moreover violates fungibility, a fundamental principle of currency that demands that all coins be equal. The overarching ambition of the COnFIDE project is therefore to reconcile public verifiability with privacy in distributed ledgers. The most promising approach to privacy are "zero-knowledge proofs", as used for example by the cryptocurrency Zcash. Their main shortcoming, which also conflicts with the spirit of decentralization, is their dependency on "trusted parameters". These are computed at system setup from random values that must then be securely disposed of (failing which enables e.g. counterfeit in Zcash). We see reducing the trust assumptions that are necessary to achieve privacy as the main challenge for distributed ledgers. Other issues with blockchains today concern their efficiency. "Proof of work" is used for consensus in all major systems, leading to Bitcoin's electricity consumption now approaching Austria's one. Alternatives either still rely on physical resources or are incompatible with privacy guarantees, and sustainable systems that protect privacy are still an open problem. Another shortcoming is scalability; while Visa's payment system handles 2000 transactions per second, Bitcoin handles 7. Moreover, all transactions remain in the blockchain forever, now over 160 GB for Bitcoin. While the current state of Bitcoin can be concisely represented by the set of unspent transactions ("UTXOs"), this is not possible in anonymous currencies, exacerbating scalability issues. To overcome the existing issues, we will first develop new cryptographic methods that reduce or eliminate the trust assumptions currently required for privacy. From these we will then build distributed ledgers with stronger privacy guarantees based on weaker assumptions. We will moreover investigate integration of means for prosecution of abuse, which is especially relevant for cryptocurrencies and their embedding in the legal framework; at the same time our goal is to prevent indiscriminate surveillance. Our next step will be reconciling sustainability with privacy in distributed ledgers. We will improve on systems based on "proof of space" and make "proof of stake", the most ecologically friendly consensus mechanism, compatible with privacy. Finally, to ensure scalability, our goal are blockchains that allow discarding obsolete information, so they only store the current state; and other means of increasing throughput, all while protecting privacy. The results of COnFIDE will be essential to the viability of next-generation distributed systems and will ensure the safety of citizens and protection of the environment in a time of vast technological change.

Wiener Wissenschafts-,
Forschungs- und Technologiefonds
Vienna Science and Technology Fund

Scientific disciplines:
Cryptology (90%) | IT security (10%)

Keywords:
cryptography; zero-knowledge; privacy; blockchains; distributed ledgers

---

VRG leader:	Georg Fuchsbauer
Institution:	TU Wien
Proponent:	Matteo Maffei
Institution:	TU Wien

Status: Ongoing (01.01.2020 - 31.12.2027)
GrantID: 10.47379/VRG18002

Further links to the persons involved and to the project can be found under
https://www.gmbh.wwtf.at/funding/programmes/vrg/VRG18-002/