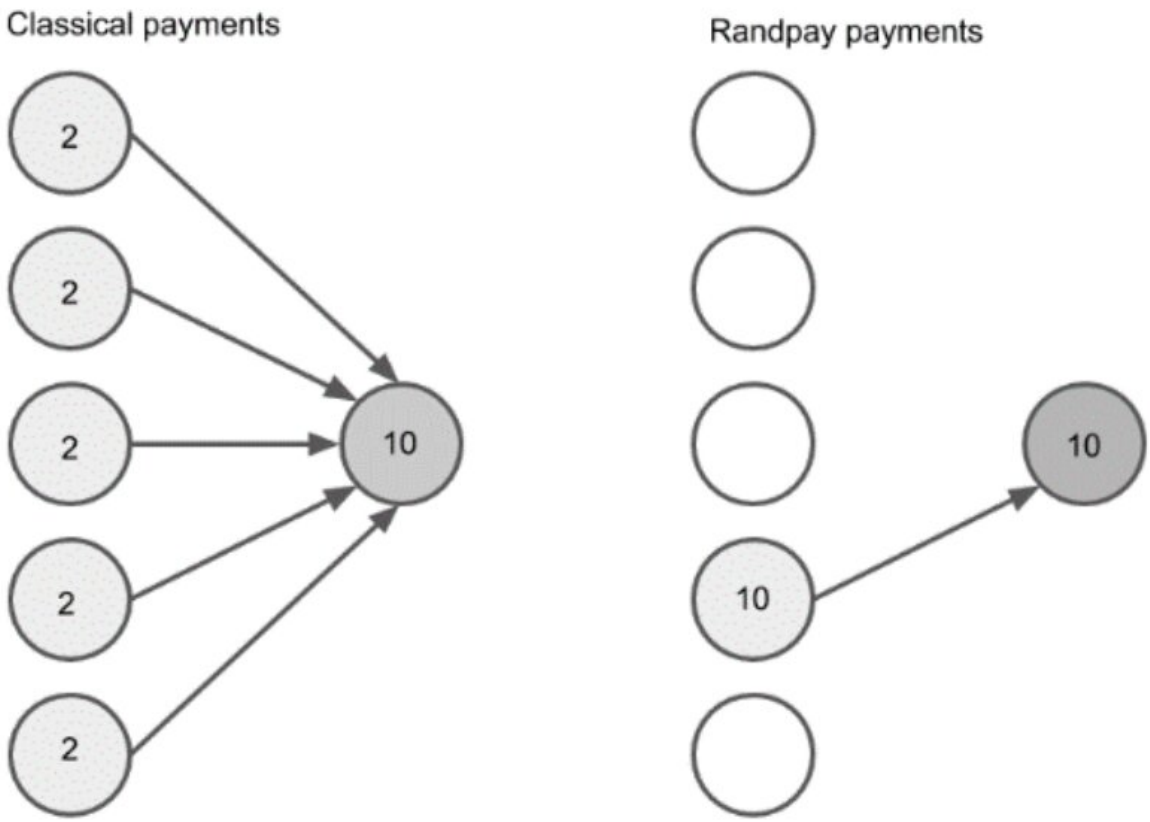
Randpay: a technology for blockchain micropayments that requires a recipient's consent

December 19 2019, by Ingrid Fadelli



A figure representing the core difference between classical payment systems and Randpay. Credit: Konashevych & Khovayko.

Two researchers at Emercoin, a decentralized peer-to-peer (p2p) network providing secure blockchain business services, have recently developed a new technology called Randpay that only allows users to complete payments and transactions with a recipient's consent. Using this new technology, presented in a paper pre-published on arXiv, users can also safely and easily micropay specific data values derived from sensors, individual stock quotes, downloaded pictures, search engine results, road tolls and other sources.

"Randpay opens a new niche in the business processes," Oleg Khovayko, one of the researchers who developed the technology, told TechXplore. "All other micropayment technologies have minimal sum limitations because of the low bound limit of transaction fees. With Randpay, transaction fees are reduced along with payment amounts. As a result, there is no payment minimum and payments can be as small as 1/100000 part of cent, if needed."

The blockchain protocol developed by the researchers draws inspiration from a system of electronic lottery tickets based on micropayments invented by Ronald Rivest in 1997. In his work, Rivest introduced the concept of electronic lottery tickets, where there is a centralized system and payments can only go through in the presence of a trusted third party and, where possible, a 'lottery facilitator'.

The blockchain protocol that is currently used by must cryptocurrency networks is unable to support peer-to-peer 'lottery' micropayments without the creation of so-called 'payment channels'. Oleg Khovayko and Oleksii Konashvych, the two researchers at Emercoin who developed Randpay, hoped to overcome this limitation by updating the more traditional blockchain protocol at its very core.

The new protocol they proposed requires a payee's signature to complete transactions and publish outputs in the blockchain. Remarkably,

Randpay is the first blockchain service that requires payment beneficiaries to sign off transactions using their private key.

When using the technology, the recipient of a payment creates a unique address, while also defining a space of possible payment addresses, including the one they created. Subsequently, the payer chooses a random address from the space delineated by the recipient, then creates and sends a payment or transaction to the selected address.

If the address he/she selected matches the one specified by the recipient, the recipient is asked to sign off the transaction. Once the recipient gives his consent, the transaction is published on the blockchain and the payment goes through. If the two addresses provided by the payee and recipient do not match, however, the transaction is considered invalid and consequently the sender's request is ignored.

In their recent paper, Khovayko and Konashevych offer mathematical proof that Randplay statistically converges to the fair amounts that all those participating in a transaction would receive or send if they used a different payment system. However, their system achieves this while significantly reducing the costs that payers usually need to pay to make transactions. This makes it ideal and economically viable, particularly for making micropayments.

"Only Randpay can process thousands of settlements per second (trillions per year)," Khovayko said. "No other blockchain technology can do this. I think that this is a unique practical achievement. Also, within our research, we provided mathematical proof of the correctness of our algorithm and its implementation based on statistics, cryptography and game theory. This is an important scientific achievement."

The blockchain technology developed by Khovayko and Konashevych has several other advantages, including the fact that it does not require

the creation and maintenance of separate channel operators. To use Randpay, in fact, users only need a regular Emer wallet and they do not have to pay network operators. This significantly reduces security risks associated with using third party operators.

Randpay offers its users the possibility to make unlimited peer-to-peer transactions, with the average payment for each action being less than the smallest unit in currently available cryptocurrency (i.e., Satoshi). In addition, the new blockchain technology allows users to find out whether their 'electronic ticket' has won almost instantly, without having to keep money in different channels for long periods of time.

Unlike lightning network blockchain technologies, which create one transaction for opening a given channel and one for closing it, Randplay creates a single transaction. Randpay is also stateless, which means that it has fewer restrictions and users do not need to enter any type of agreement with governments or other external parties. Moreover, it allows a payment to go through even if one of the parties disconnects from the internet before it is completed; thus, it also works if a user has a poor internet connection.

"In the future, Randpay could open the door for the next step after IoT (Internet of things)," Khovayko said. For instance, he says that one one EoT device could pay another for goods or services, and the payment decision made without human representation. Such devices work together when settling payments.

Khovayko said, "Imagine an EoT home controller that pays for your electricity/gas/water and earns money by selling electricity from your solar panel, data from your outdoor thermometer, or Wi-Fi traffic to outdoor strangers."

More information: Randpay: The technology for blockchain

micropayments and transactions which require recipient's consent. arXiv:1912.00007v1 [cs.CR]. arxiv.org/abs/1912.00007

medium.com/@emer.tech/randpay-6a028f16c82a

people.csail.mit.edu/rivest/pubs/Riv97b.pdf

© 2019 Science X Network

Citation: Randpay: a technology for blockchain micropayments that requires a recipient's consent (2019, December 19) retrieved 28 April 2024 from https://techxplore.com/news/2019-12-randpay-technology-blockchain-micropayments-requires.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.