ABSTRAK

UANG ELEKTRONIK BERBASIS *BLOCKCHAIN* DAN *SIGNCRYPTION* UNTUK TRANSAKSI *PEER-TO-PEER* MURNI

Oleh
Dany Eka Saputra
NIM: 33213004
(Program Studi Doktor Teknik Elektro dan Informatika)

Uang elektronik merupakan representasi digital dari uang yang digunakan sebagai alat pembayaran. Uang elektronik dapat ditransaksikan dari pemberi ke penerima melalui media elektronik seperti uang tunai. Salah satu metode transaksi yang dapat digunakan adalah *peer-to-peer*, transaksi uang elektronik dijalankan tanpa menggunakan entitas/peladen terpusat. Transaksi *peer-to-peer* digunakan untuk mengurangi kompleksitas komunikasi dan biaya transaksi, serta untuk menghindari terjadinya *bottleneck* di peladen terpusat. Meski tidak menggunakan entitas terpusat, sebagian besar uang elektronik *peer-to-peer* yang ada masih melibatkan pihak ketiga dalam transaksi, terutama untuk menjaga keamanan uang elektronik.

Penelitian ini mengembangkan metode transaksi uang elektronik yang dapat dijalankan dalam kondisi *peer-to-peer* murni, transaksi dijalankan hanya oleh pemberi dan penerima tanpa keterlibatan pihak ketiga. Permasalahan utama untuk mencapai tujuan itu adalah menjaga keamanan data uang elektronik, terutama mencegah pemalsuan data dan mendeteksi penggunaan ganda. Masalah ini menjadi masalah utama penelitian disertasi.

Untuk mengatasi permasalahan keamanan tersebut, data uang elektronik dibentuk dalam format *blockchain,* dan disimpan dalam perangkat pengguna. *Blockchain* digunakan untuk menjaga integritas data uang elektronik dari pemalsuan dan penggunaan ganda. Tiap blok dalam *blockchain* disambungkan dengan menggunakan sistem kripto *signcryption* berbasis identitas. Penggunaan sistem kripto ini memiliki fungsi ganda. Pertama, untuk meningkatkan tingkat integritas data uang elektronik. Kedua, sebagai mekanisme pelacakan identitas pelaku penggunaan ganda. Selain itu, penggunaan *signcryption* berbasis identitas memungkinkan otentifikasi pemberi dan penerima dapat dilakukan sebagai bagian dari transaksi tanpa melibatkan pihak ketiga.

Analisis kualitatif berbasis model uang elektronik dan analisis kuantitatif dengan menggunakan perhitungan Markov chain menunjukkan mekanisme ini dapat menjaga keamanan data uang elektronik. Pemalsuan data uang elektronik dapat dilakukan dengan probabilitas keberhasilan yang sangat kecil. Sementara, pelaku penggunaan ganda dapat dilacak dengan tingkat kepastian yang tinggi.

Kata kunci: uang elektronik, *peer-to-peer*, *blockchain*, *signcryption*.

ABSTRACT

BLOCKCHAIN AND SIGNCRYPTION BASED ELECTRONIC CASH FOR PURE PEER-TO-PEER TRANSACTION

By
Dany Eka Saputra
NIM 33213004
(*Doctoral Program in Electrical Engineering and Informatics*)

Electronic cash is a digital representative of money that can be used as legitimate payment method. The electronic cash can be transferred from payer to payee through electronic channel similar to how cash is transferred. Electronic cash can be transferred in peer-to-peer mode, where transaction is conducted between payer and payee without the involvement of centralized entity/server. Although centralized entity is not involved in the transaction, most of existing peer-to-peer electronic cash still involve a third party in its transaction, especially to ensure the security of electronic cash.

This research develops a pure peer-to-peer transaction method for electronic cash, where transaction is conducted without the involvement of third party in any kind. The problem with this condition is tho ensure the security of electronic cash data, especially to prevent forgery and detect double spending. This problem become the main issue in this dissertation research.

To overcome the problem, electronic cash data is structured as blockchain and stored locally in user's device. Blockchain is used to ensure the integrity of electronic data from forgery and double spending. Each block in blockchain is linked using identity-based signcryption cryptosystem. The usage of this cryptosystem serves multiple purpose. First, to strengthen the integrity of electronic cash. Second, to serve as a tracing mechanism to determine the identity of double spender. Identity-based signcryption also enable the authentication of payer and payee as a part of transaction without involving any third party.

Qualitative analysis using electronic cash model and quantitative analysis using Markov chain prove that the security of electronic cash can be maintained at adequate level. The probability to forge an electronic cash data is negligible. Meanwhile, the identity of double spender can be traced with high level of certainty.

Keywords: electronic cash, peer-to-peer, blockchain, signcryption.