Validasi Upgradeable Smart Contract untuk Mengembalikan Kepercayaan Pengguna = Upgradeable Smart Contract Validation to Restore User Trust

Christian Wisnu Purnaadi, author

Abstrak

Smart contract terinspirasi dari kontrak tradisional, dimana berperan sebagai dasar hubungan bisnis. Validasi dilakukan untuk memastikan smart contract sesuai dengan kontrak tradisional. Smart contract merupakan bagian fundamental dari blockchain bernama Ethereum. Blockchain adalah ledger terdistribusi dan diamankan dengan mekanisme konsensus berdasarkan kriptografi. Smart contract adalah program komputer yang disimpan di blockchain yang memungkinkan konversi kontrak tradisional menjadi paralel secara digital, maka akan berperilaku persis seperti yang diprogram. Blockchain dikenal memiliki immutability dengan memastikan blok-blok digabungkan dengan hash yang dienkripsi dalam blockchain, sehingga tidak ada yang dapat mengganggunya. Immutability sangat dibutuhkan untuk menjamin pencatatan dapat dipercaya, karena tidak dapat dimanipulasi oleh pihak manapun. Namun, kebutuhan akan pengembangan fitur baru telah memunculkan teknik upgrade. Di sisi lain terdapat pihak yang tidak setuju apabila smart contract dapat diupgrade karena dapat merusak immutability dalam blockchain, karena melalui upgrade akan merubah perilaku dalam smart contract. Pada kasus dimana smart contract memerlukan lebih dari satu kali transaksi. Pada jeda waktu tersebut pengembang dapat mengupgrade smart contract sehingga perilaku smart contract dapat berubah, hal ini dapat merugikan pengguna. Untuk mengatasi masalah tersebut maka diperlukan mekanisme upgrade yang transparan, sehingga dapat divalidasi. Pada penelitian ini mengusulkan sistem validasi smart contract untuk membantu pengguna publik memahami perilaku smart contract.
.....Smart contracts are inspired by traditional contracts, the basis for business relationships. Validation is done to ensure that smart contracts comply with traditional contracts. Smart contracts are a fundamental part of the blockchain called Ethereum. Blockchain is a distributed ledger and is secured by a consensus mechanism based on cryptography. Smart contracts are computer programs stored on the blockchain that allow the conversion of traditional contracts into digital parallels, so they will behave exactly as programmed. Blockchain is known to have immutability by ensuring that blocks are combined with encrypted hashes in the blockchain so that no one can interfere with it. Immutability is needed to ensure that records can be trusted because they cannot be manipulated by any party. However, the need for the development of new features has given rise to upgrade techniques. On the other hand, some parties disagree that smart contracts can be upgraded because they can damage the immutability of the blockchain. After all, upgrading will change the behavior of the smart contract, in cases where smart contracts require more than one transaction. During this time gap, developers can upgrade the smart contract so that the behavior of the smart contract can change, this can be detrimental to users. To overcome this problem, a transparent upgrade mechanism is needed, so that it can be validated. This study proposes a smart contract validation system to help public users understand the behavior of smart contracts.