# Memperkuat Fawkescoin Melawan Serangan Pembelanjaan Ganda Menggunakan Merkle Tree

**Widya Wirachantika[1], Ir. Ari M. Barmawi, MSc., PhD.[2],**

**Bambang Ari Wahyudi, S.Kom., M.T.[3]**

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]wirachantika@students.telkomuniversity.ac.id, [2] mbarmawi@melsa.net.id,
[3]bambangari@telkomuniversity.ac.id

**Abstract**

**Cryptocurrency is a digital currency with cryptographic security so that it is not easily to be faked. Recently cryptocurrency is widely used for transactions. Therefore, preserving its integrity and security is important. The technology underlying the digital currency is the Blockchain, as applied to Fawkescoin. But for securing the transaction, fawkescoin has a disadvantage when the fork occurs because it can provide opportunity to conduct double spending attack. To overcome this problem, Merkle tree proposed by applying DSA digital signatures. The application of DSA on Merkle tree is used to verify data without knowing the contents of the data. Based on the experiment results and analysis, the security of the proposed method can prevent fawkescoin against double spending attack on transactions when forking occurs than the previous method.**

**Keywords : cryptocurrency, blockchain, double spending attack, merkle tree.**

**Abstrak**

**Cryptocurrency adalah mata uang digital dengan keamanan kriptografi sehingga tidak mudah dipalsukan. Cryptocurrency baru-baru ini banyak digunakan untuk transaksi. Karena itu, menjaga integritas dan keamanannya adalah penting. Teknologi yang mendasari mata uang digital adalah Blockchain, sebagaimana diterapkan pada Fawkescoin. Tetapi untuk mengamankan transaksi, fawkescoin memiliki kelemahan ketika garpu terjadi karena dapat memberikan kesempatan untuk melakukan serangan pembelanjaan ganda. Untuk mengatasi masalah ini, pohon Merkle diusulkan dengan menerapkan tanda tangan digital DSA. Aplikasi DSA pada pohon Merkle digunakan untuk memverifikasi data tanpa mengetahui isi data. Berdasarkan hasil percobaan dan analisis, keamanan dari metode yang diusulkan dapat mencegah fawkescoin terhadap serangan pembelanjaan ganda pada transaksi ketika forking terjadi daripada metode sebelumnya.**

**Kata kunci:** ***cryptocurrency, blockchain, double spending attack, merkle tree.***

## 1. Introduction

Cryptocurrency is a digital currency with cryptographic security so that it is not easily to be faked. Since cryptocurrency is frequently used for bussiness transaction then it important to preserve the integrity and confidentiality of transaction. The technology underlying the digital currency is the Blockchain. Blockchain is a distributed database consists of transactions data history that are executed and shared between participants. The blockchain structure consists of transactions and blocks, where the transaction is exchanged between participants and a block is a collection of transaction data and other related information. The objective of blockchain is to create a node that are connected to each other based on their spending conditions to prevent double spending [1]. One of the digital currencies that implements the blockchain is Fawkescoin.

Fawkescoin is a simple cryptocurrency constructed using hash-based Guy Fawkes signature [2]. Guy fawkes signature is one simple digital signature algorithm that used to authenticate transaction based on one way hash function. However it has security problem when forking is applied on fawkescoin that is double spending attack [3]. A fork is a branching on the blockchain with a different protocol application so that if after forking process other block is found then the chain would be longer. Furthermore, the branch will become a part of the main blockchain [4]. When this condition occurred, all valid transactions from the shorter chain (the orphaned block) are added to the pool of queued transaction [1]. If this occurs, the attacker can spend the transaction more than once using the same coin in each transaction history that appears on the overwritten block, namely double spending attack [5]. Double sppending attack is occurred because the user revealing the transaction in the block as finalize message [3].

For overcoming the problem, a digital signature algorithm (DSA) (as shown in Section 3.1) and Merkle trees (as shown in Section 3.2) we proposed. Digital signature algorithm (DSA) is a public key cryptographic scheme to