Bitcoin ve Blokzincir (Blockchain) Teknolojisi

Ali Osman Çıbıkdiken
Necmettin Erbakan Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü
e-posta: aocdiken@konya.edu.tr

ÖZET

Bitcoin, 2008 yılında Satoshi Nakamoto isimli gizemli bir geliştirici tarafından matematiksel kanıt ve kriptografik yönteme dayanan bir elektronik ödeme sistemi olarak önerilmiştir [1]. Önerilen ödeme sistemi herhangi bir merkezi otoriteden bağımsız olarak çalışabilir. Para elektronik olarak güvenli, kanıtlanabilir ve değişmez olarak aktarılabilir. Bitcoin, Satoshi'nin makalesinden sonra anlık ödemeleri tercih etmek için merkezi olmayan ağı kullanan ilk dijital paradan biri oldu. Bitcoin bir yatırım olarak icat edilmese de, birçok kişi yatırım için borsalarda Bitcoin ve kripto para birimleri satın almaktadır. Bugün, insanlar dünya çapında 40'ın üzerinde borsada Bitcoin ticareti yapmaktadırlar. Pazar büyüklüğü 2018 Nisan ayı itibariyle yaklaşık 11 milyar dolara ulaşmıştır (https://coinmarketcap.com/charts/).

Blockchain, bugüne kadar yapılmış olan tüm Bitcoin işlemlerinin kaydedildiği bir halka açık defterdir [2]. Madenciler en son işlemleri kaydetmek için yeni bloklar ekledikçe (her 10 dakikada bir) sürekli olarak büyümektedir. Yeni bloklar sıralıbir düzende blok zincirine eklenir. Her bir tam düğümdeki Bitcoin ağına bağlı olan bir bilgisayar, bir müşterinin işlemleri onaylama görevini yerine getirmek üzere blok zincirinin bir kopyasına sahiptir. Bu kopya, madenci Bitcoin ağını bağladığında otomatik olarak indirilir. Bitcoin ağı, insanların hesaplama problemlerini çözmesi için bir imkan sunar ve bunu bir sorunu çözdüklerinde yeni Bitcoinler ile ödüllendirir. Yeni Bitcoinlerin oluşturulmasının tek yolu budur. Blokzincirini sayıya göre hesaplama ile doğrulamak "Bitcoin madenciliği" olarak adlandırılır.

Bizanslı Generaller (BG) Problemi [3], yani güvenilmez düğümler arasındaki konsensüsün dönüşümü, blokzincir mimarisinde çözülmüştür. Bitcoin ağında işin bir kanıtı (PoW), payın kanıtı (PoS), pratik Bizans hata toleransı (PBFT), paylaştırılmış kanıt ispatı (DPOS), Ripple, Tendermint gibi bazı konsensüs stratejileri kullanılır. PoW ve PoS çok popüler konsensüs stratejileridir. PoW'da, ağın her bir düğümü, blok başlığının [1] bir hash değerini hesaplıyarak gerçekleştirilir.

PoS (payın kanıtı), PoW'a göre bir enerji tasarrufu seçeneğidir. PoS'taki madenci, para miktarının sahipliğini kanıtlamak zorundadır. Daha fazla para birimi olan kişilerin şebekeye saldırma ihtimalinin daha az olacağı düşünülmektedir [44].

Zincirin üyeleri, veriyi girer ve eliptik eğri dijital imza kriptografik algoritması (ECDSA) ile açık bir şekilde erişilebilir bir blokzincir defterinde işlemi kabul ettiklerini onaylarlar [4].

Nakamoto, sadece A noktasından B noktasına para göndermekle kalmayıp, programlanabilir paraya ve bunu etkinleştirmek için tam özellikli bir sete sahip olmayı hayal etti. Örneğin, Turing-complete platformunu öneren bir blokzincir altyapı projesi Ethereum'dur [5]. Ethereum dağıtılmış uygulamalar oluşturmak için popüler bir platformdur. Bu, Turing-complete sanal bir makine olan (herhangi bir para, betik veya kripto para projesini çalıştırabileceği) bir genel amaçlı kripto-para birimi platformudur [6].

Blokzincir teknolojisi inanılmaz derecede disiplinlerarasıdır ve yazılım mühendisliği, ağlar, dağıtılmış sistemler, matematik, kriptografi, güvenlik, ekonomi, finans, para teorisi, risk, hukuk, felsefe, etik, sosyoloji, psikoloji ve siyaset bilimi gibi alanları bir araya getirmektedir [7].

ABSTRACT

Bitcoin has been proposed as an electronic payment system based on mathematical proof and cryptographical method by a mysterious developer going by the name of Satoshi Nakamoto in 2008 [1]. The proposed payment system can work independently of any central authority. The money can be transferred electronically in secure, provable and immutable. Bitcoin became one of the first digital cash to use the decentralized network to prefer instant payments after Satoshi's paper. Although Bitcoin was not invented as an investment, many people purchase Bitcoin and cryptocurrencies on exchanges for investment. Today, the people trade Bitcoin on over 40 exchanges worldwide. Market size reached about 11 billion dollars in April 2018 (https://coinmarketcap.com/charts/).

The blockchain is the public ledger of all Bitcoin transactions that have ever been performed [2]. It is continually growing as miners add new blocks to it (every 10 minutes) to record the most recent transactions. The new blocks are added to the blockchain in sequential order.

Each full node, every computer connected to the Bitcoin network using a client that performs the task of confirming transactions, has a copy of the blockchain. It is downloaded automatically when the miner connects the Bitcoin network. Bitcoin needs to provide a reason for people to solve the number crunching problems and it does this by rewarding people with new Bitcoins when they solve a problem. This is the only way that new Bitcoins are created. Verifying the blockchain by number crunching is called ‘mining’ Bitcoins .

The Byzantine Generals (BG) Problem [3], transformation of the consensus among the untrustworthy nodes, has been solved in the blockchain architecture. Some consensus strategies as a proof of work (PoW), proof of stake (PoS), Practical Byzantine fault tolerance (PBFT), delegated proof of stake (DPOS), Ripple, Tendermint are used in the Bitcoin network. PoW and PoS are very popular consensus strategies. In PoW, each node of the network is calculating a hash value of the block header [1].

PoS (Proof of stake) is an energy-saving option to PoW. Miner in PoS has to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network [44].

The chain members enter data and certify their acceptance of the transaction on an openly available blockchain ledger by an elliptic curve digital signature cryptographic algorithm (ECDSA) [4].

Nakamoto envisioned not only sending money from point A to point B, but having programmable money and a full feature set to enable it. One blockchain infrastructure project proposing to deliver the Turing-complete platform is Ethereum [5]. Ethereum is a popular platform for building distributed applications. It is a foundational general purpose cryptocurrency platform that is a Turing-complete virtual machine (meaning that it can run any coin, script, or cryptocurrency project) [6].

Blockchain technology is amazingly interdisciplinary and brings together fields including software engineering, networks, distributed systems, mathematics, cryptography, security, economics, finance, monetary theory, risk, law, philosophy, ethics, sociology, psychology, and political science, among others [7].

References

[1] Nakamoto, S., (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System".

[2] Collomb, A., Sok, K., (2016). “Blockchain/Distributed Ledger Technology (DLT): What Impact on the Financial Sector?”, Digiworld Economic Journal, No: 103, s. 93-110.

[3] Lamport, L., Shostak, R., Pease, M., (1982). “The byzantine generals prob- lem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401.
[4] Johnson, D., Menezes, A., Vanstone, S., (2001). “The elliptic curve digital signature algorithm (ecdsa),” International Journal of Information Se- curity, vol. 1, no. 1, pp. 36–63.
[5] Buterin, V., (2013). "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform".
[6] Swan, M., (2015). "Blockchain: Blueprint for a New Economy", O’Reilly Media.
[7] Morabito, V., (2017). "Business Innovation Through Blockchain:The B3 Perspective".