***Abstract***

Bitcoin işlemlerinin (transactionların) çoğunda kullanıcı yapmış olduğu işlemin bitmesi için onlarca dakika beklemek zorunda kalır. Üstelik bu işleme ait trasaction ın gerçekleşip gerçekleşmeyeceğine dair Bitcoin sistemi olası garanti sunar. Bu makale Bitcoin sisteminde yapılan bu transaction ları (işlemleri) saniyeler içinde yapan yeni bir Byzantine anlaşma protokolü olan ByzCoin ‘ i anlatmak için hazırlanmıştır. Byzcoin en son başaralı block miner ları gösteren anlaşma gruplarını (consensus groups) dinamik olarak oluşturarak bir Byzatine consensus (fikir birliği) protokolü oluşturur. ByzCoin transaction işlemlerini işlemek ve doğrulamak için iletişim ağaçlarını (communacation tree ) denen yapıları kullanır. Toplam *3f + 2* Byzatine hatasının oluştuğu ve *f* tolerans değerinin optimal kabul edildiği bir consensus grupta bu ağaç yapıları kullanılarak sisteme güvenilir düzeyde bir güvenlik kazandırılır. ByzCoin collectiive signed transactionlar (toplu imzalanmış işlemler) oluşturarak double spending ve selfish mining ataklarınız azaltır. Üstelik bu işlemi ByzCoin yaklışık bir dakikada yapar. Eğer bahsedilen ağaç yapılarıda düzgün optimize edilirse bu gecikme süresi yaklaşık 30 saniye kadar olur. Böylelikle ByzCoin Paybal şu an sunduğu throughput (maksimimum data transferi) den bile daha fazla throughput a ulaşır.

***Introduction***

Bitcoin şu an bankların kullandığı gibi bir merkezi otoritenin olmadığıdı bir kripto döviz kurudur (cryptocurrency) diyebiliriz. Yani transaction ları doğrulayacak, kontrol edecek bir merkezi otoriteye yoktur. Bitcoin sistemi peer to peer bir network üzerine kurulmuştur. Yani kullanıcılar bir merkezi otoriteye ihtiyaç duymadan birbileri arasında doğrudan transactionlar gerçekleştirebilmektedir. Miner denilen özel node’ lar transactionları toplar ve bu transactionlar üzerinde çeşitli hesaplamalar yaparak bu transactionların doğruluğuna karar verir ve bunları blockchain denilen dağıtık herkese açık bir veritabanına (distributed public ledger) bloklar halinde kaydeder.

Bitcoin makalesi ilk yazıldığında bu sistemde gerçekleşen bu transaction’ ların güvenilir ve geriye dönük işlenemeyeceğini söylemekteydi; fakat bu transactioların miner lar tarafından doğrulanması uzun gecikmelere sebep oldu ve bu da bitcoini gerçek zamanlı transactionlarda uygun olmadığını ortaya çıkardı. Ayrıca bu sisteme transaction reversibility, double-spending gibi ataklar yapıldı.