***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.

Mail den gelecek

ByzCoin collective signing (CoSi) adı verilen bir protokol üzerine kurulmuştur. Bu protokol yüzlerce hatta binlerce imzayı etkili bir şekilde birleştirmektedir. Ayrica CoSi PBFT round sayıların düşürerek müşterilerin transaction işlemlerinde daha hızlı sonuç alması sağlamaktadır. CoSi bir consensus protokolu değlildir. Consensus protokolü olarak Byzcoin de Byzantine consensus protokolü kullanılır. CoSi bu sistem de PBFT round ların imzalamak için kullanılır ve PBFT yi hazırlık ve işleme fazları için daha ölçeklenebilir yapar.

***Background and Motivation***

Bu bölümde Byzcoin i oluşturan cryptocurrency, Byzantine fault tolerance ve collective signing temel altyapıları anlatılacaktır.

***2.1 - Bitcoin and Variations***

Bitcoin’in dayandığı en temel altyapı blockchaindir. Bilindiği gibi blockchainde tüm transaction ların kayıtlarının tutulduğu bir dağıtık veri tabanı (ledger) vardır. Hash değerleri minerlar tarafından doğrulanan transactionlar bu veri tabanına (ledger a) eklenir. Transaction lar bloklara ayrılır ve bu blokların doğruluk değerleri proof of work denilen bir mekanizmayla sağlanır. Her blokta en son doğrulan blokların hashini tutan hash zinciri vardır ve yine her blokta sonraki çıkacak yani blokaları gösteren Merkle tree [1] denen yapılar vardır. Bu mekanizma blok zinciri oluşturulmuş olur.

Bir miner tarafından çıkarılan ve proof of work mekanizmasından geçip doğruluğu kesin olan bir blok diğer minerlar tarafından da doğruluğu onaylanırsa bu blok zincire eklenir ve zincir uzar. Blok doğrulama mekanizması blockchain de bu şekilde çalışır; fakat Bitcon’ de ki bu mekanizma sadece olası kalıcı garanti sunar ve bu durum beraberinde iki problemlere sebep olur.

İlk olarak, iki ya da daha fazla miner aynı parent a sahip farklı bloklar bulmuş olabilir ve bu durum network bu blokların doğruluğuyla ilgili karar vermesinden yani zincire eklenip eklenmemisine karar verme öncesinde probleme sebep olur. Bu duruma blockchainde fork adı verilir. Bu durum bu bloğun herhangi bir geçerli bir blok zincirine eklenmesine kadar devam eder. Yani geçici bir durumdur fakat ağda tutarsızlığa (inconsistency) ve gecikmeye neden olur diyebiliriz. Blockchainde kabul edilen thumb [2] kuralı gereği bir bloğun kalıcı olarak blok zincirine kaydedilmesi için üzerinde yaklaşık olarak 6 yeni blok daha çıkarılmalıdır. Fork durumunun oluşması (yani fork )yeni blokların zincire eklenmesini geciktireceğinden bitcoin müşterilerinin transaction işlemlerinde gecikmeye sebep olur.

İkinci problem ise Bitcoin’deki blok boyutunun 1MB olmasıdır. Böyle bir limit saniyede işlenecek transaction sayısı sınırlamaktadır.(Bu transaction sınırı Bitcoin tahminen 7TPS. (Yani saniye 7 transaction). Oysa Paypal saniye 500 TPS, VISA 4000 TPS işlem yapabilmektedir. Bu durumu ortadan kaldırmak için blok boyutları artırılabilir; fakat bu durum ise ağda oluşacak fork sayısı artırır ve bu da gecikmeklere neden olur. Ayrıca double spending attack [3][4][5] gibi atakların artmasına neden olur. Bitcoin in güvenliği oluşacak fork sayısıyla doğrudan ilişkili olduğundan bu duruma çözüm bulunması gerekir.

**Bitcoin-NG :** Bitcoin NG’ e göre [6] Bitcoin’ de ki blokların iki temel amaca hizmet eder. Birincisi muhtemel çıkacak transaction tutarsızlığında bunların nasıl çözüleceğini belirleyen leader (çözecek lider node) node un seçimi. İkinci ise transactionların doğrulanması. Yani Bitcoin-NG blokları amaçlarına göre bu şekilde 2 gruba ayırır. *Keyblocks*  (Anahtar bloklar) lider (leader) i seçmek kullanırlar ve yaklaşık her on dakikada bir mining yapılarak oluşturulurlar. *Microblocks* (mikro bloklar) transcation ları içeren bloklardır. Bu bloklar seçilen lider blok tarafından oluşturulurlar ve doğrulanırlar(signed). Blokları bu şeklide ayıtmak Bitcoin-NG ye daha fazla throughput değeri verir.

Bitcoin-NG’ de Bitcoin’ de de olduğu gibi tutarsızlık problemleri mevcuttur. Aynı anda oluşabilecek keyblock sırasında fork durumları yaşanır ve bu da muhtemel saldırı türlerine karşı bu sistemi açık kılar.

***Byzantine Fault Tolerance***

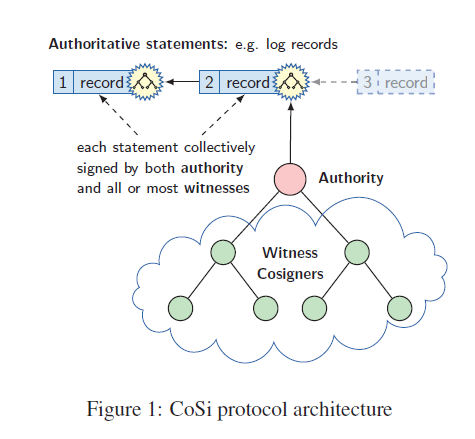
Bir sistemde fonksiyonlarını düzgün yerine getiremeyen bir ya da daha fazla eleman varsa bu elemanlar sistemin düzgün şekilde çalışmasını engelleyebilir ve bu probleme genel olarak Byzantine problemi denir. Bir sistemde f değeri kadar hata varsa başka deyişle f eleman düzgün çalışmıyorsa bu sistemi düzeltmek için 3f + 1 eleman gereklidir [6]. Practical Byzantine Fault Tolerance (PBFT) internet gibi senkronizasyon problemlerinin olduğu ortamlarda bahsedilen Byzantine problemine çözüm getiren ilk algoritmadır.

PBFT de her round farklı 3 fazdan oluşur. İlk fazda yani *pre-phase* denilen fazda current primary node ya da lider node (leader) tarafından yeni eklenecek kayıt belirlenir ve sisteme bildirilir. Bu mesajı alan node lar bu önerinin doğruluğunu değerlendirir ve diğer node lara (gruba) bir prepare mesaj denilen bu mesajı iletir. Bu mesajı ilettikten sonra nodelar yeterli çoğunluk sağlanırsa yani 2f +1 mesaj toplanırsa bu mesajı işlerler (commit).

PBFT roundların yani bu algoritmanın kullanıldığı bu sisteminin düzgün çalışabilmesi tamamen correct leader (doğru lider) bağlıdır. Bu yüzden bu lider doğru ya da sahte olup olmadığı kontrol eden view-change denilen bir protokol vardır. Nodelar sürekli olarak liderin hareketleriniz izlerler. Eğer lider node un hareketlerinde şüpheli bir durum varsa nodelar liderin gönderdiği mesajları doğrulamayı durdurlar. Eğer nodelar arasında 2f + 1 kadar node liderin doğru olmadığı kararına varısa yeni lider seçilir.

PBFT algoritması bazı kısıtları vardır. İlk olarak bu sistemdeki kopyalar iyi tanımlanmış sabit uzunlukta gruplar olmalıdır. Böyle bir sistemde Bitcoin sisteminin öne sürdüğü dağıtık ve herkese açık olma kuralıyla uyuşmamaktadır. İkinci problem ise her kopya herhangi bir rounda diğer kopyalarla doğrudan haberleşir. Bu işlem yaklış O(n^2) lik bir karmaşıklık yaratır. Bu karmşıklık değerleri n=4 ve daha düşük değerler için uygundur; fakat n değeri yani node sayısı yüzlerce olduğunda bu algoritma uygulanabilir değildir. Son problem ise PBFT servisine bir transaction gönderildiğinde client transaction ın doğruluğunu öğrenmek için birden çok kopyayla(replicas) haberleşmek zorundadır.

***Scalable Collective Signing***

******

CoSi ölçeklenebilir ve toplu bir şekilde imzalanmayı (scalable collective signing) sağlayan bir protokoldür. Bu protokol de doğrulamayı sağlayan *author* denilen ve toplu imzalamayı sağlayan *witnesses* denilen yapılardan oluşur. Tek bir imza mekanizmasıyla karşılaştırıldığında daha fazla işlem yüküne ve maliyete sebep olsada bir işlemin hem leader hem de witness lardan tarafından onaylananmasıyla sistem daha güvenli hale gelir.

Sistemi daha ölçeklenebilir yapmak için CoSi protokolü multicast protokollerde kullanılan haberleşme ağaçlarını (communication trees) [8][9][10] ve Schnorr multi signature [11] yapılarını birlikte kullanır. Bir mesajın topluca (collective) imzalanabilmesi için leader tarafından dört fazdan oluşan bir işlem başlatılır. Bu işlem leader ve witness lar arasında olur ve bu iki yapının haberleşmesi için communication trees kullanılır.

**1-Announcement :** Bu fazda lider haberleşme ağacına collective signing işleminin ilk round un başladığını bildirir ve ek olarak imzalanacak mesajı gönderilebilir. Eğer mesaj gönderilmezse 3. Fazda gönderilir.

**2-Commitment :** Her node rastgele bir secret seçer ve bunu bir Schnorr commitment (Schnorr taahhütü) değerini hesaplamak için kullanır. İlk olarak alt node larından (childrens) değerlerini alır ve bunları birleştirerek bir Schnorr commitment oluşturarak haberleşme ağacına iletir.

**3-Challenge :** Lider kriptografik hash fonksiyonlarını kullanarak collective Schnorr challenge değerini hesaplar ve bunu ağaca aktarır. Eğer mesaj birinci fazda gönderilmediyse bu fazda mesaj da ağaca aktarılır.

**4-Response :** Leader den gelen schnorr challenge değeri nodelar tarafından alınır ve ortak bir response üretilir.

Tüm bu dört fazın sonunda Schnorr imzası denilen ve 64 byte olan bir değer ortaya çıkar. Bu imza daha sonra imzalama işlemlerinde efektif bir şekilde kullanılabilir.

***Byzcoin Design***

Bu bölümde Byzcoin adım adım en temel yapıtaşlarından ki bunlar; strowman combination of PBFT ve Bitcoin başlayarak ele alınacaktır.

***System Model***

İlk olarak Byzcoin güvenilmeyen networkler için geliştirilmiştir. Bu tür networkler mesajlar iletilmeye bilir, gecikebilir ya da mesajlar çoklanabilir(duplicate). Byzcoin N block miner dan oluşur ve bu minerlar key pairlerini üretebilirler; fakat güvelinen bir public-key altyapısı yoktur. Bu yapıda her nodeun sınırlı hash hesaplayabilme gücü vardır. Herhangi bir t anında bir miner grubu bir hacker tarafından ele geçirilirse bu ele geçirilen miner grubunun toplam hash gücü sistemin toplam hash gücünün 1/4 den büyükse ve bu sistemde selfish mining[14] attack gibi ataklar yapılabilir.