Zentachain

E-mail:Team@zentachain.io

WHITEPAPER CONTRIBUTORS

Core-Member

Harun Kacemer

Musa Mani

Daniel Wale

Ali Muhammed

Göktas Polat

0xSha512

SPECIAL THANKS TO

Zentachain and friends!

Zentachain

Güvenlik ve anonimlik için tasarlanmış, merkezi olmayan bir blockchain tabanlı ekosistem.

Zentachain Lab
Zentachain.io

(Tarih: Aralık 2018, Versiyon 0.1)

Zentachain güvenlik ve anonimlik üzerinde güçlü bir odaklanma ile tasarlanmış, yüksek verimli, merkezi olmayan blok zincir tabanlı bir ekosistemdir. Ekosistem şifreli verileri saklama ve ölçeklenebilir merkezi olmayan uygulamaları ve dağıtılmış hizmetleri barındırma yeteneğine sahiptir. ZentachainMVP, Ethereum blockchain üzerine inşa edilecek ve Zenta olarak da adlandırılan ERC20 standardını kullanacak. İstenilen performans ve sürdürülebilirlik gereksinimlerini karşılamak, için, Zentachain Raiden veya Casper gibi en son teknolojiye sahip lightning ağları ile etkileşime girer ve çeşitli katmanlarda yenilikler yapar. Ethereum Smart sözleşmeleri, Zentachaingeliştiricilerinin uygulamalar oluşturmasını ve platformda özel hizmetler dağıtmasını sağlar. Alfa lansmanından sonra Zentachain ekibi kendi blok zincirini başlatacak. Şu anda Zentachain Labs, diğerlerinin yanı sıra Nano (blok kafes), EOS ve Ontoloji gibi temel yapıların temelini oluşturmak için çeşitli seçenekler düşünüyor.Ekosistem ölçeklenebilir ademi merkeziyetçi uygulamalar ve dağıtılmış hizmetler ve P2P merkezi olmayan bulut depolaması oluşturmak ve barındırmak için gerekli tüm yapı taşlarını tutar. 5 katmanlı mimarisi, her biri özel bir işlevi olan beş bağlı katmandan oluşur.

İÇİNDEKİLER

1. Çözmeye Değer Problem

Kişinin güvenli etkileşim ve dijital veri depolama ihtiyacı

A. İzinsiz veri erişimi ve bilgi akışlarının manipülasyon durumunu çözmek
B. Hacker'lara karşı koruma - İzinsiz erişim sağlama ve bilgi çalma, verilerinizi kaydetme, toplama ve satma.
C. Leverage net neutrality
D. Veri ve veri güvenliğinin sahipliğini sağlamak
E. dApp'lerin barındırılması ve oluşturulması için güvenli bir çerçeve sağlama
F. Cloud Storage(Bulut depolama) alanının sahipliği ve güvenliği
G. Şifrelenmemiş, güvensiz veri depolama işleminizde bazı dijital ortamlarda yaptığınız işlem tarafından cihazınızda yapılan her işlem potansiyel olarak kaydedilebilir ve bir veritabanında veya dosya sunucusunda bir yerde saklanır. Bu verilerde bunun uygun şekilde şifrelenmemiş veya anonimleştirilmemiş olması muhtemeldir.

2. Vizyon

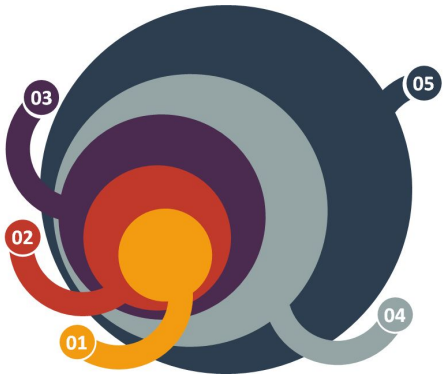
Zentachain, net tarafsız veri ve işlem değişimi için merkezi olmayan bir ekosistem inşa edilmesini ve veri depolama işlemlerini gerçekleştirmeyi planlamakadır. Ekosistem, kullanıcıları tarafından korunur ve her türlü siber saldırı ve ataklara karşı bağışıklık kazanır. Bunun yanında, güvenlik ve veri sahipliği problemleri için uygun çözümler mevcut. Zentachain açık kaynak kodludur. Zentachain, IPFS (https://ipfs.io) gibi merkezi olmayan meshnet bulut hizmetleri ile DNS ve HTTPS gibi dinamik yönlendirme ve adresleme protokolleri arasındaki boşluğu doldurmayı hedeflemektedir. Bu, Zenta Labs'in IPFS eşler arası hypermedia protokolünü en gelişmiş blok zinciri teknolojisi ile geliştireceği gerçeğine dayanmaktadır.

Ağ yalnızca ultra güvenli ve merkezi olmayan ve kalıcı hale gelmeyecek. Ayrıca daha hızlı ve daha şeffaf hale gelecektir. Zentachain, IPFS ile büyük miktardaki verileri ele almayı ve bir blok zincir işlemi kullanarak değişmez, kalıcı IPFS bağlantılarını Zenta defterine yerleştirme özelliğini sağlayacak. Bu zaman damgası, verileri ZentaChain'e koymak zorunda kalmadan içeriğin güvenliğini sağlar. Bunun yanında, Zentachain meshnet üzerinde depolanan dosyalara ek şifreleme ekleyecektir. Zentachain, web'in özgürlüğünü ve bağımsız ruhunu tam güçte ve düşük maliyette sunar. Ekosistem, içeriği önemli ölçüde tasarruf etmenizi sağlayacak şekilde sunmaya yardımcı olacaktır.

Yüksek gecikmeli ağlar, gelişmekte olan dünyaya gerçek bir giriş engelidir, Zentachain, düşük gecikmeden veya omurgaya bağlantıdan bağımsız olarak verilere esnek erişim sağlar. Zentachain, herhangi bir istisna olmadan merkeziyetsizlik istemekte olup ve ekosistemi, kullanıcılarını asla takip etmeyecek ve IP adresini veya kişisel bilgilerini asla kaydetmeyecek şekilde tasarlayacaktır. Ekosistem tasarım gereği bu bilgilere sahip değildir ve işlemleri belirli bir kullanıcı veya kimliğe bağlayamaz.

3. Zentachain Ekosisteminin Mimarisi

Zentachain 5 katmanlı mimarisi güvenli bir olanak sağlar ve aynı zamanda dApps ve güvenli taşıma katmanlarının geliştirilmesi için optimize edilmiş bir modülerliğe sahiptir.



01 **zentacore** : güvenlik & iş core

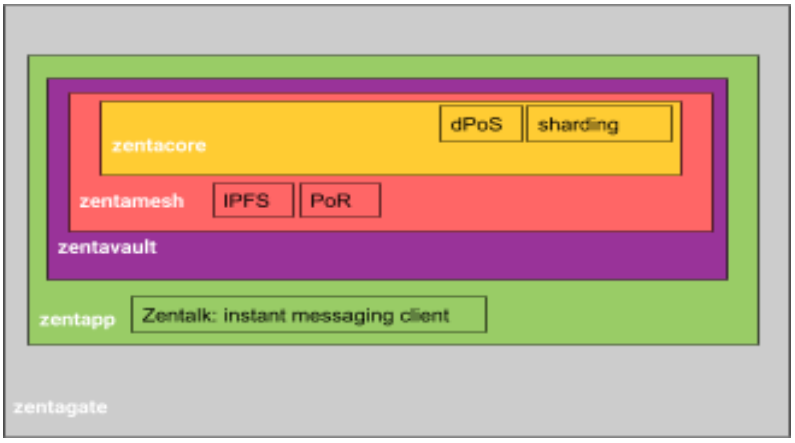
02 **zentamesh**: Merkezi olmayan meshnet

03 **zentavault**: Merkezi olmayan veri depolama

04 **zentapp**: dApp yapma ve sahipllik

05 **zentagate** : internet girişi

Bunlar Zentachain' i harika yapıyor:



Güvenlik & İş

Zentacore, ekosistemin tüm iş mantığına sahiptir. Akıllı sözleşmelere ev sahipliği yapmaktadır - yöneten ve fikir birliği modelleri - meshnet yönetimi ve Zentachain gibi blockchain teknolojisini kullanan bu tür teknolojiler kullanılarak Ethereum ölçeklenebilirliğini büyük ölçüde artıracaktır. Sharding , ağdaki verilerin yatay olarak bölümlenmesini sağlar. Yatay olarak ölçeklendirerek, böylece sistem işlemlerini bölerek ve yükü dağıtarak, saniyede Yüksek İşlem (TPS) oranıyla sonuçlanan yüksek miktarda veri elde edecektir.

3.1 Zentacore

3.2 Zentamesh merkeziyetsiz meshnnet Merkle Ağacı

3.3 Zentavault merkezi olmayan veri depolama

3.4 Zentapp dApp yapma ve sahiplik

3.5 Zentagate internet Bileşenleri için Ağ Geçidi

4.Zentachain'i harika yapan şey nedir?

ZentDapp: Dağıtık gizlilik hizmetleri için tasarlanmıştır. Zenta, kullanıcıların ekosistem içinde dApps oluşturmasını ve barındırmasını sağlar. Tüm çalışan dApp'ler tasarım olarak anonim ve güvenli olacak, hiçbir kullanıcı kaydı ve bağlantılı işlemler platformda saklanmayacaktır. ZentaChain'in yeteneklerini kanıtlamak ve göstermek için ekip, merkezi olmayan ultra güvenli bir mesajlaşma uygulaması tanıtıyor.

Zentalk

Zentalk güvenli ve merkezi olmayan bir peer to peer(eşler arası) mesajlaşma dApp'dir. Kullanılabilirliğin yanı sıra, arka planda son teknoloji şifreleme ve güvenlik bulacaksınız, dolayısıyla Zentachain tam bir gizlilik garanti etmektedir. Zentalk aracılığıyla gönderilen ve alınan tüm mesajlar, yüksek performanslı bir MeshNet olan Zentamesh aracılığıyla tünellenecek ve iletilecektir. Bu, Zentalk'a sansür ve gizli dinleme teşebbüsü gibi herhangi bir hack veya müdahale olaylarına karşı tam koruma olması konusunda benzersiz bir avantaj sağlar.

Zentavault

Zentavault, yüksek verimli şifreli ve dağıtılmış bir dosya kasası (şifreli depolama) ve transfer hizmetidir. Düzenli veri depolama sistemlerinden farklı olarak, Zentavault, kullanıcıların cihazında hiçbir şey depolamaz. Zentavault, içeriği IPFS'ye güvenli bir şekilde şifreleyip dinamik olarak dağıtabilen bir şifreleme dağıtım aracı olarak işlev görür. IPFS, tüm bilgi işlem aygıtlarını aynı dosya sistemine bağlamayı amaçlayan eşler arası dağıtılmış bir dosya sistemidir. Bazı açılardan IPFS, World Wide Web'e benzer, ancak IPFS, tek bir BitTorrent swarm olarak görülebilir ve bir Git deposunda nesneler alışverişinde bulunabilir.

Zentagate

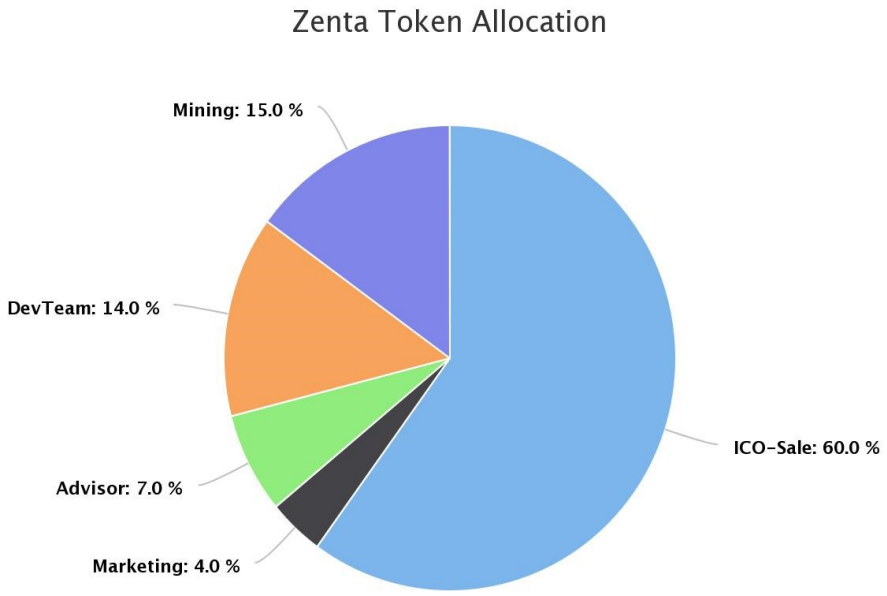
„IPFS-DNS ve HTTP-Gateway, ZentaGate için 2 görev olacak “

ZentaChain'de güvenliği ve anonimite olayını çok ciddiye alıyoruz. ZentaChain'i, kendi özel Mesh ağında çalışacak şekilde tasarladık. Zentagate, ekosistemi internet gibi güvenli olmayan ağlara bağlar. Zentagate, kullanıcı verilerinin ve işlemlerin güvence altına alındığından emin olmak için ek bir şifreleme ve saldırı önleme katmanı sağlar. Güvenli olmayan ağ geçişlerinin yanında,merkezi olmayan bir isim hizmeti de uygulamayı planlıyoruz. Zentagate bu servisi çalıştıracak - veri ve işlemlerin ZentaChain'e girip çıkarılmasını sağlayacak.

5.Ekonomi & ICO

Token Dağıtımı

Resmi token adı: **ZENTA**
Token Sembolü: **ZENTA**
Algoritma: **DPOS**
Blockchain: **Ethereum - ERC20**
Token Sayısı(Total supply): **260.514.201 ZENTA**
Softcap başlangıç token satışı: **$3.000.000**
Hardcap başlangıç token satışı: **$10.000.000**
Satış için planlanan token sayısı **60% - 156,308,520**



Token fiyatı bu formülle hesaplanacaktır:

OrtalamaETHfiyatı / (Hardcap/TokensForSale/Rate/ProCenture)(PubSale/TokenForSale/Rate/ProCenture-0%)

6.Gelir Akışı

DPoS - Zenta staking ve ekosistemi yönetme Delegated Proof of Stake (DPoS olarak da bilinen), ağdaki gerçek üzerinde reddedilemez bir anlaşmayı sürdüren, işlemleri onaylayan ve dijital demokrasinin bir şekli olarak hareket eden bir fikir birliği algoritmasıdır. DPoS, mutabakata varmak için sosyal itibar sistemi ile birlikte gerçek zamanlı oylama kullanır. En kapsayıcı şekli olduğu için, diğerlerine kıyasla en az merkezi konsensüs protokolü olduğu görülebilir. Her token sahibi, ağda olanlarla ilgili bir ölçüde etkide bulunabilir. Başka bir deyişle: Zenta tokenlerinizi elinizde tutmak, oy kullanma gücü sağlayarak fazladan tokenler ile sizi ödüllendirecek.

1) **Ağdaki tüm düğümler birbirine bağlı.**
2) **Mevcut düğümler ağdan ayrılmayacak ve yeni düğümler ağa katılamayacak.**
3) **Tüm düğümler aynı ağırlığa veya oylama gücüne sahiptir ve bu nedenle aynı hisseye sahiptir.**
4) **Ağda gecikme yoktur.**

PoR - Zentameshnet üzerinde veri aktarımı

Aktarma işlemleri tokenlerle ödüllendirilecektir. Zentamesh, sunucu yönetiminden bağımsız olarak işlem yönetimini bu istemcilere taşır ve bu durumda aynı ağa ait eşleri arayacaktır. Her ağ, tüm katılımcılar tarafından iyi tanımlanmıştır: bilgi ömrü daha sonra ağdaki aktif akran sayısına bağlıdır. Bilgi alışverişi blok zincirinin kendisidir. Bu nedenle, bir eş senkronizasyon mekanizmasına sahip olmak gereklidir.

Literatürde,Cryptovalut'a da değinen birkaç algoritma var, blockchain röle ispatına dayanan özel bir uygulamaya sahip: zaman ispatının dinamik bir evrimi. Böylece, mesh ağını oluşturan eşler arasında hareket eden ve defteri onaylayan grupları birleştiren bir röle geliştirdik. Proof of relay kullanmanın faydaları şöyledir:

1. **Mesh konfigürasyon ile uyumludur.**
2. **Ağ tıkanıklığına yanıt verir.**
3. **Daha sonra proof of time olarak hareket eder.**
4. **Durdurulabilir**

Listelenen tüm olumlu faktörler, zaman içinde yanıt oranını artırabilen ve aynı zamanda çok az elektrik tüketen bir blok zincirine sahip olmak için uygulanmıştır. Zincir servisleri küçük bir ağ işlem ücreti gerektirir. Ekosistem, giriş ücretleri Zentachain yöneticilerine geri dönecek şekilde tasarlanacaktır.

Whitepaper

zentachain.io

“Gelecek, bugünün potansiyelini göstermektedir”

8.Ön Aşama

Dijital devrim, içinde bulunduğumuz dünyayı yeniden yazdı. Şimdiden geleceğimizin yeni bir versiyonunda yaşıyoruz. Barbrook'un 2006'da dediği gibi: "Yeni teknolojinin önemi burada ve şu anda yapabilecekleri için değil, daha gelişmiş modellerin bir gün yapabilecekleri içindir. Bugün embriyo'da gelecek olarak anlaşılıyor - ve gelecek, mevcut potansiyelini aydınlatıyor". Dijital dönüşüm, geleceğimize daha büyük katkı sağlamaktadır. Bu günlerde insanlar teknolojiye her zamankinden daha fazla güveniyorlar. Kişisel bilgisayar ve son zamanlarda akıllı telefon icat edildiğinden, neredeyse tüm dünya birbirine bağlanmış gibi görünüyor. Dijital iletişim ve etkileşimler, sosyal medya, kullanıcılar tarafından oluşturulan web siteleri ve ücretsiz çevrimiçi ansiklopediler olmadan bir dünya düşünemiyoruz. İnternetin önemi, hepimizi birbirine bağlayan fiberler, artmaya devam ediyor. Artık dünyaya erişiminiz var ve de dünyanın size erişimi var. Daha fazla dijitalleşme olumlu olarak değerlendirilebilir, çünkü bütün çalışma biçimini değiştirir, daha kullanışlı ve verimli kılar. Hareketliliği ve üretkenliği arttırmış ve özel bir çalışma alanına olan ihtiyacı azaltmıştır. Ancak dijital devrimin de karanlık bir tarafı var ve bu tam olarak ZentaChain'in veri dosyalarınızı ve belgelerinizi merkezi bir sunucuda saklayan şirkete karşı koruyacağı şeydir. Zentalk sizleri, iletişim ve mesaj geçmişinize sahip olarak bu bilgileri satabilecek büyük şirketlerden korur.

9.Çözülmeye Değer Problem

Girişimcilerin sahip olmak istediği güvenli etkileşim ve dijital veri depolama ihtiyacıdır. İzinsiz veri erişimi ve bilgi akışlarının manipülasyonu her zaman bir tehdit olmuştur, ancak bu tehdit ilk ağın icat edilmesinden bu yana artmaktadır.

Hackerlar şimdi size birçok ülkeden, farklı bölgelerden ve aynı anda birden fazla yerden saldırabilir. Yeterince kötü değilse, verilerinizin kaydedilmesi, toplanması ve satılması ile kazanç elde eden milyar dolarlık şirketler de vardır.

Konum geçmişinizi, mesajlarınızı, fotoğraflarınızı, belgelerinizi ve hatta sizin için oluşturdukları profilleri satabilirler. Hakkınızdaki her şey, niyetleri ne olursa olsun, bu verileri isteyen tüm dünyadaki yozlaşmış organizasyonlara açık artırma ile satışa hazır. Bazı telekomünikasyon şirketleri kullanıcı verileri ve işlemlerle ilgili depolama yapabilir. Düzenlemeleri bu şekilde olsa ve bunu yapmamaları gerekse bile(kanunen satmamaları gerekiyor), asla bunu yapmadıklarını bilemezsiniz, belki de "eğitim" amaçları için bir gün ihtiyaçları olacak. Şifrelenmemiş, güvenli olmayan veri depolama aygıtınız üzerinde yaptığınız işlemle, bazı dijital ortamlarda yaptığınız işlemlerin tümü, potansiyel olarak günlüğe kaydedilir ve bir veritabanında veya bir dosya sunucusunda bir yerde saklanır.

Bu verilerin uygun şekilde şifrelenmemiş veya anonimleştirilmemiş olma ihtimali yüksektir. Sosyal medya şirketleri tarafından sunulan hizmetler ve mesajlaşma uygulamaları, tüketiciye hiçbir bedel ödenmeyen "ücretsiz bir hizmet" olarak kendilerini tanıtmaktadır. Bunun yerine, bu şirketler tüm verilerini ve içeriklerini çevrimiçi olarak depolamak ve manipülatif olduğu bilinen sinsi kuruluşlara satmak için düzenli olarak çalışmaktadır. Bu, hizmet için aylık ücretler yerine verilerini vermektesiniz.

10.Veri Hack'leme & Zaaflar

İnternet kullanıcı sayısı her geçen gün artmaktadır (2007'de 1.36 milyardan - 3.57 milyara 2 milyardan fazla kullanıcı artışı son 10 yıl içinde gerçekleşti)günlük hayatımızın nasıl daha da sanallaştığı ve duygularımız, düşüncelerimiz ve kişisel bilgilerimizin - temelde kimliklerimizin, çevrimiçi dünyaya girme yolunda ilerleyen, onları bu verileri kendi kişisel kazançları için kullanmak isteyen hırsızlara karşı savunmasız bıraktığı gözlemlenebilir.

Herşeyin ve herkesin hedef olabileceği bir noktaya geldik. Kimlik avı yoluyla yapılan kişisel saldırılardan, ClickJacking, sosyal mühendislik ve diğer benzer teknikler, hackerların büyük miktarlarda kişisel bilgilere erişme potansiyeli olan merkezi bir şirket veritabanlarındaki büyük ölçekli sızmalara kadar. Birincisi, çoğu durumda, güvenli tarama uygulamalarının bilinçli bir şekilde kullanılmasıyla engellenebilse de, etkilenen verilerin kapsamı ve gerçekliği nedeniyle, bizi en çok endişelendiren husus budur. Bu durumda, kişisel bilgilerimizin güvenliği tamamen kendi elimizde değildir.

11.Gizlilik

Son yirmi yılda, İnternetin günlük hayatımız üzerindeki etkisi nedeniyle, bir bireyin gizlilik hakkının güvenliği sorunu, fiziksel ortamımızdan dijital çevremize doğru genişlemiştir. Ünlü "Bilgi Güçtür", sözü günümüz dünyasında "Veri Güçtür" şekline dönüşmüş durumda, sadece kötü niyetli bilgisayar korsanları ile ilgili değil, biz kendimiz gönüllü olarak bireysel verilerimizi kendi elimizle şirketlere sunmaktayız.

Bir yandan kimliklerimiz, kredi kartı numaralarımız, dijital varlıklarımız vb. için hedef alınıyor, diğer yandan daha rahat bir kullanıcı deneyimi karşılığında bilgilerimizi veriyoruz. Kullanıcıları korumak için Avrupa Genel Veri Koruma Yönetmeliği (GDPR) gibi önlemler uygulanmasına rağmen, bunların etkileri ve yürütme seviyeleri hala çok fazla sorunu barındırmaktadır.

Zayıf ve verimsiz ülke yönetimleri, kullanıcılarının verilerini toplayan şirketler tarafından sunulan şüpheli uygulamalara izin vererek, bilgilerimizi bizden izinsiz ve ücretsiz kullanmalarına izin vermektedir. Bu Whitepaper'ın Veri İhlalleri bölümündeki en son gizlilik olaylarından bazılarından bahsetmiştik. Bu ve benzeri olayların ne yazık ki uygun tepkiler ve daha geniş halkın tepkisi olmadan unutulmaya mahkum olduğu görülüyor veya bazen kişilerarası iletişimimize zarar veren bir paranoya ve güvensizlik atmosferi yaratmaktadır. Bu nedenle, gizlilik haklarımızın farkında olmamız şart ve zorunlu zincirleme sorunlarına çözüm olarak blockchain gibi yeni fikirlerimiz var. Blockchain, kullanıcıların kişisel veri dağıtım araçlarını tam olarak kontrol etmeleri için gereken araçları sağlamaktadır. Bu verileri korumak için daha yüksek derecelerde anonimlik (bazıları tamamen anonimlik bile sağlar) ve farklı şifreleme yöntemlerinin kullanılmasına izin verir. Korunmasız merkezi veritabanlarından kurtulur ve veri çalınması ve manipülasyonuna karşı bağışıklık kazanır. Nihayetinde, kendisini dünyanın önde gelen işletmelerinin sergilediği acımasız nakit kapma davranışı nedeniyle kaybedilen güveni yeniden kurma potansiyeli olan bir platform olarak sunuyor.

12.Merkezi Mesajlaşma Uygulamaları

Nasıl çalışıyorlar ve ne gibi sorunlar getiriyorlar?

İnternetin günlük yaşamımızdaki varlığı arttıkça, daha verimli, daha yaygın çevrimiçi iletişim araçlarına ihtiyaç duyuldu. Takip eden yıllar, özel mesajlar, çok kullanıcılı gruplar ve dosya paylaşımı dahil olmak üzere daha gelişmiş özellikler içermeye başlanan AIM, ICQ ve PowW gibi popüler mesajlaşma uygulamalarının ortaya çıkmasını sağlamıştır.

Son zamanlarda, mesajlaşma uygulamalarının popülaritesindeki artış, akıllı telefon kullanımındaki artışla doğrudan ilişkilidir. Masaüstü uygulamaları, hareket halindeyken ve anlık iletişim kurmayı sağlayan mobil uygulamalar ile yer değiştirdi. Kullanıcı tabanı, katlanarak büyüdü; WhatsApp, Facebook, Messenger ve WeChat gibi uygulamalar, ayda 1 milyardan fazla aktif kullanıcıyı bir araya getirdi.

Ancak günümüzdeki mesajlaşma sistemleri kusursuz olmaktan uzaktır. Son olaylar, gizlilik sorunları hakkında ciddi durumları gözler önüne serdi. Facebook (en popüler iki mesajlaşma platformunun sahibi), siyasi amaçlarla kullanım için kullanıcı verilerini satma iddiasıyla karşılaştı ve Blockchain alanındaki en popüler mesajlaşma uygulaması olan Telegram, kullanıcılarının verilerini "ilgili makamlara vermeyi kabul etti(mahkeme emri olursa). Bu, doğrudan mevcut mesajlaşma uygulamalarının merkezi mimarisi ile ilgili bir konudur. Bu tür bir mimari, uygulama sahiplerinin içeriği potansiyel olarak ciddi gizlilik ihlallerine karşı savunmasız bırakarak içeriği kullanmalarını, yönetmelerini ve kısıtlamalarına sebep olur.

Günümüzdeki mesajlaşma uygulamaları, uçtan uca şifreleme çözümleri uygulayarak bu sorunu çözmeye çalışıyorlar, ancak yine de, bu uygulamaların, şifreleme kalitesi ve gerçekliği hakkında sorunları devam etmektedir. Bugünün mesajlaşma uygulamalarının bir diğer zayıf yanı, SIM swap(takas) saldırılarına karşı güvenlik açığı olmasıdır. Çoğu uygulama kaydolmak için bir telefon numarası gerektirdiğinden, bilgisayar korsanları, kuryeyi, kurbanın numarasını kendi sahip oldukları bir SIM karta dönüştürmeye ikna ederek kullanıcının mesajlaşma içeriğine erişme potansiyeline sahiptir.

13.Merkezi Bulutlar(Clouds)

Nasıl çalışıyorlar ve ne gibi sorunlar getiriyorlar?

Merkezi Clouds, uzaktaki sunuculara veri depolamayı ve bu verilere internet üzerinden erişmeyi sağlayan servislerdir. Ya kullanımı ücretsizdir ya da genellikle sözleşmenin uzunluğuna ve depolama kapasitesine dayanan aylık bir ücret talep ederler. Merkezi Clouds, kullanıcıya bir web arayüzü aracılığıyla bağlanabilen sanallaştırılmış veri merkezlerini kullanarak çalışır. Kullanıcı, dosyalarını internet üzerinden yükleyerek veri sunucularına kaydeder.

Kullanıcılara, yalnızca kullanıcının dosyaları görüntülemesine, düzenlemesine, aktarmasına veya senkronize etmesine izin veren meta veri derlemesini tetikleyen benzersiz bir kimlik sağlayarak erişilebilir. Kesintisiz veri alımı ve bütünlüğü sağlamak için dosyalar birden fazla sunucuda saklanmalıdır. Farklı türlerde merkezi bulut depoları vardır:

Genel Bulut Depolama - müşterinin yalnızca kullanılan kaynaklar için ücretlendirildiği ve hizmet sağlayıcısının bulut altyapısı bakımından sorumlu olduğu ortak bir kaynak ortamıdır. *Özel Bulut Depolama* - genellikle tek bir müşteri / kuruluş tarafından kullanılan ve servis sağlayıcı tarafından sağlanan şirket içi bir hizmettir. *Hibrit Bulut Depolama* - hassas ve genel olarak erişilebilir bilgilerin farklı bulut türlerinde saklanma esnekliğini sağlayan genel ve özel bulut depolama kombinasyonudur. Merkezi bulutların neden son zamanlarda popülerlik kazandığı açıktır.

Veri taşıması ve erişilebilirliğe yönelik artan talep, kullanıcıların HDD'ler ve USB flash sürücüler gibi fiziksel rakiplerinden geçiş yapmalarına neden oluyor. Bununla birlikte, doğru yönde atılmış bir adım olmasına rağmen, merkezileştirilmiş hizmetlerin hala sorunları vardır. Öncelikle, müşteri veri sahibi değildir.

Merkezi sunucu mimarisi, kullanıcının verilerini servis sağlayıcıların ellerine verir ve ayrıca veri erişim kesmelerini ve veri erişiminin sürekliliğini kesintiye uğratan DDoS saldırılarına karşı savunmasız kılar. Genel Bulut hizmetleri, özellikle bulutun istemcilerinden biri aracılığıyla kötü niyetli izinsiz girişlere izin veren kaynak paylaşım bileşenleri nedeniyle ortaya çıkar.

Yasalar ve düzenlemeler bir başka önemli endişe kaynağıdır; veri güvenliği ve gizliliği, dünyanın farklı hükümetlerinin belirlediği sürekli değişen kurallara bağımlıdır. Bulut üzerinde karmaşık veriler kullanmak isteyen daha küçük kuruluşlar için, büyük bant genişliği gereksinimlerinin finansal olarak uygun olmadığı kanıtlanabileceğinden maliyet ciddi bir sorun olabilir.

14.Zentachain'in Vizyonu

Zentachain bu sorunlara uygulanabilir çözümler sunar. Açık kaynak, merkezi sunucularda depolanmayan içerik ve daha fazla güvenlik için MeshNet gibi teknolojilerin entegrasyonu, bu platformda geliştirilen uygulamaları kullanmanın faydalarını açıkça göstermektedir. Kullanıcıların verilerini tamamen güvenli bir veri koruma ekosistemi ile, ihlallere ve her türlü siber saldırılara karşı korumak için sabırsızlanıyoruz!

Zentachain ekibi müşterilerini daha kalıcı hale getirmek için en yeni en sen teknolojileri geliştirmektedir. Bugün insanların kullandıkları her hizmetin, perakendeciler ve kuruluşlar , hedeflenen tüketici reklamları için bilgi almak amacı ile gizli bir bilgi kaynağı olduğu anlaşılıyor. ZentaChain'in amacı, insanlara ve şirketlere, gizli dinleme, casusluk veya veri toplama korkusu olmadan, güvende kalmalarını sağlamaktır. Zentachain, müşterilerimizin gili verilerini tutmayacağına söz verir ve IP adresinizi, e-postanızı veya telefon numaranızı kaydetmez. Yüklenen cüzdan uygulamamız ve Zentachain (Zenta) tokenlerimiz hariç, servis kullanımı için hiçbir şey gerekmeyecektir. Tüm hizmetlerimizde olduğu gibi, Zentachain kimliğiniz, hangi bölgede yaşadığınız veya hakkınızdaki kişisel bilgileriniz hakkında hiçbir kayda sahip olmayacaktır. Zentachain bu kişisel etkileri umursamıyor çünkü tek amacımız tüketiciye mutlak anonimlik, güvenlik ve mahremiyet sağlayacak dünya standartlarında hizmetler sunmaktır.

15.Zentachain Ekosistemi ve Zentacore

Zentacore, Ethereum blockchain'in ölçeklenebilirliğini ve işlem hızlarını büyük ölçüde iyileştirmek için sharding kullanacaktır. Keskinleştirme fonksiyonlarını anlamanın en kolay yolu, yatay veritabanı bölümlemesi ile paralellikler çizmektir. Milyonlarca kayıt içeren geniş bir veritabanına sahip olduğunuzu ve yalnızca belirli bir özellik içerenleri aramaya çalıştığınızı hayal edin. Teknik açıdan bakıldığında bu, yürütülmesi için önemli miktarda zaman alan bir görevdir. Ancak, veritabanını özelliklerine göre tablolara bölersek, arama süresini kısaltır, çünkü bu durumda sadece tek bir tablo sorgulanır.

Parçalama(Sharding) çözümü tüm Zentachain ekosistemi ile bağlantılıdır ve tüm blok zincirinin düğümler (bölümler) içinde bölünmesine ve depolanmasına olanak tanır, daha sonra blok zincirindeki her bir işlemi işlemesi gereken her bir düğümün tersine, yalnızca içinde bulunan işlemleri doğrulamaktan sorumludur. Her bir parça, bir işlem işlenmeden önce ve sonra parça ve durumu hakkında bilgi içeren derlemeler oluşturma görevini üstlenen görevliler olarak adlandırılan düğümleri içerir. Collation'lar süper düğümler tarafından toplanır ve eğer geçerli(tüm karşılaştırma işlemleri ve karşılaştırma durumları geçerli olmalı ve tüm karşılaştırıcıların ⅔' si tarafından imzalanmalıdır) bulunursa ayrı ayrı bloklara yerleştirilir ve blok zincirine eklenir. Zentacore, sharding kullanarak, kullanıcılara tüm Zentachain ürünlerinde kesintisiz ve gecikmesiz bir deneyim sunmak için temel bir ekosistem bileşeni haline gelir.

Akıllı Sözleşmeler / HTTP

Zentacore, Ethereum blockchain-Akıllı Sözleşmelerin bir diğer önemli özelliğini kullanmaktadır. Bu dijital sözleşmeler, ZentaChain'in dApp'lerini çalıştırmak ve ağı sürdürmek için gerekli işlemleri güvenli ve otomatik hale getirir; görevler ve komutlar, hız, hassasiyet ve tutarlılık ile kusursuz bir şekilde yürütülmektedir. Diğer akıllı sözleşmelerle etkileşime girebilir ve geliştirici tarafından tanımlanır. Bu sözleşmeler yapılırsa asla değiştirilemez, kurallar kesinleşir ve tahrif edilmeyi imkansız hale getirir. Bu, güvenli ve tutarlı bir Zentachain ekosistemine olanak sağlar.

HTTP'nin verimsizlik, geçmiş sürümü olmaması ve merkezileşme gibi birçok dezavantajı vardır. Böylece IPFS, HTTP'nin dezavantajlarının üstesinden gelir. Zentachain, bilimsel araştırma kayıtlarının blok zinciri teknolojisi, IPFS ve Zentachain akıllı sözleşmeleri kullanılarak güvenli ve hack olaylarına dayanıklı bir ortamda yapılabileceği bir çerçeve sunmaktadır. Proje raporları, mutabakat zaptı, proje finansmanı belgeleri, katılım kayıtları ve toplantı tutanakları gibi belgelerin saklanması için, belirli erişim kontrol yöntemleri ile birlikte, ağdaki tüm katılımcı düğümlerin tüm önemli bilgilere ulaşması için bulunması gerekmediğinden, IPFS ve Zentacore kullanılır. Gizli paylaşım ve asimetrik anahtar şifreleme sistemi gibi yöntemler sistemde erişim yapısını yalnızca sistemin belirli kullanıcılarına sınırlamak için ek işlevsellik olarak uygulanabilir. Zentavalut'ta saklanan belgelerin kaynak meta veri bilgileri, bilgilerin bütünlüğünü sağlamak için blok zincirine yüklenir. Baş Araştırmacı (PI), bu belgelere yalnızca bu zincir bilgisini blok zincirinde kullanarak erişim izni olan kullanıcılar tarafından erişilmesini ve değiştirilmesini sağlayabilir.

16.Zentachain Akıllı Sözleşmeler ve IPFS

Proje raporları, proje finansman detayları, mutabakat zaptı, katılım kayıtları ve toplantı tutanakları gibi belgeler IPFS ve Zenta'da şifrelenir ve saklanır. IPFS, her bir belgenin benzersiz bir hash yaratan dağıtılmış bir dosya sistemidir ve ağdaki diğer düğümler, yalnızca dosyanın tek hash şifresi biliniyorsa dosyalara erişebilir ve bunları görüntüleyebilir. Ağdaki belirli düğümlere erişimi kısıtlamak için, belirli erişim kontrol yöntemleri uygulanabilir.

Akıllı sözleşmeler C ++, javascript ve Python gibi kodlama dillerinden etkilenen Solidity adlı yüksek seviyede bir kodlama dilinde yazılmıştır. Ethereum akıllı sözleşmeleri geliştirmek için tarayıcı tabanlı bir IDE olan Remix IDE kullanılabilir. Bir diğeri, yerleşik akıllı sözleşme derleme, bağlama, dağıtım ve ikili yönetimi destekleyen Truffle sistemidir. İki erişim kontrolü yöntemi uygulanabilir: Erişimi kısıtlamanın bir yolu, Sha256 / AES / GnuPG üzerinden asimetrik şifreleme düzenini uygulamaktır. Bu şemada, yalnızca anahtarı olan kullanıcılar belgenin şifresini çözebilir. Diğerleri belgenin veya verilerin şifresini çözemez.

Dokümanın bağlantısı kullanıcılara sağlanmış olsa bile, kullanıcılar dokümanın şifresini yalnızca anahtarı bulunduğunda çözebilirler. Bu yüzden önerilen sistemde, bu özel gizli anahtara ana anahtar denir. Bu ana anahtar, sisteme kaydolurken sisteme erişmesine izin verilen kullanıcılara verilir. Bu ana anahtarı hem PI hem de JRF kullanarak IPFS dosya sistemine erişebilirsiniz. Bu nedenle, tüm dosyalara sisteme yalnızca kayıtlı kullanıcılar erişilebilir durumdadır. Kullanıcı Zentavalut'a giriş yapabilir ve dosyaya erişebilir, indirebilir, şifresini çözebilir ve ardından görüntüleyebilir. Ancak, burada önemli bir kısıtlama uygulanmaktadır. Yalnızca PI, IPFS ağına belge yükleyebilir ve oluşturabilir. IPFS ağına yeni belgeler yüklemek ve oluşturmak JRF için sınırlandırılmıştır. JRF'nin IPFS'den belirli bir belgeye erişmek istediği ilk senaryoyu düşünün. Bu durumda, JRF belgenin linkini alabildiğinden, indirebildiğinden ve ana anahtarı kullanarak belgenin şifresini çözebildiğinden ve sonra belgeyi görüntüleyebildiği için bir problem yoktur. JRF, indirilen belgeyi değiştirmek ya da silmek gibi her şeyi yapabilir. Ancak tüm bu işlemler yalnızca JRF'nin indirilen belgesinin yerel kopyasında etkilenecektir. IPFS'deki orijinal belge değişmeden kalır.

Türetilmiş anahtar, genellikle parola tabanlı anahtar türetme işlevi kullanılarak bir paroladan türetilir. Bir anahtar türetme işlevi (KDF), bir veya daha fazla gizli anahtarı bir Sözde Rastgele İşlev (PRF) kullanan bir şifre veya ana anahtar gibi başka bir gizli değerden türeten bir işlevdir. Birçok modern tabanlı anahtar türetme işlevi vardır. Bu asıl veriler daha sonraki denetim amaçları için çok gereklidir. IPFS dosya sisteminin günlükleri, saklanan dokümanların asıl verilerini toplamak için kullanılabilir. Bu provenans veri bilgisi, aynı zamanda Ethereum blockchain içerisine gömülebilir ve Solidity Programlama Dili, Truffle ve Remix IDE Algoritması kullanılarak yapılan akıllı sözleşmeler ile yapılan işlemler, akıllı sözleşmeleri kullanarak blok zincirinde saklanan IPFS'den bir dosya almak için akıllı sözleşmenin anahtarını sunar.

1)Automatically AES Key Encryption 256-bit on Zentavalut over APIs

Encrypt: 1) FileEncrypt(F) → (CTF ,K, kw): DO selects a keyword set kw from the file F, randomly selects AES key K from the key space, computes CTF = EncK (F), where EncK (F) denotes using AES algorithm to encrypt F, the encryption key is K. DO uploads the ciphertext CTF to IPFS, records the file location hlocation returned by IPFS. 2) KeyEncrypt(PK,K, hlocation,P) → CTmd : DO computes CTI = EncK (hlocation). In order to encrypt the AES key K under the access policy P, DO computes where <bXi,bYi> = <Xi.ki , Yi,ki>, IP is a subscript set of P. Then, DO randomly selects sRZ p , computes CTK = <P,C0,C1,C2>, where C0 = K · Y s P , C1 = g s , C2 = X s P . DO randomly selects AES key K1, computes CTmd = EncK1 (CTK ,CTI), embeds CTmd into transaction TXct , and broadcasts TXct to the Zenta blockchain. when transaction has been approved, record the transaction id txid and corresponding key K1. The length of txid and K1.

Decryption by AES Privat Key 256-bit on Zentavalut over APIs

(CTI,CTk , SKd , PK) → F: DU computes d = F(kwf||1,Ks), computes txidj = d ⊕ txid gj , K1j = d ⊕ Kf1j for txid gj Stxid , Kf1j Sk1. DU reads transaction txidj data from the Ethereum blockchain, and computes (CTK ,CTI) = DecK1j (CTmd), where DecK1j (CTmd) denotes using AES algorithm to decrypt CTmd , the decryption key is K1j . DU first checks whether his attributes set S PP, and if not, returns ⊥ and reads the next transaction data; otherwise, computes σ P = Q i I P b σ i , then AES key K is recovered as computes

$$\text{where } b\sigma i = \sigma i,ki = g\ H0(y||i||ki)H1(sk)\ H0(x||i||ki)$$

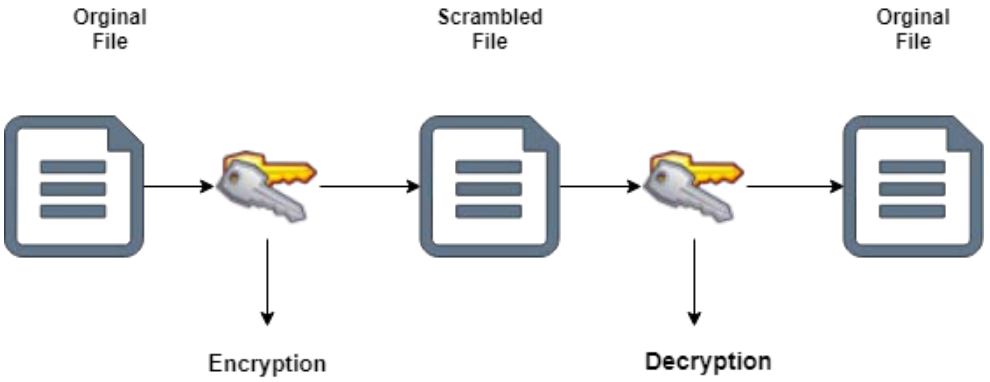
DU computes hlocation = DecK (CTI), then downloads CTF from IPFS based on hlocation, computes F = DecK (CTF) to recovery original file F.

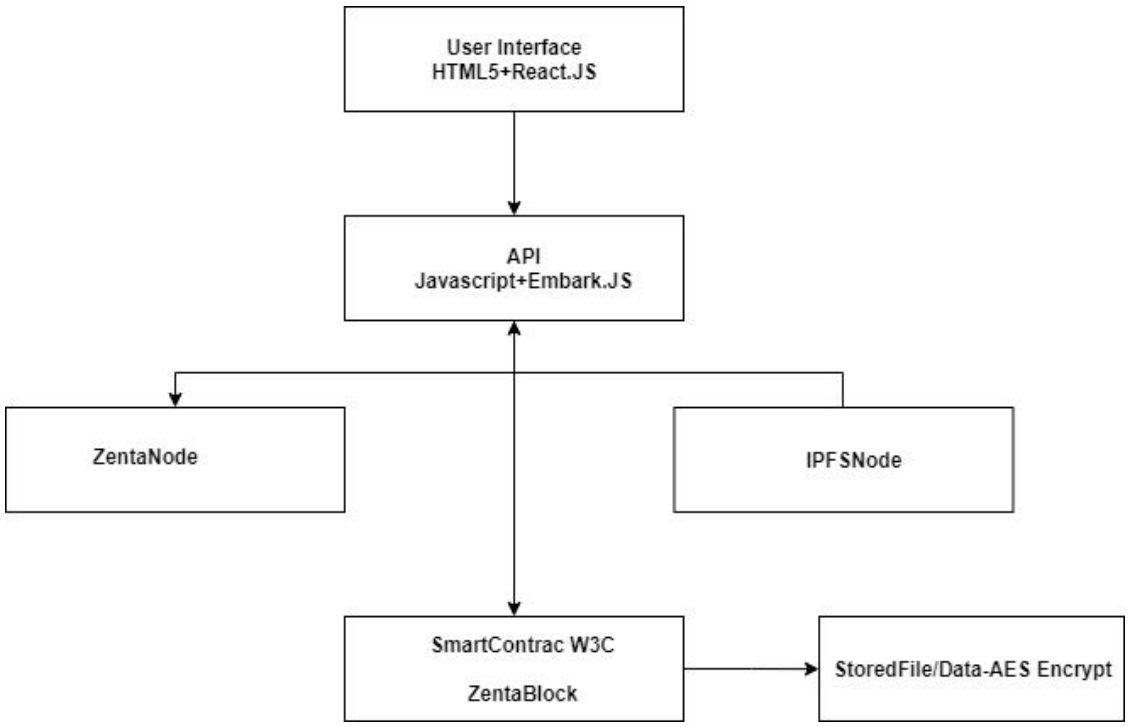
Simetrik ve Asimetrik Şifreleme Algoritmalarını Uygulama

Simetrik ve asimetrik algoritmalar arasındaki fark performans ve boyuttur. Simetrik şifreleme daha hızlıdır ve büyük bir veri kümesini şifrelemek için kullanılır. Asimetrik küçük mesajları şifrelemek için çok uygundur. Ancak bu iki stratejiyi kullanmak Zentavalut uygulamasında sağlam bir güvenlik sistemi uygulamanıza yol açar.

Simetrik-Anahtar Şifreleme

Simetrik anahtar şifrelemesinde şifreleme anahtarı şifre çözme anahtarından hesaplanabilir ve bunun tersi de geçerlidir. Çoğu simetrik algoritma ile aynı anahtar hem şifreleme hem de şifre çözme için kullanılır.





2.)Zentachain Web Kriptografi API

Zentachain JavaScript API hash, imza oluşturma ve doğrulama, şifreleme ve şifre çözme gibi web uygulamalarında temel şifreleme işlemlerini gerçekleştirmek içindir. Bu işlemleri gerçekleştirmek için gerekli olan anahtarlama malzemesini oluşturma ve / veya yönetme uygulamaları için API kullanılır.

Bu API için kullanılanlar, kullanıcı veya hizmet kimlik doğrulaması, belge veya kod imzalama ve iletişimin gizliliği ve bütünlüğü arasındadır. Zentachain Web Şifreleme API'si, kullanıcı aracıları tarafından yönetilen veya maruz bırakılan şifreleme anahtar malzemesiyle etkileşime geçmek için düşük düzeyli bir arabirim tanımlar. Şifreleme dönüşümleri, genel şifreleme işlemlerini gerçekleştirmek için bir dizi yöntem tanımlayan SubtleCrypto arabirimi aracılığıyla ortaya çıkar.

İmza oluşturma - doğrulama, hash ve doğrulama , şifreleme ve şifre çözme gibi işlemlere ek olarak API, anahtar oluşturma, anahtar türetme ve anahtar alma ve verme işlemlerine ilişkin arabirimler sağlar. Bir web uygulaması, kullanıcıların yüklemeden önce uzak servis sağlayıcılarla saklanan verilerin ve belgelerin gizliliğini korumalarına izin vermek isteyebilir. Şifreleme Zentachain API, uygulamanın bir kullanıcının özel veya gizli bir anahtarı seçmesine, isteğe bağlı olarak seçilen anahtardan bir şifreleme anahtarı almasına, belgeyi şifrelemesine ve şifreli verileri mevcut API'leri kullanarak servis sağlayıcısına yüklemesine izin verebilir. Bu kullanım durumu, Korunan Doküman Değişimi kullanım durumuna benzer, dokümanın görüntülenmesi kullanıcının kendisi ile sınırlıdır.

Bunun yerine, CryptoKey'in yapılandırılmış klon algoritmasıyla kullanılmasına izin vererek, yapılandırılmış klonlanabilir nesnelerin depolanmasını destekleyen mevcut veya gelecekteki herhangi bir web depolama mekanizması CryptoKey nesnelerini depolamak için kullanılabilir.

Uygulamada, çoğu yetkilinin, anahtarın uygulama için anlamlı olan dize tanımlayıcısı olduğu ve değerin bir CryptoKey nesnesi olduğu anahtar / değer çiftlerinin ilişkisel olarak depolanmasını sağlayan Dizine Alınmış Veri Tabanı API'sini kullanması beklenir. Bu, ana materyali uygulamaya veya JavaScript ortamına bırakmadan, ana materyalin depolanmasına ve alınmasına olanak sağlar. Ek olarak, CryptoKey'in kendisiyle birlikte herhangi bir ek meta veriyi saklamak için tam esneklik sağlar.

CryptoKey arayüz Zentachain (Örnek)

```
enum KeyType { "public", "private", "secret" };

enum KeyUsage { "encrypt", "decrypt", "sign", "verify", "deriveKey", "deriveBits",
"wrapKey", "unwrapKey" };

[SecureContext,Exposed=(Window,Worker)]
interface CryptoKey {

  readonly attribute KeyType type;   readonly
attribute boolean extractable;   readonly
attribute object algorithm;   readonly attribute
object usages;

};
```

KeyAlgorithm sözlüğü

KeyAlgorithm sözlüğü, bir CryptoKey'in ortak özelliklerinin bir uygulamaya nasıl yansıtıldığını belgelemeye yardımcı olmak için sağlanmıştır. Asıl sözlük türü uygulamalara asla maruz kalmaz.

```
dictionary KeyAlgorithm {
  required DOMString name;
};
```

KeyType : Anahtar Tipi

Tanınan anahtar tipi değerleri "public", "private" ve "secret" dır. Simetrik algoritmalar için kullanılanlar da dahil olmak üzere opak anahtarlama materyali "secret " ile temsil edilirken, kamusal / özel anahtarlıklardan oluşan asimetrik algoritmaların bir parçası olarak kullanılan anahtarlar "public" veya "private" olacaktır. KeyUsage; Bir anahtar kullanılarak gerçekleştirilebilecek bir işlem türüdür. Tanınan anahtar kullanım değerleri : **"encrypt", "decrypt", "sign", "verify", "deriveKey", "deriveBits", "wrapKey" and "unwrapKey".**

Simetrik Şifreleme (JavaScript Örnek)

```
var encoder = new TextEncoder('utf-8');
var clearDataArrayBufferView = encoder.encode("Plain Text Data");

var aesAlgorithmKeyGen = {
  name: "AES-CBC",
  // AesKeyGenParams
  length: 128
};

var aesAlgorithmEncrypt = {
  name: "AES-CBC",
  // AesCbcParams
  iv: window.crypto.getRandomValues(new Uint8Array(16))
};

// Create a key generator to produce a one-time-use AES key to encrypt some data
window.crypto.subtle.generateKey(aesAlgorithmKeyGen, false, ["encrypt"]).then(
  function(aesKey) {
    return window.crypto.subtle.encrypt(aesAlgorithmEncrypt, aesKey,
[ clearDataArrayBufferView ]);
  }
).then(console.log.bind(console, "The ciphertext is: "),
       console.error.bind(console, "Unable to encrypt"));
```

Bir imzalama anahtarı çifti oluşturun(JavaScript Örnek)

```
var encoder = new TextEncoder('utf-8');

// Algorithm Object
var algorithmKeyGen = {
  name: "RSASSA-PKCS1-v1_5",
  // RsaHashedKeyGenParams
  modulusLength: 2048,
  publicExponent: new Uint8Array([0x01, 0x00, 0x01]),  // Equivalent to 65537   hash: {
    name: "SHA-256"
  }
};
var algorithmSign = {
  name: "RSASSA-PKCS1-v1_5"
};
window.crypto.subtle.generateKey(algorithmKeyGen, false, ["sign"]).then(
  function(key) {
    var dataPart1 = encoder.encode("hello,");
    var dataPart2 = encoder.encode(" world!");
    return window.crypto.subtle.sign(algorithmSign, key.privateKey, [dataPart1,
dataPart2]);   },
  console.error.bind(console, "Unable to generate a key")
).then(
  console.log.bind(console, "The signature is: "),
  console.error.bind(console, "Unable to sign")
);
```

17.Sharding (Zentashard)

Ethereum'daki ölçeklenebilirlik talebi giderek acil hale gelmektedir. Cryptokitties olayı, Ethereum ağının ne kadar çabuk tıkanma-aksama olabileceğini gösterdi. Zentachain, yüksek TPS kurmak için, gelecekteki altyapı kanıtı , Sharding kullanacaktır. ZentaChain'in neden Sharding kullandığını anlamak: Bir blok zincirinin en büyük sorunlarından biri, düğüm sayısındaki artışın ölçeklenebilirliğini azaltmasıdır. Bu durum daha sezgisel görünebilir çünkü daha fazla düğüm daha fazla güç veya daha fazla hıza neden olmaz, bunun tersi doğrudur: Bir Blockchainin güvenli olmasının nedenlerinden biri herbir düğümün herbir işlemi işlemesi gerekir. Bu, raporunuzu şirketteki her muhasebeci tarafından kontrol ettirmek gibidir. Bu, raporunuzun hatasız olmasını sağlayabilir, ancak geri dönüp nihayet onaylanmanız da uzun zaman alacaktır. Ethereum da benzer bir sorunla karşı karşıya. Düğümler sizin muhasebeciniz, her işlem sizin raporunuz.

Bu problem nasıl çözülür?

Zentachain, hızdan memnun kalana kadar düğüm sayısını (sayaç) azaltabilir. Ancak, atama (işlem) bekleme listesi arttıkça, muhasebeci sayısını daha da azaltmamız gerekecek. Bu sonuçta bize birkaç "güvenilir" muhasebeciye güvenmemizi sağlayacaktır. Merkezi bir grup. Bu, blockchain merkeziyetsizliği ideolojisine karşı. Tüm şirketten (tüm ağ) daha küçük bir düğüm grubunu ele geçirmek / bozmak çok daha kolaydır.

"Sharding" Nedir?

Raporlarınızı (işlemlerinizi) geri döndürme hızını artıracak kadar küçük olmakla birlikte, güvenliği korumak için yeterli sayıda düğüme sahip bir sisteme sahip miyiz? Temel olarak, özelliklerin üçünde de “maksimize edemediğimizi” söylüyoruz: Ölçeklenebilirlik, Güvenlik, Merkeziyetsizleşme.

Daha fazla ölçeklenebilirlik elde etmek için “yeterli” merkeziyetsizlik ve güvenliğe sahip olabilir miyiz?

Küresel finansal sistemimiz değişime dirençli, başarısızlığa ve saldırılara karşı savunmasız ve temel finansal araçlara ihtiyaç duyan milyarlarca insana erişilememesi için oldukça merkezi bir konumdadır. Öte yandan, merkeziyetsizlik, bir grup karşılıklı güvensiz katılımcı arasında tutarlı bir görüşün sağlanmasında yeni zorluklar ortaya koymaktadır. Açık üyeliğe izin veren ve merkeziyetsiz sistemin katılımcılarının sürekli hareketini gerektiren (yani, katılma / ayrılma) izinsiz çalışma şekli bu görevi daha da zorlaştırmaktadır. Ayrıca, merkezi olmayan bir sistem de dahil olmak üzere herhangi bir sağlam finansal sistemin gerçekçi piyasa yüklerine yeteri kadar hizmet edebilmesi gerekir. Bu, çok sayıda katılımcıya kolayca ölçeklenmesi gerektiğini ve çıktılarını kullanılabilir kılmak için nispeten düşük gecikmelerle yüksek bir işlem hacmini ele alması gerektiği anlamına gelir. Bu özelliklerin bir arada elde edilmesi aynı zamanda katılımcıların her birinden önemli kaynaklar gerektirmemelidir, aksi takdirde herkes tarafından kolayca erişilebilir bir araç oluşturma fikrine aykırıdır.

Sharding, “Ağı daha küçük gruplara ve parçalara ayıralım” demenin güzel bir yolu. Her grup bir parçadır. Bir parça düğümlerden ve işlemlerden oluşur. Yani bizim muhasebeci analojimizde, bir grup muhasebeci ve görev grubundan oluşacaktır. Şimdi, ağın tamamındaki raporları kontrol etmek zorunda olan bir muhasebeci , yalnızca kendi grubundaki (grup) görevlendirmelerden sorumlu olacaktır. Bu, her düğümün (muhasebecinin) onaylaması gereken işlem sayısını büyük ölçüde azaltır.

Bugün Bitcoin Ölçeklenebilirliği: Gerçeklik Kontrolü, Bitcoin sisteminin bazı temel ölçümlerini bugün olduğu gibi analiz ediyoruz. Maksimum verim. Maksimum verimlilik, blok zincirinin işlemlerini onaylayabildiği maksimum orandır. Bugün, Bitcoin'in maksimum verimi 3,3–7 işlem / sn'dir. Bu sayı, maksimum blok boyutu ve bloklar arası süre ile sınırlıdır. Gecikme. Bir işlemin onaylanma zamanı. Bir bloğa dahil edildiğinde, kabaca 10 dakika içinde bir işlemin onaylandığı kabul edilir.

Bitcoin blok zinciri gibi bazı blok zincirler halka açıktır; Bu, herkesin ekipman satın alabileceği, ağa bağlanabileceği ve "madenciliği" başlatabileceği anlamına gelir. Ancak diğerleri, konsensüs sürecindeki katılımcıların, kurucu çekirdek geliştiricileri tarafından önceden belirlenmiş bazı gereksinimleri yerine getirmelerini gerektirir.

- Proof-of-Work: Orijinal blok zinciri olan Bitcoin blok zinciri, işlemleri onaylamak ve yeni bloklar oluşturmak için İş Kanıtı (PoW) adlı bir prosedür kullanır. PoW başlangıçta bir hizmet ağında dağıtılmış hizmet reddi saldırılarını (DDoS) ve spam gibi diğer hizmet suistimallerini engellemek için ekonomik bir önlem olarak tasarlandı. Bunu, genellikle bir bilgisayar tarafından işlem yapılmasını gerektiren hizmet istekçisinden bazı "işlerin" yapılmasını talep ederek başarır. Örneğin, Bitcoin blok zincirinde "iş" geçerli bir çift SHA256 hash(karma) hesaplamaktır. Hizmet isteğinin yerine getirmek zorunda olduğu "iş", sahte veya etik olmayan davranışlarda bulunmanın fırsat maliyetini artıran, işlem gücü gibi sermaye yoğun kaynakların harcanmasını gerektirir. Bu, veri güvenliği ile sermaye kaynakları arasında bir denge sağlar. Bu nedenle, iş ne çok zor ne de çok kolay olmamalıdır. Gereken iş çok zorsa, iş daha kolay olabileceği ve aynı sonuçları verebileceği için verimsizlik yaratır. Bununla birlikte, eğer gerekli iş çok kolay ise, sistem amacına hizmet etmekte başarısız olur, bu da kaynakların verimsiz kullanımıyla sonuçlanır. Halen, tüm kamuya açık blockchainler bir tür PoW(İş Kanıtı) doğrulamasına ve bir tür fikir birliği sürecine dayanmaktadır. Bununla birlikte, PoW ile ilgili temel sorun, inanılmaz derecede enerjisi yoğun bir süreç olmasıdır. Blok zincirinin korunmasında enerji gereksinimlerinin azaltılmasını amaçlayan birçok potansiyel çözüm ortaya konulmuştur. PoW için en umut verici çözüm, PoS(Proof os Stake) kavramıdır.

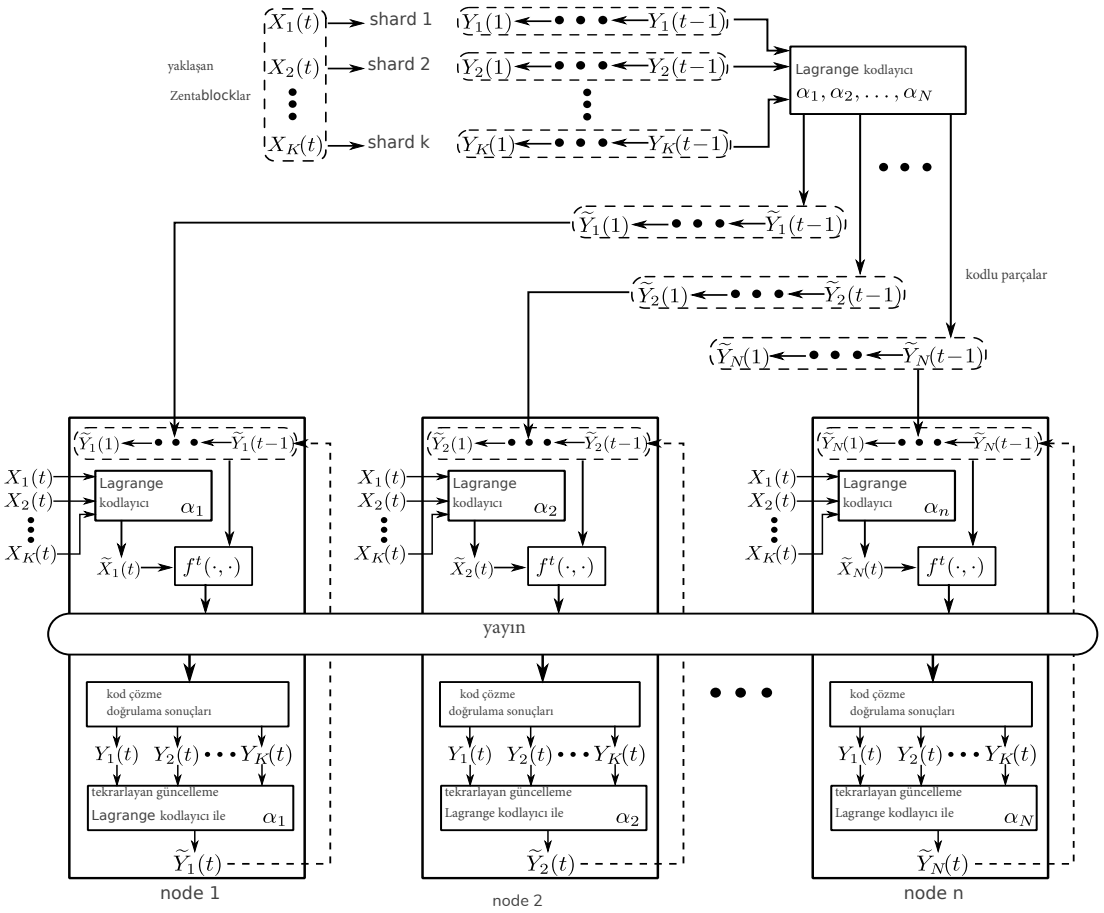
- Proof-of-Stake: Proof-of-Stake (PoS)Blockchain ağlarında dağıtılmış fikir birliği sağlamak için bir algoritmadır. İş Kanıtı(Proof of Stake), İş Kanıtı için potansiyel bir ikame olarak önerilmiştir ve işlem gücü ve enerjisi gibi sermaye kaynaklarının yetersiz kullanımı sorununu çözmeyi amaçlamaktadır. İş Kanıtının(PoS) temel fikri, bir üyenin ağda sahip olduğu "hisseye(stake)" bağlı olarak madencilik imtiyazlarını tahsis etmektir. Birçok farklı İş Kanıtı(PoS) versiyonları önerilmiştir ve optimal uygulamanın nasıl sağlanacağı konusunda görüşler farklı olsa da, temel prensip aynı kalmıştır. İş Kanıtının en basit hali, blockchain'in yerel dijital para biriminin mülkiyetine dayanan madencilik imtiyazlarını devretmektir. Madencilik imtiyazlarının sadece para sahipliğine değil, diğer faktörlere de bağlı olduğu, "İş Kanıtı" sisteminin birçok farklı sürümü önerilmiştir. Bu faktörler arasında işlem sıklığı ve üyenin ağdaki yer aldığı süre de vardır.

- Önceki çalışmaların ölçeklenebilirliğini ve güvenlik sınırlamalarını çeşitli yollarla geliştiren Bizans esnek bir halka blok zinciri protokolü olan ZentaChain'i öneriyoruz. Zentachain, yüksek düzeyde, düğüm kümesini, ayrık işlem bloklarına paralel olarak çalışan daha küçük düğüm gruplarına ayırır. İşlemlerin ve / veya verilerin çok sayıda düğüm grubu arasında bölüştürülmesi, genellikle, sharding olarak adlandırılır ve son zamanlarda blok zincir protokolleri bağlamında incelenmiştir.

- Konsensüs çalışmasının ve depolamanın paralelleştirilmesini sağlayarak, paylaşım temelli konsensüs, temel Satoshi Nakamoto konsensüsünün aksine sistemin verimini, komite sayısına orantılı olarak ölçeklendirebilir. Herhangi bir zamanda protokoldeki katılımcı sayısını n gösterelim ve m = n her ZentaChain'in yarattığı boyutu, m = c logn düğüm büyüklüğündeki c = n / m komitelerini oluşturur, c yalnızca güvenlik parametresine bağlı olan bir sabittir. Bitcoin'in aksine, Sharding-Tabanlı Konsensüs, birden fazla düğüm komitesinin gelen işlemleri paralel olarak işlemesini sağlayarak, ağa katılan katılımcı sayısı ile işlem işleme gücünü artırabilir. Bu nedenle, her konsensüs turunda protokolün tamamı tarafından işlenen toplam işlem sayısı, komite sayısı ile çarpılır. Bitcoin işlem modelinde sadece sharding işlemine odaklanan sonuçları araştırdığımız gibi, sharding tabanlı blockchain protokollerinde çok sayıda heyecan verici, paralel çalışma vardır.

Zentashard Yapısı

Her grupta, "Karşılaştırıcı"olarak atanan düğümlerimiz var. Karşılaştırıcı' lar işlemlerin küçük açıklamalarını ve parçanın mevcut durumunu toplamakla görevlendirilir. Analojimizde, Karşılaştırıcı' ları Muhasebe Asistanları olarak düşünebilirsiniz. Shard / grup içindeki tüm AA'lar, shard içindeki bütün ödevlerin ilk akışını yapar. Sonunda süper düğümlerimiz var. Her bir süper düğüm, her bir parçanın karşılaştırıcıları tarafından yaratılan karşılaştırmaları(collation) alır. Daha sonra bu karşılaştırmaların içindeki işlemleri işler. Dahası, aynı zamanda, karşılaştırıcılardan aldıkları tüm parçaların tam açıklama / durum verilerini de korurlar.



of decoding a Reed-Solomon code with dimension (K − 1)d+1 and length N (see, e.g., [38]). In order for this decoding to be robust to μN malicious nodes (i.e., achieving the security $\beta_{\text{Zentashard}}$ = μN), we must have μN ≤ (N −(K −1)d)/2. In
other words, a node can successfully decode $f^t(u_t(z), u^{t-1}(z))$ only if the number of shards K is upper bounded as $K \leq \frac{(1}{-2\mu)N} + 1$.

$$\tilde{Y}_i(t) = \sum^{K} \ell_{ik} z_k^t X_k(t) = \sum^{K} \ell_{ik} Y_k(t),$$

d

Alt zincirlerin güncellenmesi, O (NK) olan blok kodlama aşaması ile aynı hesaplama karmaşıklığına sahiptir.

Since the set of coefficients ℓ_{ik}s in are identical to those in appending a coded block to a coded sub-chain is equivalent to appending uncoded blocks to the uncoded sub-chains, and then encoding from the updated sub-chains. This commutativity between sub-chain growth and storage encoding allows each node to update its local sub-chain incrementally by accessing only the newly verified blocks instead of the entire block history.

The total number of operations during the verification and the storage update processes is O(NK) + Nc(f^t) + $O(N^2 \log^2 N \log\log N)$, where the term O(NK) + $O(N^2 \log^2 N \log\log N)$ is the additional coding overhead compared with the uncoded sharding scheme. Since $K_{\text{zentashard}} \leq N$, the coding overhead reduces to $O(N^2 \log^2 N \log\log N)$.

Zentashard'ın kodlama ve kod çözme işlemlerinin karmaşıklığı, kodlama ek yükü ile ölçeklenmediğinden, zincir büyüdükçe önemsiz hale geldiğini görüyoruz. Zentashard programı, eşzamanlı olarak güvenlik, depolama verimliliği ve verim üzerinde en iyi ölçeklendirmeyi sağlar.

SONUÇLAR

Zentashard, açıklanan ödeme blockchain sistemindeki Zentashards'ın performansını değerlendirmek için simülasyonları ayrıntılı olarak anlatmıştır. Bu sistem, müşteriler arasındaki tüm bakiye transferlerinin kayıtlarını tutar ve yeni blokları, doğrulama fonksiyonunu hesaplayan daha önce doğrulanmış blokların toplamıyla karşılaştırarak doğrular. Daha spesifik olarak, sistem, her biri M istemcilerini yöneten K parçaları içerir. Herbir zaman diliminde t, her blokta bir işlem bloğu sunulur. Sırasıyla tam çoğaltma, kodlanmamış sharding ve Zentashards şemalarını kullanarak bu sistemi N düğümleri üzerinden simüle ediyoruz. Her şemanın verimini, N ve t değerlerinde, ölçeklenebilirliğini anlamak için ölçüyoruz. Verim, zaman birimi başına doğrulanan blok sayısı olarak tanımlanır ve K (düğüm başına üretilen blok sayısını) N düğümlerinin ortalama doğrulama zamanına (ölçülecek) bölerek ölçülür. Zentashard için doğrulama süresi ayrıca her bir düğümün blokları kodlamak için harcadığı zamanı da içerir. Bununla birlikte, kodlama süresi sabit olduğu için, zincir uzadıkça denge toplamı t ile artarken, kodlama zamanının ihmal edilebilir hale gelmesi beklenmektedir. Her planın depolama verimliliğine ve güvenlik seviyesine sistem parametreleri tarafından karar verildiğini ve bu nedenle ölçümlere gerek olmadığını unutmayın. Bu sistemi t = 1000 devir için, farklı sayıdaki K parçaları kullanarak simüle ediyoruz. Her shard(parça) M = 2000 istemcisini yönetir. Oran: N / K = 3 . Böylece, düğümlerin sayısı N'dir. Şekil 3'teki üç planın N, t ve verim arasındaki tam ilişkisini çiziyoruz. Daha yakından bakmak için, Şekil 5'te N = 150 iken t ve verim arasındaki ilişkiyi ve Bölüm'de Şekil 2'de T = 1000 olduğunda N ile verim arasındaki ilişkiyi çizdik.

$$\text{Zentashard} = \liminf_{t\to\infty} \frac{K_{\text{Zentashard}} N c(f^t)}{N c(f^t) + O(N^2 \log^2 N \log\log N)}.$$

Farklı ağ boyutu N altındaki üç şemanın depolanması ve güvenliği.

Depolama verimliliği

N	15	30	60	90	120	200
γ_{full}	1	1	1	1	1	1
γ_{sharding}	5	10	20	30	40	60
zentashard	5	10	20	30	40	60

Güvenlik

N	15	30	60	90	120	200
β_{full}	7	15	30	45	60	100
β_{sharding}	1	1	1	1	1	1
zentashard	5	10	20	30	40	100

18.Zentalk

Zentalk, kullanıcıların şu anda mesajlaşma hizmetleri hakkındaki düşüncelerini tamamen değiştirmek için tasarlanmış, eşler arası(Peer to Peer) mesajlaşma servisidir.

Zentalk, hizmetin mevcut en güvenli ve özel mesajlaşma uygulaması olmayı hedefleyen Zentachain platformunda bulundurulacaktır.

Zentalk, Mesh Networking teknolojilerinin entegrasyonuyla gizlilik ve güvenliğini sağlar. Mesh Networking (MeshNet), mevcut en güvenli ve en güvenilir ağ(network) çeşitlerinden biridir. MeshNet teknolojisi güçlüdür, mükemmel yük dağılımına sahiptir ve merkezi yönetim içermez.

Bir ağ, her düğümün ağ için veri ilettiği bir ağ topolojisidir. Zentachain .cjdns-, adres tahsisi için ortak anahtar şifrelemesi ve yönlendirme için dağıtılmış bir hash(karma) tablo kullanarak şifreli bir IPv6 ağı uygular. Bu, sıfıra yakın yapılandırma ağı sağlar ve mevcut ağları saran güvenlik ve ölçeklenebilirlik sorunlarının çoğunu önler. Tüm ağ düğümleri ağdaki verilerin dağıtımında işbirliği yapar. Zentalk kullanan cihazlar, MeshNet'te düğüm görevi görür. Bu düğümler, birbirleriyle dağıtılmış bir şekilde birbirleriyle bağlantı kurma özelliğine sahiptir.

Mesh ağları, bir sel tekniği veya bir yönlendirme tekniği kullanarak mesajları iletebilir. Yönlendirme ile mesaj, bir noktadan hedefine ulaşana kadar düğümden düğüme atlayarak bir yol boyunca yayılır. Tüm yollarının kullanılabilirliğini sağlamak için, ağ sürekli bağlantılara izin vermeli ve Kısa Yol Köprüleme gibi kendi kendini iyileştiren algoritmalar kullanarak kendini bozuk yollarda yeniden yapılandırmalıdır. Kendi kendini iyileştirme, bir düğüm bozulduğunda veya bir bağlantı güvenilir olmadığında yönlendirme tabanlı bir ağın çalışmasına izin verir. Sonuç olarak, ağ bir kaynak ve bir hedef arasında genellikle birden fazla yol olduğundan, ağ oldukça güvenilirdir. Çoğunlukla kablosuz durumlarda kullanılsa da, bu kavram kablolu ağlar ve yazılım etkileşimi için de geçerli olabilir.

Gündelik hayatta kullanılan ortak ağ teknolojisi bir örneği kablosuz domotika (Z-dalga protokolü gibi) olacaktır. Evde yeni bir düğüm kaydettiğinizde, yeni bir ampul diyelim, cihaz kontrol merkezi ile kendiliğinden yapılandırılmış bir ağ üzerinden eşleşiyor. Her yeni cihaz ağda veri iletişimini ileten yeni bir düğümdür. Mesh ağları tipik olarak kablosuzdur - ancak Zentachain Meshnet, blok zinciri tabanlı ağ topolojisi ve daha az ortam altyapısı ile ilgilidir.

Zentalk teknolojik karanlığa ulaşır, bu da kullanıcıları veya mesajları hakkında hiçbir meta veri bulunamadığı anlamına gelir. Bu, MeshNet ve mimarisinin entegrasyonu ile sağlanır. Zentalk, tüm mesajları ve verileri MeshNet üzerinden iletir ve tüneller. Bu, gönderen ve alıcı arasında paylaşılan mesajların en yüksek gizlilik seviyelerine sahip olmasını sağlar.

Bir mesh ağında, her ağ düğümü bir veya daha fazla düğüme bağlanır. Birden fazla düğüm birbirine bağlandığında, bu tamamen bir mesh ağ olarak bilinir. Zentalk' tan bir mesaj gönderildiğinde, veriler MeshNet üzerinden gönderilir ve mesaj istenen alıcıya ulaşana kadar bir düğümden diğerine geçirilir. MeshNet'teki tasarım düğümleri, hangi düğümün hangi mesajı gönderdiğini ya da tam olarak hangi düğümün hangi mesajı aldığını bilmez. Bu, gönderen veya alıcı için tamamen anonimlik sağlar. Gönderen, alıcısına ulaşmak için 1 düğümü kullanır. Bu bir düğüm ZENTA'da şifreli mesajı iletmek için ödüllendirilecektir.

19.Zentamesh

ZentameshNet, sansür direnci sağlama yeteneğine katkıda bulunan kendi kendini iyileştirme özelliklerine sahiptir. Kendi kendini iyileştirme, bir düğüm bağlantısının engellenmesi veya devre dışı bırakılması durumunda, mesh ağı, kaybolan düğümün peşine takılabilir ve yeniden yönlendirilebilir. Veri yönlendirilir ve ağ hala işlevseldir. Mesh ağlar hem kablolu hem de kablosuz ağlara uygulanabilir, Zentalk ise bir mesh WLAN (Kablosuz Yerel Erişim Ağı) kurar. Bu MWLAN, Meshed WiFi düğümleri kullanılarak elde edilir. Bu çevrimdışı iletişim için gerekli olacaktır.

Bu, Zentachain token sahibinin, internet bağlantısı olmayan (çevrimdışı -> çevrimdışı) cihazlarla iletişim kurmanın yanı sıra, bir ağ uplink'i kurma (çevrimiçi ->çevrimdışı) ve paylaşma yeteneğine sahip olduğu anlamına gelir. Bu, çok az veya doğrudan altyapı olmadan gerçekleştirilebilir. Veri aktarma işlemi Zenta tokenleriyle ödüllendirilecektir.

Düğümler, cep telefonları, yönlendiriciler, anahtarlar, köprüler ve ağ geçitleri gibi aktif ağ bileşenleridir. Ağdaki bir düğüm bir bağlantı noktasıdır. Bu, yeniden dağıtım noktası veya veri aktarımındaki bir son nokta olabilir. İletimleri diğer ağ düğümlerine bulma, işleme ve iletme özelliğine sahiptir. Bir ağ düğümünün en az iki fakat genellikle diğer ağ elemanlarına daha fazla bağlantısı var.

Zentalk'ta, bir düğümün rolü bir cep telefonunda, tablette veya bir bilgisayarda çalışan eşler arası mesajlaşma dApp ile bağlı cihaz olacaktır.

Mesh teknolojisini kullanmak için 3 Sebep:

1. Ağ kararlılığı

(Kablosuz) Mesh ağındaki veriler çeşitli düğümler üzerinden iletilebilir. Düğümlerden biri veya bir kısmı hatalı veya bozuksa, veriler ekosistemdeki diğer düğümler üzerinden yönlendirilir.

2. Yüksek bant genişliği

Mesh ağları, daha yüksek bir bant genişliği sağlayan en uygun (dinamik) rotaları izleyecek şekilde tasarlanmıştır. Düğüm sayısındaki ve olası yol sayısındaki artışla, genel bant genişliği büyük ölçüde artar.

3. **Emniyet ve güvenlik**

WLAN'ın tek atlama mekanizmasıyla karşılaştırıldığında, bir Mesh ağının çoklu atlama mekanizması, kullanıcı iletişiminin birkaç düğümden geçmesi gerektiğini belirler.

4. **Zentalk & Hyperboria**

Zentachain, Hyperboria adında İnternet'e merkeziyetsiz bir alternatif kullanarak gizlilik ve çevrimiçi güvenlik konularını ele almaktadır. Hyperboria, uçtan uca(end to end) şifrelemeyi sağlamak için cjdns protokolünü kullanan bir Mesh Ağıdır. Bu, adres tahsisi için açık anahtarlı şifreleme ve yönlendirme için dağıtılmış bir hash tablo kullanılarak gerçekleştirilir. İki düğüm arasındaki iletişim ancak bağlantı doğrulaması gerçekleştikten sonra kurulabilir, bu üçüncü şahısların girmesi veya gizlice ayrılma ihtimalini ortadan kaldırır. Zentachain, Açık İnternet'e inanmaktadır. Hyperboria'yı kullanarak, kullanıcılarımıza kötü niyetli kuruluşlardan veya merkezi hizmet sağlayıcılardan istenmeyen izinsiz girişlerden korkmadan, verilerini hızlı, güvenli ve özel bir şekilde iletme fırsatı sağlıyoruz.

Tamamen bağlı bir Zentamesh topolojisi(Resim)

Zentamesh'in merkezinde Mobil istemci erişimi bulunuyor

Kısmen bağlı ağlarda bile, her cihaz birbiriyle iletişim kurabilir.

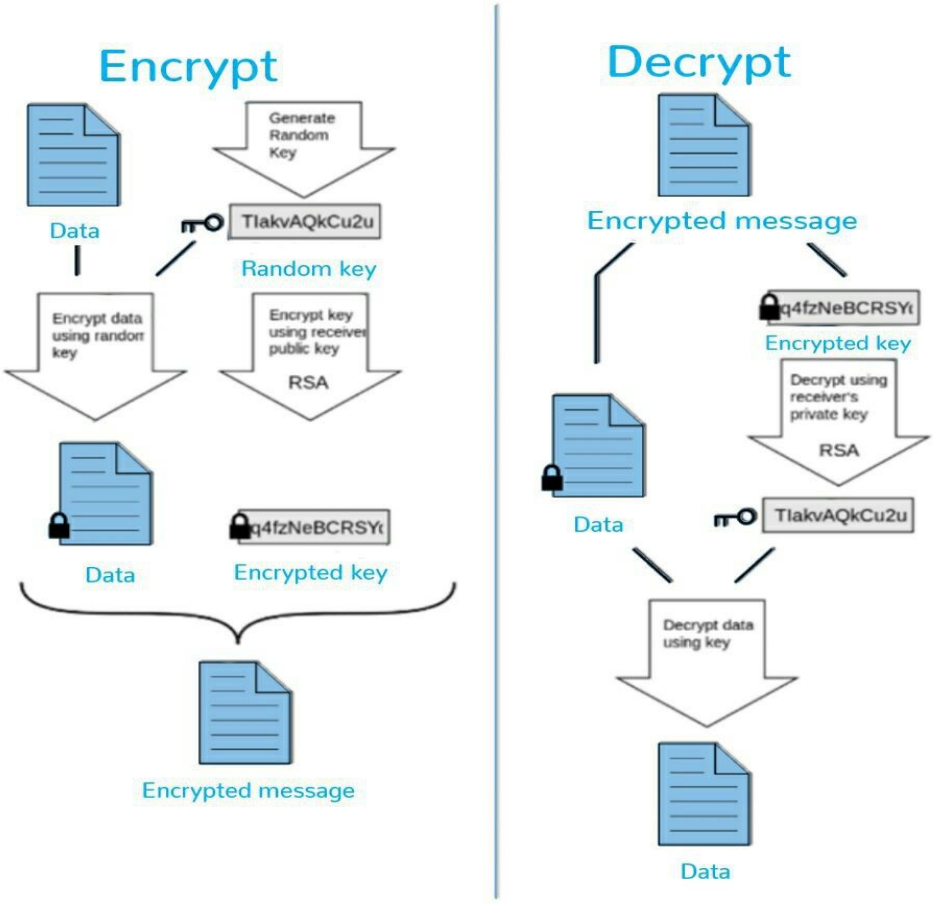
S: Neden mesh ağlarına karşı tutkulu olmalısınız?

C: Heyecan verici mesh ağlarının temel nedeni, merkezi bir altyapının gerekli olmamasıdır.

Bir meshnetteki gizlilik, "Uçtan uca şifreleme" ile garanti edilir.

“Uçtan Uca şifreleme” (E2EE) ile veriler gönderenin sisteminde veya cihazında şifrelenir ve yalnızca o alıcının şifresini çözebilir. Aradaki hiç kimse verileri okuyamaz veya değiştiremez. ISS (İnternet Servis Sağlayıcısı), Uygulama Servis Sağlayıcısı veya kötü amaçlı bir bilgisayar korsanı olması farketmez.

Böylece şifreleme ve şifre çözme yalnızca iletimin son noktalarında gerçekleşir. Şifreleme ve şifre çözme için kullanılan şifreleme anahtarları yalnızca terminallerde depolanır. Bu nedenle, bu tür şifrelemenin güvenliği çok yüksektir, çünkü gizli anahtar olmadan hiçbir şifre çözülemez.



“Uçtan uca şifrelemenin” bir başka avantajı: Daha fazla güvenlik ve özgünlük. E2EE dijital imza ile birleştirilebilir. Dijital olarak imzalanmış ve şifrelenmiş bir mesaj, gönderenin gerçekten de iletinin 'gerçek' göndereni olduğunu kanıtlar. İletim sırasında mesajın değiştirilmemesini de sağlar. Kitle gözetimi yoktur. Uçtan uca şifreleme, mesajlarınızı toplu gözetimden korur.

20.Zentavault

Zentavault, Zentachain uygulamalarının ikincisidir. Zentavault, yüksek oranda şifrelenmiş ve dağıtılmış bir depolama hizmeti olarak tasarlanmış, yüksek performanslı bir dApp'dir. Bu servis Zentachain platformunda saklanacaktır. ZentaChains dApps hiçbir zaman merkezi sistemlere güvenmez. Ve kesinlikle kullanıcıların meta verileri için hiçbir yedekleme veritabanına sahip olmayacaktır. Bunu yaparak, Zentavault gizlilik, anonimlik ve ticari performansı artıracaktır.

Zentavault aylık kullanım ücreti gerektirmez, bunun yerine veri yüklemek için yalnızca çok az bir işlem ücreti alınır. Zentavault bir dosya şifreleme ve dağıtım aracıdır. İçeriği seçtikleri şekilde şifrelemek, depolamak ve paylaşmak için kullanıcıyı çarkın gerisine ve kontrol altına alın.

Zentavault ile, verilerinizin IPFS olarak da adlandırılan, InterPlanetary Dosya Sistemine kalıcı olarak şifrelenmiş ve gömülü olduğundan emin olabilirsiniz. Bir ilişkisel bellek stratejisi kullanarak içeriğin gömülmesine ve paylaşılmasına olanak sağlayan özel bir ağdır.

İçerik IPFS'de olduğunda, kriptografik hash veya hash kimliği olarak bilinen benzersiz bir tanımlayıcı atanır. Bu, kullanıcıların verilerini bulmak veya iki taraf arasında paylaşmak için kullanılabilir. İçeriğiniz IPFS'ye dahil edildikten sonra, başkalarına içerik bulma veya paylaşmanın bir yolunu sağlayan bir hash Kimliği atanır. IPFS gibi eşler arası bir hiper medya protokolü teknolojilerini kullanarak, Zentavault daha hızlı, korumalı ve erişilebilir bir dosya depolama ve aktarma hizmeti sağlayabilir.

IPFS (InterPlanetary Dosya Sistemi)

Modern internet, çağımızın çığır açan teknolojilerinden biri olmasına rağmen, 1990'lı yıllardaki kuruluşundan bu yana kısıtlamaları olduğunu göstermiştir. Teknolojik gelişmeler ilerledikçe, daha fazla teknolojinin, iyileştirmeye ya da hatta kavramsal olarak yeniden güncellemeye ihtiyaç duyduğu görülüyor. HTTP protokolü ile durum böyle.

Son zamanlarda, gizlilik, güvenlik ve hız konularına, yani HTTP protokolünün “göreve bağlı” olarak gösterilmediği alanlara hitap edecek çözümlere yönelik bir talep gördük. Neyse ki birçok sorun için çözüm geliştiren IPFS ortaya çıkmıştır.

Ama nasıl çalışır?

Buna bir BitTorrent swarm açısından bakabiliriz ancak zaman içinde dosya sürümlerini saklama ve izleme özelliğine sahiptir. Kaynakları konum tabanlı IP adresleriyle eşleyerek çalışan HTTP'nin aksine, IPFS içerik adresli bir sistem kullanır. Bu merkezi olmayan sistem, dosyaları eşler arasında depolar ve adres olarak kullanılan bir dosyada şifreli bir hash aracılığıyla onlara erişim sağlar. Bu, kullanıcının aynı anda hem istemci hem de ana bilgisayar olduğu anlamına gelir.

Merkle DAG (Yönlendirilmiş Asiklik Grafikler) veri mimarisi ile mümkün kılınır ve IPFS'de üstünlük ve içerik sürümü sağlar. Benzer yapıları nedeniyle IPFS, blok zinciri entegrasyonu için mükemmel bir seçimdir. Bundan biraz daha ileride olsa da, blockchain'in sürükleyici veri depolama sorununu çözmek ve blockchain ile birlikte büyük veri ve dosyaları depolamak, şifrelemek ve paylaşmak için bir çözüm oluşturur. Her ne kadar henüz başlangıç aşamasında olsa da, IPFS, HTTP'nin halefi olmak ve World Wide Web'in yeni bir döneminde kullanmak için tüm araçlara sahiptir.

IPFS Kimlikleri

Düğümler, S / Kademlia'nın statik kripto yapbozuyla [1] oluşturulan, bir kamu anahtarının şifreleme hash3 olan bir Düğüm Kimliği ile tanımlanır. Düğümler ortak ve özel anahtarlarını saklar (bir kripto ile şifrelenir). Kullanıcılar, her başlangıç sırasında "yeni" bir düğüm kimliği yerleştirmekte özgürdür, ancak bu, var olan ağ avantajlarını kaybettirebilir. Dolayısıyla düğümlerin aynı kalması genelde teşvik edilir.

IPFS Ağı

IPFS düğümleri ağda potansiyel olarak geniş bir internet üzerinden yüzlerce başka düğümle düzenli olarak iletişim kurar. IPFS ağ yığını özellikleri:

- İletme: IPFS herhangi bir aktarım protokolünü kullanabilir ve WebRTC DataChannels (tarayıcı bağlantısı için) veya uTP (LEDBAT) için uygundur.

- Güvenilirlik: IPFS, temel ağlar sağlamazsa, uTP (LEDBAT) veya SCTP kullanarak güvenilirlik sağlayabilir.

- Bağlantı : I PFS ayrıca ICE NAT geçiş tekniklerini kullanır.

- Bütünlük: İsteğe bağlı bir hash sağlama toplamı kullanarak iletilerin bütünlüğünü denetler.

- Doğruluk: İsteğe bağlı olarak, gönderenin genel anahtarı olan HMAC kullanarak iletilerin orijinalliğini kontrol eder.

IPFS Yönlendirme

Yönlendirme için IPFS, S / Kademlia ve Coral'a dayanan Dağıtılmış Özensiz Tabloları kullanır.
Amacı:

1. Düğümlere eklenen verileri duyurun
2. Belirli düğümler tarafından istenen verileri bulun

1 KB'den küçük veya ona eşit olan veriler doğrudan DHT'de depolanır. 1 KB'den büyük veriler için DHT, bloğa hizmet edebilecek eşlerin Düğümleri olan referansları saklar.

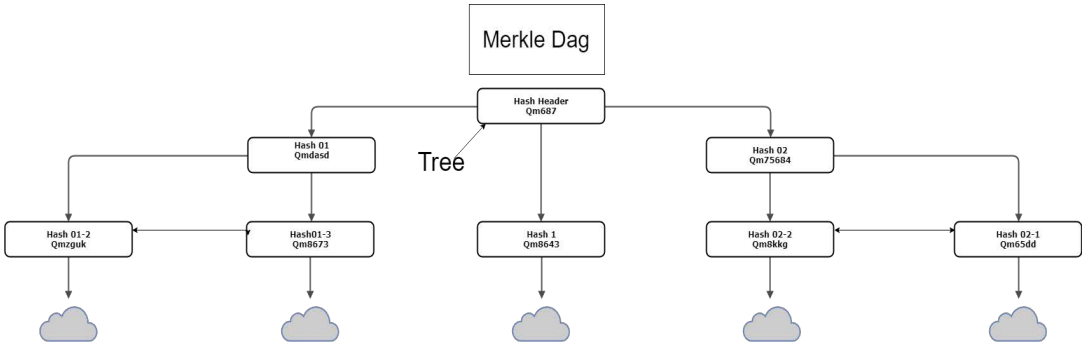
Objects Merkle DAG

Merkle DAG (Merkle Direction Asyclic Graph), Nesneler Arası Dosya Sistemindeki nesne dosyalarının sırasını korumak için kullanılır. Merkle DAG, dosyaların bir hash kimliği olarak bilinen benzersiz şifreleme hash değerleri ile birbirine bağlanmasını sağlar. Hash id (object), tüm hash id object linklerini içerir. Merkle DAG, IPFS'ye aşağıdaki gibi faydalı özellikler sunar:

- İçerik koruması: Merkel DAG, ipfs'teki tüm içeriğin güvenliğini, emniyetini ve bütünlüğünü garanti eder. İpfs'te saklanan veya barındırılan herhangi bir nesne tahrif edilmiş veya başka bir şekilde bozulmuşsa, Merkle DAG kök hashini otomatik olarak değiştirir. Bu, dosyaya yapılan değişiklikleri gösterir.

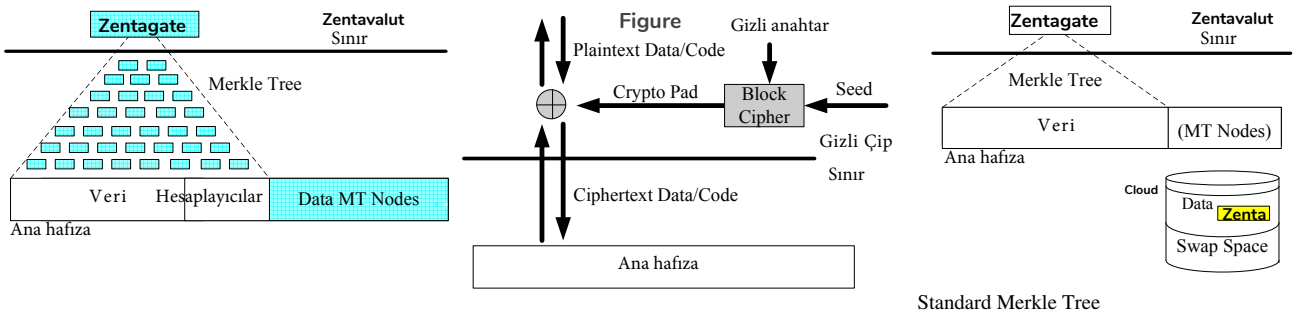
- Verimlilik için anti-çoğaltma: IPFS'de içerik tutan tüm nesneler sıralanır, çoğaltılan nesneler tanınır ve silinir. Bu, içeriğin IPFS'de birden çok kez saklanmadığını garanti eder.

- İçerik adresleme: Tüm içerik, bağlantılar dahil olmak üzere benzersiz hashid veya çoklu hash tanımlanarak bulunabilir.



Adresten Bağımsız Çekirdek(Seed) Şifrelemesi Kullanma

Bellek şifrelemenin amacı, güvenli işlemci sınırı dışında depolanan tüm verilerin ve kodların anlaşılmaz olmasını sağlamaktır, depolanan gerçek değerler hakkında hiçbir şey göstermez. Şekil, karşı mod şifrelemede bunun nasıl elde edildiğini göstermektedir. Bir blok belleğe tekrar yazıldığında, bir çekirdek bir blok şifre (ör. AES) ve sadece işlemci tarafından bilinen bir gizli anahtar kullanılarak şifrelenir. Şifreli çekirdek bir şifreleme rampası olarak adlandırılır ve bu rampa, blok belleğe yazılmadan önce bloğun şifreli metnini üretmek için bit şeklinde bir XOR işlemi vasıtasıyla düz metin bloğu ile birleştirilir. Aynı şekilde, bir şifreli metin bloğu bellekten alındığında, aynı çekirdek bloğu şifrelemek için kullanılan aynı rampanın üretilmesi için şifrelenir. Blok çip üzerine ulaştığında, rampalı bir başka bit XOR değeri bloğu orijinal düz metin biçimine geri yükler. Matematiksel olarak, eğer P düz metin ise, C şifreli metindir, E blok şifreleme işlevidir ve K gizli anahtardır, şifreleme C = P EK (Çekirdek) gerçekleştirir. Her iki tarafı da EK (Çekirdek) ile XOR yaparak, şifre çözme düz metni P = C EK (Çekirdek) olarak verir.

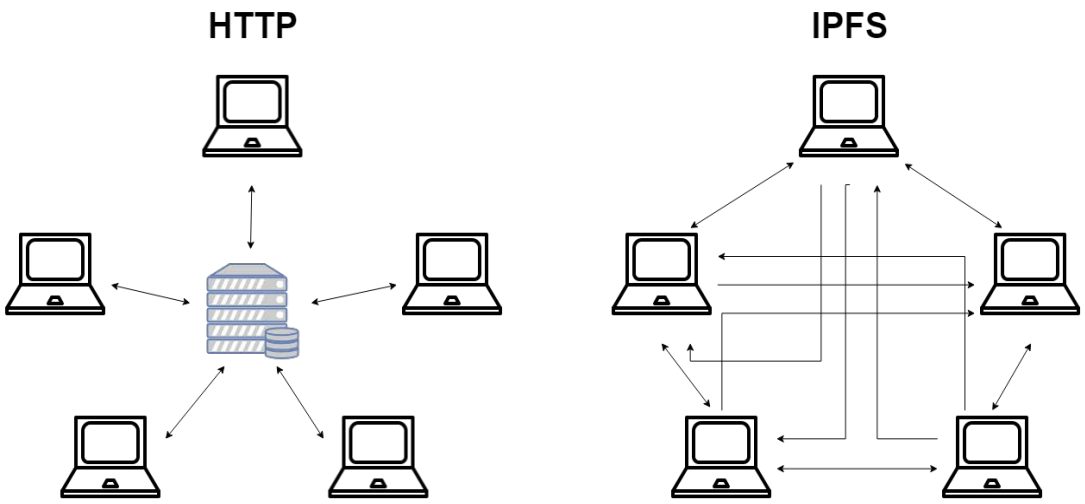


Standard Merkle Tree

IPFS Dosyaları

IPFS ayrıca, Merkle DAG'ın üstündeki sürümlü bir dosya sistemini modellemek için bir nesne kümesi tanımlar. Bu nesne modeli Git'inkine benzer:

1. blok: değişken boyutlu bir veri bloğu.
2. liste: blok veya diğer listelerden oluşan bir koleksiyon.
3. ağaç: blok, liste veya diğer ağaçlar topluluğu.
4. taahhüt: Bir ağacın versiyon geçmişinde bir anlık görüntü.



21.Neden IPFS'e ihtiyacımız var ?

Bant genişliği

Verilere sadece merkezi bir konumdan erişebilmenin, dezavantajları olabilir. Bir dosyayı, bir oda dolusu insanla paylaşmak istediğinizi düşünün. Daha sonra bu dosyayı muhtemelen sizden uzakta bir yere (internetin omurgası) bulunan ve yolda birkaç sunucu üzerinden yönlendirilen merkezi bir sunucuya yüklersiniz. Diğer insanlar daha sonra bu uzak sunucuya tekrar bağlanıp dosyayı alarak bu dosyaya erişebilirler. Özellikle resim ve video gibi büyük dosyalarda, bu dosyayı, muhtemelen sizinle aynı yerel alan ağına bağlı olan insanlarla dolu bir odayla paylaşmak için çok fazla bant genişliği kullanılmasına neden olabilir.

IPFS ile bu dosya, yerel alan ağı üzerinden dosyaya sahip olan odadaki tüm bilgisayarlar tarafından doğrudan sunulabilir ve böylece çok daha az bant genişliği kullanabilir, çünkü merkezi sunucuya yönlendirilmeye gerek kalmaz. Bu, depolama maliyetinden çok daha yavaş azalan bağlantı hızı maliyetine bakıldığında özellikle önemlidir. Bu eğilim devam ederse, kullanıcılar çok daha fazla veri depolayabilecek ve böylece ağ kullanımlarını artıracaktır. Ancak, bant genişliği aynı hızda gelişmiyorsa, bağlantı hızı yavaşlar. Güvenlik de artar - örneğin DDos saldırıları işe yaramaz, çünkü IPFS'lerin sahip olmadığı merkezi bir dağıtım sistemine saldırmaya güveniyorlar. Hız artan bir başka faktördür. Dağıtılmış bir ağda, bir şey isteyen her düğüm, tek bir merkezi konum yerine onu kendisine en yakın olan düğümden ister.

Gecikme

İlgili bir sorun da gecikmedir. Işık hızı sabit olduğu ve değiştirilemediği için gecikmeyi azaltmanın tek yolu, verileri kullanıcıya daha yakın bir noktadan sunmaktır. Bu nedenle büyük bulut servis sağlayıcıları bölgelere göre depolama yerleri sunmaya başladı. IPFS, mümkünse istenen verilere hizmet veren bilgisayara olan mesafeyi azaltmayı amaçlamaktadır.

Çevrimdışı Olma

Her gün kullandığımız hizmetlerin çoğuna yalnızca çevrimiçi olduğumuzda güvenebiliriz. Aynı odadaki diğer kişilerle birlikte bir belge üzerinde birlikte çalışmak veya telefonunuzdan dizüstü bilgisayarınıza veri aktarmak istiyorsanız, bunu yalnızca internetin merkezi sunucularına bağlıysanız yapabilirsiniz. Bant genişliği veya tıkanıklık, ISS kesintisi veya veri merkezi sorunları gibi altyapı sorunları varsa, bu hizmetleri artık kullanamazsınız. IPFS, bu merkezi sunuculara bağlanmanıza gerek kalmadan doğrudan diğer eşlere bağlanmanıza izin vererek bunu değiştirmeyi umuyor.

Sansürleme

Bir P2P ağına kıyasla, merkezi sunucularda saklanır ve çalıştırılırsa verilere veya hizmetlere erişim sansürlenebilir veya kısıtlanabilir. Buna bir örnek, Mısır hükümeti, protestocular arasında iletişimi engellemek ve kısıtlamaları engellemek için 2011 yılında Arap baharı boyunca İnternete tüm erişimi kesti. Bağlantılı olarak P2P IPFS, bu sansürü imkansız hale getirmeyi umuyor.

Devamlılık

Herkes daha önce bir 404 hatasıyla karşılaşmıştır. Bu, silinen veya taşındığı için gerekli içeriğin bulunamadığı anlamına gelir. Örneğin, sağladığınız içerik için elzem olduğundan, bu içeriğe bağlanmak istiyorsanız bu çok büyük bir problem olabilir. Genel olarak, web'de biriken bilgilerin çoğunun erişilebilir kalması ve silinmemesi toplum için faydalı olacaktır, çünkü birisi kasıtlı olarak veya yanlışlıkla bazı web sitelerini kapatabilir. IPFS ile bağlantılı içeriğin bir sürümünü kendiniz kaydedip saklayabilirsiniz ve bu şekilde, orijinal ana bilgisayarlar artık saklamasa da, bu içeriğin kullanıcılar tarafından her zaman kullanılabilir olmasını sağlar. Nihai fikir, hiçbir içeriğin kaybedilmediği kalıcı bir ağ oluşturmaktır çünkü tüm içerik onu değerli bulan birçok kişi tarafından saklanmaktadır.

Güvenlik

Son yıllarda sayısız saldırıların gösterdiği gibi, sadece sunucular ve istemciler arasındaki iletişimde güvenliği düşünmek yeterli değildir. IPFS, gelişmiş kimlik doğrulama ve şifreleme yöntemleriyle verilerin kendisini korumasını ve şifrelemesini amaçlar.

Kendinden Sertifikalı Dosya Sistemleri- SFS

İnterneti kapsayacak hiçbir güvenli ağ dosya sistemi geliştirilmemiştir. Mevcut sistemlerin tümü güvenlik için küresel ölçekte yeterli anahtar yönetiminden yoksundur. İnternetin çeşitliliği göz önüne alındığında, bir dosya sisteminin anahtarları yönetmek için kullandığı herhangi bir mekanizma birçok kullanım türünü desteklemeyecektir. Şifre yönetimini dosya sistemi güvenliğinden ayırmayı öneriyoruz, bireylerin şifreleri nasıl yönetirse yönetsin dünyanın tek bir global dosya sistemini paylaşmasına izin veriyoruz. Dahili anahtar yönetimini önleyen güvenli bir dosya sistemi olan SFS'yi sunuyoruz. Diğer dosya sistemleri, dosya adlarını şifreleme anahtarlarıyla eşleştirmek için anahtar yönetimine ihtiyaç duyarken, SFS dosya adları etkin şekilde ortak anahtarlar içerir ve bu sayede kendi kendini sertifikalandıran yol adları oluşturur. SFS'deki şifre yönetimi, kullanıcıların dosya adları oluşturmayı seçtiği prosedürde, dosya sisteminin dışında gerçekleşir. Kendiliğinden Sertifika Veren Dosya Sistemi (SFS) [8], şifreleme dosya sistemlerinde anahtar yönetimi sorununu ele alır ve anahtar yönetimini dosya sistemi güvenliğinden ayırmayı önerir.

Sunucularda ortak bir anahtar bulunur ve istemciler sunucunun kimliğini doğrulamak ve güvenli bir iletişim kanalı oluşturmak için sunucu ortak anahtarını kullanır. SFS, kullanıcıların daha önce hiç duymadan, yerinde bulunan sunucuları kimlik doğrulamalarına izin vermek için, "kendi kendini onaylayan bir yol adı" kavramını ortaya koyar.

Kendini onaylayan bir yol adı(pathname), sunucunun genel anahtarının hash değerini içerir, böylece istemci, gerçekten yasal sunucuyla konuştuğunu doğrulayabilir. İstemci sunucuyu doğruladıktan sonra güvenli bir kanal kurulur ve gerçek dosya erişimi gerçekleşir. Uzak SFS dosya sistemlerine / sfs bağlama noktasından erişilir. Bir SFS yol adı şu söz dizimine uyar:/ sfs / location: hostid / real / pathname, burada `` konum '', dosya sistemini dışa aktaran sunucunun adı (IP adresi veya DNS Adı) ve `` hostid '' sunucunun genelini(anahtar ve diğer bazı bilgiler) içeren bir dizenin özetidir. SFS, yol adının kullanıcı tarafından nasıl elde edildiği ile ilgilenmez; bir kullanıcı sonunda mevcut bir PKI (Genel Anahtar Altyapısı) kullanarak ana bilgisayar kimliklerini alabilir. Öte yandan, ilgilendiği dosyalar için kendinden onaylı bir yol adı alındığında, kullanıcıların herhangi bir anahtarı hatırlamaları gerekmez.

Bu, IPFS için IPNS ad sistemini uygulamak amacıyla kullanılır. Kullanıcının, adresin geçerliliğini doğrulayabildiği uzak bir dosya sistemi için bir adres oluşturmamızı sağlar. SFS, Self-Certified Dosya Sistemlerini oluşturmak için bir teknik ortaya koydu: uzaktaki sistemlere aşağıdaki şema ile erişmek:

```
/sfs/<Location>:<HostID>

where Location is the server network address, and:

HostID = hash(public_key || Location)

Thus the name of an SFS file system certifies its server.
```

Yukarıda okuduğunuz üzere, web zaten çalışıyor gibi işleyecek şekilde tasarlanmıştır. IPFS, yalnızca belirli programların anladığı özel bir bağlantı veya başka dosyaları indirmek için bir dosya yerine, IPFS, tarayıcıda çalışan ortak bağlantılarla çalışmak üzere tasarlanmıştır ve özel bir yazılım yüklemeniz gerekmez. IPFS, herhangi bir ağ mimarisini kullanabilir ve her türlü dosya DAG olarak kullanılabilir. Bu özelliğe IPLD (Gezegenlerarası Bağlantılı Veri) adı verilir.

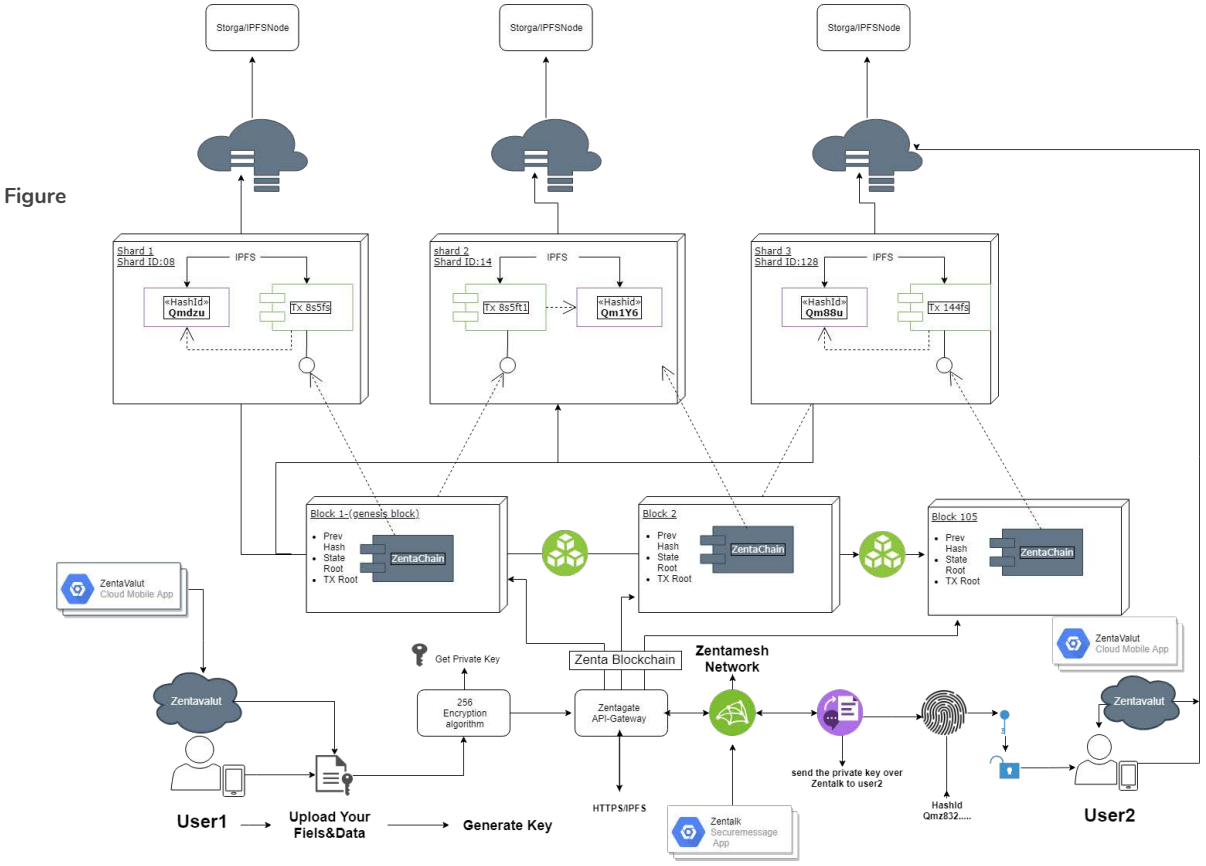
22.Zentagate

Zentagate, dapp zentavault ile IPFS'de depolanan içeriği kolayca yüklemenizi ve erişmenizi sağlayan bir ağ geçididir. Zentagate'in kendisi, makinelerin IPFS'ye bağlı olduğu sabit bir ağ geçididir. Zentagate ile bağlantılı olan bu Makineler, kümede dosyaların yayınlanmasını ve alınmasını kolaylaştırmaya yardımcı olan dağıtılmış bir sistem parçası olarak kullanılır. Zentagate ayrıca, ön uç Dapps'ın IPFS ile sunucu olmadan doğrudan etkileşime girmesini sağlayan bir Javascript API'sine sahiptir. Bu, Zentavault gibi Dapps'ın doğrudan ipfs'e içerik eklemesini mümkün kılacaktır. Zentavault, tamamen IPFS üzerinden sunulan şifreli içeriği tutmak için kullanılan statik web siteleri oluşturmak için Zentagate'i kullanır. Bu, kullanıcıların hükümetler, şirketler veya diğer kuruluşlar tarafından sansür edilemeyecek bilgiler içeren güvenli içerik depolaması oluşturmasını sağlar. ZentaChain'in ağ geçidinin sizin adınıza talep ettiği her dosya için, içeriğin geçiş sırasında değiştirilmediğinden emin olmak amacıyla dosyanın hash' ini kontrol eder. Her dosyaya otomatik olarak eklenecek olan zentagate şifrelemesi üzerinden IPFS' ye dosya içeriğinin hash değerinden türetilmiş bir adres verilir. Bu adres parmak izi gibidir. Dosyaya benzersiz bir şekilde aittir ve dosyanın IPFS'de nerede depolandığına bakılmaksızın aynı olacaktır.

Q:Dosyalarımı ZentaValut'a yükledikten sonra düğümü çalışır durumda tutmam gerekir mi?

A:Hayır, hash'e sahip olduğunuzda problem yok.(Qm.....)

Figure



23.Referanslar

IPFS
Sharding JDBC

Ethereum (Smart)

Hyperboria IpV6

Gateway-Blockchain

Meshnet Blockchain

Network Landscape

Sha256/516

API Application Cyber

Protect/P2P Cjdns

Protocol Whitepaper

Sharding Ethereum

Hyperboria/IPV6 W3C/

AES JavaScript APIs

rsaEncryption

RSAPrivateKey

ECMAScript

Blockchain shards

Polynomially code (PS)

Ölçeklendirme

Verimliliği Depolama

Verimliliği Cjdns

Cjdns supernode

Hyperboria API Seed

Şifreleme

DPOS

1. Mathis T. Ethereum: Your Guide To Understanding Ethereum, Blockchain,and Cryptocurrency [Internet]. Level Up Lifestyle Limited; 2018. Available: https://market.android.com/details?id=book-NzVODwAAQBAJ

2. Adams M. Ethereum: The Beginners Guide to Understanding Ethereum, Ether, Smart Contracts, Ethereum Mining, Ico, Cryptocurrency, Cryptocurrency Investing [Internet]. Createspace Independent Publishing Platform; 2018. Available: https://books.google.com/books/about/Ethereum.html?hl=&id=SH4atwEACAAJ

3. Blokdyk G. Erc20 Second Edition [Internet]. Createspace Independent Publishing Platform; 2018. Available: https://books.google.com/books/about/Erc20_Second_Edition.html?hl=&id=qEl HtAEACAAJ

4. Skvorc B, Kendel M, Attard D, Javor M, Jankov T, Ward C. A Developer's Guide to Ethereum [Internet]. SitePoint; 2018. Available: https://market.android.com/details?id=book-5RFqDwAAQBAJ

5. Dannen C. Advanced Concepts. Introducing Ethereum and Solidity. 2017. pp. 173–179. doi:10.1007/978-1-4842-2535-6_11

6. Li J, Wu J, Chen L. Block-secure: Blockchain based scheme for secure P2P cloud storage. Inf Sci . 2018;465: 219–231. doi:10.1016/j.ins.2018.06.071

7. Patil S. Preventing unauthorized Data Access in Fully Obscure Attribute Based Encryption with Security Solutions. International Journal for Research in Applied Science and Engineering Technology. 2018;6: 2950–2957. doi:10.22214/ijraset.2018.5481

8. Asarudeen SS, Sheik Asarudeen S, Mba FY, Srinivasan College of Arts &Science, Perambalur, Priya RPR. Recruitment of Ethical Hackers. J Appl Sci Res. 2012;2: 145–146. doi:10.15373/22778179/jan2013/50

9. Guo B. Why Hackers Become Crackers – An Analysis of Conflicts Faced by Hackers. Public Administration Research. 2016;5: 29. doi:10.5539/par.v5n1p29

10. Fischetti M. Data Theft: Hackers Attack. Sci Am. 2011;305: 100–100. doi:10.1038/scientificamerican1011-100

11. Cornwall H. Data Theft: Computer Fraud, Industrial Espionage and Information Crime [Internet]. 1990. Available: https://books.google.com/books/about/Data_Theft.html?hl=&id=Db0lnQEACA AJ

12. Gilroy AA. Access to Broadband Networks: The Net Neutrality Debate [Internet]. DIANE Publishing; 2011. Available: https://books.google.com/books/about/Access_to_Broadband_Networks.html?hl=&id=IVGN5J28tuEC

13. Nelson D. The Problems of Data Ownership and Data Security. Science Trends. 2017; doi:10.31988/scitrends.3265

14. Tiemensma J, Biermasz NR, van der Mast RC, Wassenaar MJE, Middelkoop HAM, Pereira AM, et al. Increased psychopathology and maladaptive personality traits, but normal cognitive functioning, in patients after long-term cure of acromegaly. J Clin Endocrinol Metab. 2010;95: E392–402. doi: 10.1210/jc.2010-1253

15. Loukas G. Physical-Cyber Attacks. Cyber-Physical Attacks. 2015. pp. 221–253. doi:10.1016/b978-0-12-801290-1.00007-2

16. Rampling B, Dalan D. DNS For Dummies [Internet]. For Dummies; 2003. Available: https://books.google.com/books/about/DNS_For_Dummies.html?hl=&id=8EBjIp 8w5pwC

17. Reschke J. Initial Hypertext Transfer Protocol (HTTP) Method Registrations [Internet]. 2014. doi:10.17487/rfc7237

18. The New York Times Editorial Staff. Net Neutrality: Seeking a Free and Fair Internet [Internet]. The Rosen Publishing Group, Inc; 2018. Available: https://books.google.com/books/about/Net_Neutrality.html?hl=&id=g9xoDwAA QBAJ

19. Drescher D. Reinventing the Blockchain. Blockchain Basics. 2017. pp. 213–220. doi:10.1007/978-1-4842-2604-9_23

20. Solidity — Solidity 0.4.23 documentation. (2018). Solidity.readthedocs.io

21. Remix - Solidity IDE. (2018). Remix.ethereum.org. [Online]

22. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system

23. The GNU Privacy Guard. (2018). Gnupg.org

24. Blockchain Proof Engine | API. (2018)

25. Blockchain and Distributed Ledgers as Trusted

26. Recordkeeping Systems

27. Practical scheme for non-interactive verifiable secret sharing

28. Truffle Suite - Your Ethereum Swiss Army Knife. (2018). Truffle Suite. [Online]. Available:http://truffleframework.com

29. K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer et al., “On scaling decentralized blockchains,” in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 106–125.

30. Y. Sompolinsky and A. Zohar, “Secure high-rate transaction processing in bitcoin,” in International Conference on Financial Cryptography and Data Security. Springer, 2015, pp. 507–527.

Teşekkürler

Zentachain.io