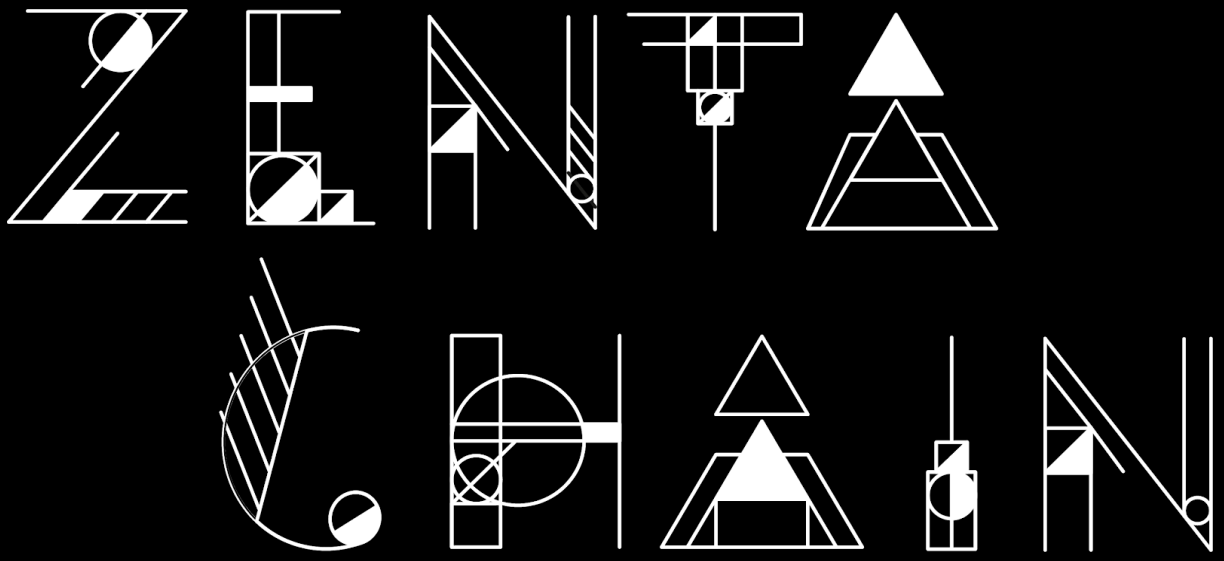


Whitepaper

“Gelecek, bugünün potansiyelini aydınlatır”

Version 1.2

WHITEPAPER’I YAZANLAR

Zentachain.io

ÖZEL TEŞEKKÜR Zentachain ve arkadaşlara!
E-posta:: team@zentachain.io

Güvenlik, Anonimlik ve Çevrimdışı İletişim İçin Tasarlanmıştır
Zentachain Labs
Zentachain.io
(Tarih: 03.01.2020, Versiyon 1.2)

Önsöz:

Dijital devrimin, içinde bulunduğumuz dünyayı yeniden yazması ile birlikte şimdiden geleceğimizin yeni bir versiyonunda yaşamaktayız. Barbrook'un 2006'da söylediği gibi: ‘Yeni teknolojilerin önemli olması, burada ve şu anda yapabilecekleri için değil, daha gelişmiş modellerin gelecekte neler yapabileceği içindir. Bugün embriyoda gelecek gibi anlaşılıyor ve gelecek, bugünün potansiyelini aydınlatıyor'. Dijital dönüşüm geleceğimize daha büyük katkı sağlamaktadır. Bu günlerde insanlar teknolojiye her zamankinden daha fazla güveniyorlar. Kişisel bilgisayarlar ve son zamanlarda akıllı telefonlar icat edilmesi ile birlikte tüm dünya birbirine bağlanmış gibi görünüyor. Dijital iletişim ve etkileşimler, sosyal medya, kullanıcı tarafından oluşturulan web siteleri ve ücretsiz çevrimiçi ansiklopediler olmadan bir dünya düşünemiyoruz. İnternetin önemi, hepimizi birbirine bağlayan fiberler, her geçen gün artmaya devam etmektedir. Artık dünyaya erişiminiz var ve aynı zamanda da dünyanın size erişimi var. Daha fazla dijitalleşme olumlu olarak değerlendirilebilir, çünkü bütün çalışma biçimini değiştirdi, daha kullanışlı ve verimli hale getirdi. Hareketliliği ve üretkenliği arttırdı ve özel bir çalışma alanına olan ihtiyacı azalttı. Ancak dijital devrimin de karanlık bir tarafı var ve bu tam olarak Zentachain'in veri dosyalarınızı ve belgelerinizi merkezi bir sunucuda saklayan şirketlere karşı koruyacağı şeydir. Zentalk, aynı zamanda iletişim ve mesaj geçmişinize sahip oldukları için onları satma ihtimali olan büyük şirketlere karşı da korur. Kriptografi, gizli anahtarlar ortaya çıkarılmadığı veya merkezi bir platformda bulunmadığı sürece, Zentachain'e güvenilmeyen kanallar üzerinden kimliği doğrulanmış şekilde iletişimi sağlar. Zentachain için, internet üzerinden bilgi alışverişini korumak ve gizli verilerin merkezi olmayan bir şekilde depolanması önemlidir. Zentachain ekibi, iletişim ve veri depolama konusunda çok hassas olarak çalışmakta ve onları üst düzey güvenlik seviyesine ulaştırmak için anonimlik ve şifreleme konusunda çok titiz davranmaktadır. Ana ürünler verileri şifreleyip kullanıcının kendi cihazında barındırabilir. Zentalk, bulut depolaması olmayan ve merkezsiz hibrit bir mesajlaşma uygulamasıdır. Zentamesh network adı verilen kendi ağına sahiptir; bu, kullanıcıların kendi arasında çevrimdışı olarak internet erişimi olmadan geniş bir alanda iletişim kurmasına yardımcı olur. Zentalk, Blake2 algoritmasını içermektedir. Zentachain, Zenta adı altında kendi blok zincirini başlatacaktır. Zenta blockchain' ini Zentamesh ağında çevrimdışı iletişime olanak sağlayacak şekilde tasarladık. Zentalk kullanıcıları, Zenta ile ödüllendirilmek için Zentamesh ağında Zentanode sahibi olabilirler. Zentachain Labs, temelini oluşturmak için çeşitli seçenekler düşünmektedir. Seçeneklerimiz arasında şunlar mevcuttur: Cosmos (BPOS), Polkadot (Parachain & Blake2 ve NPOS) ve Ethereum (POW & POS). Ekosistem, ölçeklenebilir merkeziyetsiz uygulamalar ayrıca dağıtılmış hizmetler ve eşler arası(P2P) merkezi olmayan bulut depolaması oluşturmak ve barındırmak için gerekli tüm yapı taşlarını bulundurur.

İÇERİK

1. Problem

- Kişilerin güvenli etkileşim ve dijital veri depolama ihtiyacı.
- Yetkisiz veri erişimi ve bilgi akışlarının manipüle edilmesi sorununun çözülmesi.
- Bilgisayar korsanlarına karşı koruma - yetkisiz erişime sahip olma ve bilgi çalma, kaydetme, toplama ve kullanıcı verilerini satma.
- Kullanıcı bilgisi için ağ tarafsızlığını kullanma.
- Veri sahipliğini, veri güvenliğini ve iletişimi sağlamak.
- Bulut depolama için sahiplik ve güvenlik.
- Şifrelenmemiş veya güvenli olmayan bir veri depolama işlemi, bir kullanıcı cihazında veya dijital ortamlarda potansiyel olarak kaydedilebilir ve bir veritabanında yada bir dosya sunucusunda bir yerlerde saklanmaktadır. Bu verilerin uygun şekilde şifrelenmemesi veya anonimleştirilmemesi ise olasıdır.
- Bir sunucu veya buluta dayalı iletişim uygulaması.
- Büyük şirketler tarafından şifrelenmesi gereken ama şifrelenmemiş veri ve iletişim geçmiş bilgileri yada kullanıcıların bir fonksiyon başlatma zorunluluğu.
- Kullanıcı verilerine ve bilgilere erişebilme amacı ile programlarda hak kazanmak için birbirlerine karşı casusluk yapan uygulamalar.

2. Vizyon

Zentachain net nötr veriler, işlem değişimi ve veri depolama için oluşturulmuş merkezi olmayan bir ekosistemdir. Ekosistem kullanıcıları tarafından korunmakta olup çeşitli siber saldırılara karşı tamamen koruma altındadır. Bunun yanında, güvenlik ve veri sahipliği problemleri için uygun çözümler mevcuttur. Zentachain açık kaynaklı bir projedir. Zentachain, IPFS (https://ipfs.io) gibi yerel ağ tabanlı ağ bulut hizmetleri ile DNS ve HTTPS gibi dinamik yönlendirme ve adresleme protokolleri arasındaki boşluğu doldurmayı hedeflemektedir. Bu, Zentachain Labs'in IPFS eşler arası hypermedia protokolünü, en gelişmiş blockchain teknolojisi ve Zentameshnet olarak adlandırılan kendi ağı ile geliştireceği gerçeğine dayanmaktadır.

Ağ yalnızca ultra güvenli, merkezsiz ve kalıcı hale gelmeyecek, aynı zamanda daha hızlı ve daha açık hale gelecek. Zentachain, IPFS ile büyük miktardaki veriler ile işlem yapmayı ve blok zinciri işlemi kullanarak sabit ve kalıcı IPFS bağlantılarını Zenta defterine kaydetme olanağını sağlayacaktır. Bu, verileri Zenta'nın üzerine koymak zorunda kalmadan içeriğe zaman bilgisi verir ve koruma altına alır. Zentachain, iletişimde özgürlüğü ve bağımsız ruhu en güçlü halde ve düşük bir maliyetle sunmaktadır. Ekosistem, içeriğin kullanıcıya önemli miktarda para ve kullanıcı bilgisi kazandıracak şekilde sunulmasına yardımcı olacaktır.

Yüksek gecikmeli ağlar, gelişmekte olan dünyaya giriş için gerçek bir engel teşkil etmektedir. Zentachain, düşük gecikmeden veya omurgaya bağlantıdan bağımsız olarak verilere esnek erişim sağlar. Zentachain, istisnasız olarak merkezsizdir ve ekosistemi, kullanıcılarını asla izlemeyecek ayrıca IP adresini veya kişisel bilgileri asla kaydetmeyecek şekilde tasarlamıştır. Tasarım gereği, ekosistem bu bilgilere sahip değildir ve işlemleri belirli bir kullanıcı veya kimlik ile eşleyemez.

Zentachain'in vizyonu büyük ölçüde iletişime dayanır. Zentachain üstün bir veri şifrelemesi kullanır ve iletişimde çoklu şifreleme uygulamaktadır. Zentalk, halihazırda bildiğiniz gibi yalnızca bir iletişim uygulaması olmayacak. Zentachain'in bu yönde bir hedefi bulunuyor ve çevrimdışı iletişim kurmanın zamanının geldiğinin farkındadır. Veri ve bilgilerinizle sözde ücretsiz uygulamalar için ödeme yaparken Zentachain, bugünün iletişim ve uygulamalarının aksine kullanıcıdan hiçbir kişisel bilgi istemez. Zentachain, ağı destekleyen kullanıcılara kendi kripto parası olan Zenta ile ödeme yapacaktır.

Güvenlik & İş

Zentacore ekosistemdeki tüm iş mantığını elinde tutmaktadır. ZentaMesh ağının yönetiminde çevrimdışı iletişim kabiliyeti mevcuttur - yöneten ve fikir birliği modelleri. Zentacore NPOS, BPOS, DPOS veya Blake2 gibi blockchain teknolojisinden birini kullanacaktır. Zentachain, bu tür bir teknoloji ve blok zincirini

kullanarak ölçeklenebilirliği büyük ölçüde geliştirecektir. Zentachain, ağdaki verilerin bölümlenmesini sağlayan bir tanık mekanizmasına sahiptir. Merkezileşme problemini çözmek için, her pay sahibi oy kullanır ve n-bit temsilcileri (genellikle n =101 olur), n değerine blok zincirdeki düğüm sayısı ile karar verilir. Düğüm sayısı arttıkça, = n değeri de artar ve: n düğüm temsilcileri aynı hakları paylaşır.

3. Zentachain'i mükemmel yapan nedir?

Zentachain, kullanıcılara ekosistem içerisinde Zentalk & Zentavault ile veri iletişimi ve saklama olanağı sağlar. Çalışan tüm merkezsiz uygulamalar anonim ve güvenli olacak, Zentachain'in yeteneklerini kanıtlamak ve göstermek için bir kullanıcı kaydı veya bağlantılı işlem gerektirmeyecek olup, ekip merkezsiz ve ultra güvenli bir mesajlaşma uygulaması sunmaktadır.

Zentalk

Zentalk ultra güvenlikli, hibrit ve şifreli merkezi olmayan eşler arası(P2P) bir meajlaşma uygulamasıdır. Kullanılabilirliğin yanı sıra, arka planda, AES-256, Diffie-Helman, RSA ve El-Gamal güvenliği ile modern şifreleme tekniklerini bulacaksınız. Zentalk merkezsizdir yani sunucu noktası yoktur. Zentachain, Blake2 hash fonksiyonu ve Tor-network'ü içeren Zentanode' ları kullanarak gönderici ile alıcı arasında tam anonimlik ve çevrimdışı iletişimi garanti eder.

Zentavault

Zentavault, yüksek verimli şifreli ve dağıtılmış bir dosya deposu(şifreli depolama) ve transfer hizmetidir. Normal veri depolama sistemlerinin aksine, Zentavault kullanıcının cihazında hiçbir şey depolamaz. Zentavault, İçeriklerarası Dosya Sistemi'ne (IPFS) güvenli bir şekilde içeriği şifreleyerek dinamik bir şekilde 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 sürüsü olarak görülebilir ve bir Git deposunda nesne alışverişinde bulunulabilir.

Zentagate

„ Zentamesh Ağına Geçit "
Zentachain, güvenliği ve anonimliği çok önemsemektedir. Zentachain'i kendi Zentamesh ağında çalışacak şekilde tasarladık. Zentagate, internet gibi Zentamesh ağlarını kullanmak için ekosisteme bağlanır. Zentagate, kullanıcının güvenli bir şekilde bağlanmasını ve korunmasını sağlamak için AES ve hack karşıtı katman tarafından ek şifreleme sağlamaktadır. Sınır koruması ve güvenli olmayan ağ geçişlerinin yanında, merkezi olmayan bir isim hizmeti de uygulamayı planlamaktayız.

Zentagate, Zentamesh ağı içindeki ve dışındaki verilerin ve işlemlerin, kullanıcının internet erişimi olmadan bağlantıda kalmasını sağlayan Zentanode' lar ile yönlendirilmesini sağlayan bu hizmeti çalıştıracaktır.

4. Zenta Ekonomisi

Zenta Dağıtımı:
Zincir Adı: ZENTA
Sembol: CHAIN
Algoritma: POS (Mainnet)
Zenta sayısı: 5.500.000

5. Çözmeye Değer Problem

Giderek daha fazla insanın, yaptığımız her şeyin bir bilgisayar sisteminde bir yere kaydedildiği ve bazı elektronik yollarla iletildiği bir çağda gizlilik konusunda endişeleri bulunmaktadır. Güvenli etkileşime ve dijital veri depolamasına olan gereksinim - kullanıcının izinsiz veri erişimi ve bilgi akışlarının manipülasyonuna uğrama tehlikesi her zaman olmuştur, ancak bu tehdit her geçen gün artmaktadır. Hackerlar şimdi size birçok ülke, farklı bölgeler ve aynı anda birden fazla yerden saldırabilir. Ve daha da kötüsünden bahsetmek gerekirse, verilerinizin kaydedilmesi, toplanması ve satılmasını sağlayarak para kazanan multi milyar dolarlık şirketler de bulunmaktadır.

Konum geçmişinizi, mesajlarınızı, fotoğraflarınızı, belgelerinizi ve hatta sizin için oluşturdukları profilleri dahi satarlar. Hakkınızdaki her şey bu verileri isteyen tüm dünyadaki yozlaşmış ve kötü niyetli organizasyonlara açık artırmaya hazır halde bulunur. Bazı telekomünikasyon şirketleri kullanıcı verileri ve işlemleri ile kazanç sağlayabilir. Bir düzenleme olsun veya olmasın ve her ne kadar bunları yapmamaları gerekiyorsa da, bunları yapmadıklarından emin olamayız. Çünkü belki de bu verileri bir gün sözde "eğitim amaçlı" kullanabilirler.

Bu verilerin uygun şekilde şifrelenmemesi veya anonimleştirilmemesi olasıdır. Sosyal medya şirketleri tarafından sunulan hizmetler ve mesajlaşma uygulamaları, tüketiciye hiçbir bedel ödenmeyen "ücretsiz bir hizmet" olarak kendilerini tanıtıyor. Aslında bu şirketler tüm bu verileri ve içerikleri çevrimiçi olarak depolamak ve manipülatif olduğu bilinen kötü niyetli kuruluşlara satmak için düzenli olarak çalışıyorlar. Bu, hizmet için aylık ücretler yapmak yerine veri yoluyla ödeme yapmanız anlamına gelir.

6. Veri Hackleri ve İhlalleri

İnternet kullanıcılarının sayısı hızla artıyor. (2007'de 1.36 milyar olan sayı son 10 yılda 2 milyardan fazla kullanıcı artışı ile 2017'de 3.57 milyara yükseldi) Günlük hayatımızın nasıl daha da sanallaştığını fark ediyoruz ve duygularımız, düşüncelerimiz ve kişisel bilgilerimiz çevrimiçi dünyaya giriyor ve bu veriler kişisel kazançları için elde etmek isteyen hırsızlara karşı savunmasız kalıyor.

Her şeyin ve herkesin hedef olabileceği bir noktaya geldik. Kimlik avı yoluyla yapılan kişisel saldırılar, ClickJacking, sosyal mühendislik ve diğer benzer teknikler ve hackerların büyük miktarlarda kişisel bilgilere erişme potansiyeli olan merkezi şirket veritabanlarındaki büyük çapta sızıntılar önemli derecede tehdit teşkil etmektedir. Bilgilerimizin bireysel yolla korunması, güvenli tarama uygulamalarının bilinçli bir şekilde kullanılmasıyla önlenebilir olsa da, etkilenen verilerin tam kapsamı nedeniyle büyük çaptaki veri hırsızlıkları asıl endişe kaynağıdır. Bu durumda verilerimizin güvenliğini sağlamak bizim kontrolümüz dışında kalır.

7. Gizlilik

Son yirmi yılda, çoğunlukla internetin günlük yaşamımız üzerindeki etkisi nedeniyle, bir bireyin gizlilik hakkını koruma konusundaki sorunlar fiziksel ortamdan dijital çevremize doğru genişlemiştir. Ünlü söz "Bilgi Güçtür", bugünün dünyasında "Veri Güçtür"e doğru evrildi; kişisel bilgilerimizi yalnızca bilgisayar korsanlarına ve kötü niyetli kişilere değil, aynı zamanda ''altın madeni'' olarak adlandırılan kuruluşlara da veriyoruz ve bu şirketler görünüşte yasalara uyan faaliyetlerde bulunuyor. Bir yandan kimliklerimiz, kredi kartı numaralarımız, dijital varlıklarımız vb. hedefleniyor, bir yandan da daha rahat bir kullanıcı deneyimi için bilgilerimizi kendimiz veriyoruz. Kullanıcıları korumak için Avrupa'nın Genel Veri Koruma Yönetmeliği (GDPR) gibi önlemler uygulanmasına rağmen, etkileri ve yürütme düzeyleri hala birçok soruyu gündeme getirmektedir.

Zayıf ve güçsüz ülke yönetimleri, kullanıcılarının verilerini toplayan bazı kötü niyetli şirketler tarafından üretilen uygulamalara izin vererek, bilgilerimizi tamamen kendi istedikleri şekilde kullanmalarına imkan tanıdı. Bu Tanıtım Belgesinin Veri İhlalleri bölümünde, en güncel gizlilik problemlerinden bazılarına değindik. Bu ve diğer benzer olaylar, ne yazık ki, halktan büyük tepkiler görmeden ortadan kayboluyor gibi görünüyor, ya da bazen kişilerarası iletişime zarar veren bir paranoya ve güvensizlik atmosferi yaratıyor. Bu nedenle, gizlilik haklarımızın farkında olmamız şarttır ve bu gizlilik sorunlarına çözüm olarak blockchain gibi yeni fikirlere odaklanmalıyız. Blockchain, kullanıcıların kişisel veri dağıtım araçlarını tam olarak kontrol etmeleri için gereken araçları sağlar. 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 verilerin istismar edilmesi ve manipülasyonuna karşı bağışıklık kazanır. Nihayetinde blockchain, kendisini dünyanın önde gelen işletmelerin sahip olduğu

acımasız para kazanma tutkusuyla kaybedilen güveni yeniden inşa etme potansiyeli olan bir platform olarak sunuyor.

8. Merkezi Mesajlaşma Uygulamaları

İnternetin günlük yaşamımızdaki varlığı arttıkça, daha verimli ve daha yaygın çevrimiçi iletişim araçlarına ihtiyaç duyuldu. Sonraki on yıl, özel mesajlar, çok kullanıcılı gruplar ve dosya paylaşımı dahil olmak üzere daha gelişmiş özellikleri bir araya getirmeye başlayan AIM, ICQ ve PowW gibi popüler mesajlaşma uygulamalarının ortaya çıkmasıyla daha farklı bir boyuta taşındı.

Son zamanlarda, mesajlaşma uygulamalarına olan ilgideki artış, akıllı telefon kullanımındaki artış ile doğrudan ilişkilidir. Masaüstü uygulamaları, hareket halinde iletişim kurmamızı sağlayan mobil sürümleri ile değiştirildi. Kullanıcı tabanı katlanarak büyüdü; WhatsApp, Facebook Messenger ve WeChat gibi lider servis sağlayıcılar, aylık 1 milyardan fazla aktif kullanıcıyı bir araya getirdi.

Ancak günümüzde mesajlaşma sistemleri kusursuz olmaktan uzaktır. Son olaylar, gizlilik sorunları hakkında ciddi soruları gün yüzüne çıkarmıştır. Facebook (en popüler iki mesajlaşma platformunun sahibi), siyasi amaçlarla kullanım için kullanıcı verilerini satma iddialarıyla karşı karşıya kaldı ve Blockchain alanındaki en popüler mesajlaşma uygulaması Telegram, mahkeme kararıyla sonuçlanacak iddiaya göre kullanıcılarının verilerini "ilgili makamlara ifşa etmeyi kabul etti." 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 kısıtlamalarını sağlar.

Günümüzdeki mesajlaşma programları, uçtan uca şifreleme çözümleri uygulayarak bu sorunu çözmeye çalışıyorlar, ancak yine de, bu kapalı kaynaklı uygulamalar, şifreleme kalitesi ve gerçekliği hakkında sorunları gündeme taşıyor. Günümüzün mesajlaşma uygulamalarının bir diğer zayıf yanı, SIM değişikliği saldırılarına karşı güvenlik açığı olmasıdır.

Çoğu uygulama kaydolmak için bir telefon numarası gerektirdiğinden, bilgisayar korsanları kurbanın numarasını kendi sahip oldukları bir SIM karta dönüştürmeye ikna ederek kullanıcının mesajlaşma içeriğine erişme şansını yakalayabilir.

9. Merkezi Cloud(Bulutlar)

Merkezi bulutlar, uzak sunucularda 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 bulutlar, kullanıcıya bir web arayüzü aracılığıyla bağlanabilen sanallaştırılmış veri merkezlerini kullanarak çalışır. Kullanıcı, dosyalarını internet üzerinden yükler ve ardından veri sunucularında depolar.

Kullanıcılara sadece benzersiz bir kimlik sağlar ve bu kimlikle dosyalarını görüntülemesine, düzenlemesine, aktarmasına veya senkronize etmesine izin verir. 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 ücret ödediği 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 bellidir.

Veri hareketliliği ve erişilebilirliğe yönelik artan talep, kullanıcıların HDD'ler ve USB flash sürücüler gibi fiziksel rakiplerinden uzaklaşmasına neden olmaktadır. Bununla birlikte, doğru atılmış bir adım olmasına rağmen, merkezi hizmetlerin hala sorunları bulunmaktadır. İlk olarak, müşteri veri sahibi değildir.

Merkezi sunucu mimarisi, müşterinin verilerini servis sağlayıcıların ellerine doğrudan teslim eder, veri erişim kesintilerinin olmasının yanı sıra veri erişiminin sürekliliğini kesintiye uğratabilecek DDoS saldırılarına karşı da savunmasız hale getirir. Genel Bulut hizmetleri, özellikle bulutun istemcilerinden biri aracılığıyla kötü niyetli izinsiz girişlere izin veren kaynak paylaşım bileşeni nedeniyle saldırılara maruz kalır.

Yasalar ve düzenlemeler bir başka önemli endişe kaynağıdır; veri güvenliği ve gizliliği, dünyanın farklı hükümetlerinin belirlediği ve sürekli değişen kurallara bağlıdır. Bulut üzerinde karmaşık veriler kullanmak isteyen daha küçük kuruluşlar için, maliyet açısından ciddi bir sorun olabilir, çünkü bant genişliği gereklilikleri finansal olarak zorluklar meydana getirebilir.

10. Zentachain Hakkında

Zentachain tüm bu sorunlar için uygulanabilir çözümler sunmaktadır. Açık kaynak, merkezi sunucularda depolanmayan içerik ve güvenliği en üst seviyeye çıkarmak için Zentameshnet, Hyperborea ve Tor-network gibi teknolojilerin entegrasyonu, bu platformda geliştirilen uygulamaları kullanmanın faydalarını açıkça göstermektedir. Zentachain, müşterilerin datalarını tamamen güvenli veri korumasıyla, ihlallere ve her türlü siber saldırılara karşı korumak için sabırsızlanmaktadır!
Bugün insanların kullandığı her hizmetin, perakendeciler ve kuruluşlara 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, hiçbir zaman meta verilerinizi müşterilerimizde tutmamaya söz verir ve IP adresinizi, e-postanızı veya telefon numaranızı kaydetmez. Hizmet kullanımında, alıcı ile gönderici arasındaki ödemeyi korumak için katman 2'ye sahip Zentawallet(Zentachain' in kendi cüzdanı) içeren Zentalk Uygulaması dışında hiçbir şey gerekmeyecektir. Tüm hizmetlerimizde olduğu gibi, Zentachain kimliğiniz, hangi bölgede yaşadığınız veya hakkınızdaki kişisel veriler ile ilgili hiçbir bilgiye sahip olmayacaktır. Zentachain bu kişisel etkileri umursamıyor çünkü tek hedefimiz tüketiciye mutlak anonimlik, güvenlik ve mahremiyet sağlayacak dünya standartlarında hizmetler sunmaktır. Zentachain'in bir diğer önemli yanı da, merkezi olmayan Zentalk App üzerinden çevrimdışı iletişim sağlamaktır.(İnternet bağlantısı gerekmeden iletişim imkanı sağlayacaktır) Zentalk, çoklu kripto şifrelemesiyle kuantum direncine sahip olacaktır.

11. Zentachain Ekosistemi

Zentachain ekosistemi, kendi değerini yüksek tutmak ve kullanıcıyı kendi blok zincirinde korumak için çoklu çözümlere ve de merkezi olmayan uygulamalara sahiptir. Zenta, Zentanode' lara sahip olan insanlar için bir ödül olarak kullanılacaktır. Zentanode sahipleri aylık olarak ödüllendirilecek, bu Zentamesh ağının başarılı olması için gereklidir. Madencilik sistemi ile aynıdır ancak daha enerji verimli ve kullanıcı dostudur. Zentalk, çoklu iletişim şifreleme kabiliyetleri ile modern iletişim için buradadır. Zentavault, veriyi şifreli ve güvenli bir şekilde saklayabilecek merkezi olmayan bir IPFS bulut depolama uygulamasıdır.

- **Anti-enflasyon**

Zentachain, anti-enflasyon sistemi ve gizlilik koruması ile inşa edilmiş merkezi olmayan bir ağdır. Bugün, iletişim uygulamalarının ve bulut depolamasının çoğu, kullanıcı verilerini ve daha birçok bilgiyi elde etmeyi kendilerine temel vizyon olarak belirlemiştir. Zentachain diğerlerinden farklıdır, Zentalk ve Zentavault kullanıcılarını ve destekçilerini ödüllendirir. Zentachain, hiçbir zaman kullanıcı verileri ve bilgileriyle var olmayacak, ürünleri, tamamen gizliliğe odaklanan iletişim sistemi ve yüksek verimli kendi blockchain'i ile yaşayacaktır.

- **Zenta Ödülü**

Zentachain, ağda bulunan tüm Zentanode ağlarını her ay ödüllendirecektir. Ağda hiçbir zorluk derecesi olmayacak ve Zenta'nın ödülleri sabit olacaktır. Bir kullanıcının yapması gereken tek şey Zentanode'u çalıştırmaktır. Eğer bir kullanıcı bağlantıyı keserse Zentanode artık Zenta ile ödüllendirilmeyecek olup, bu da kullanıcının Zentanode'u kalıcı olarak çalıştırması gerektiği anlamına geliyor.

- **Zentanode**

Zentachain Zentanode adındaki kendi node'larına sahip olacaktır. Zentanode bir düğümden farklı değildir, Zentamesh ağındaki bir cihaz veya veri noktasıdır. Zentanode' lar sadece resmi sitemizde satışa sunulacaktır. Zentanode' lar uzun bir çevrimdışı iletişim yelpazesine sahip olmak için oluşturulmuş olup, Zentanode' lardan elde edilen tüm gelirler Zenta Blockchain'i desteklemek için kullanılacaktır.

- **Zentalk**

Zentalk ultra güvenlikli, hibrit ve şifreli merkezi olmayan eşler arası(P2P) bir mesajlaşma uygulamasıdır. Zentalk uygulaması ilk önce ücretsiz ve tamamen açık kaynak olarak ortaya çıkmayacak.

- **Zentavault**

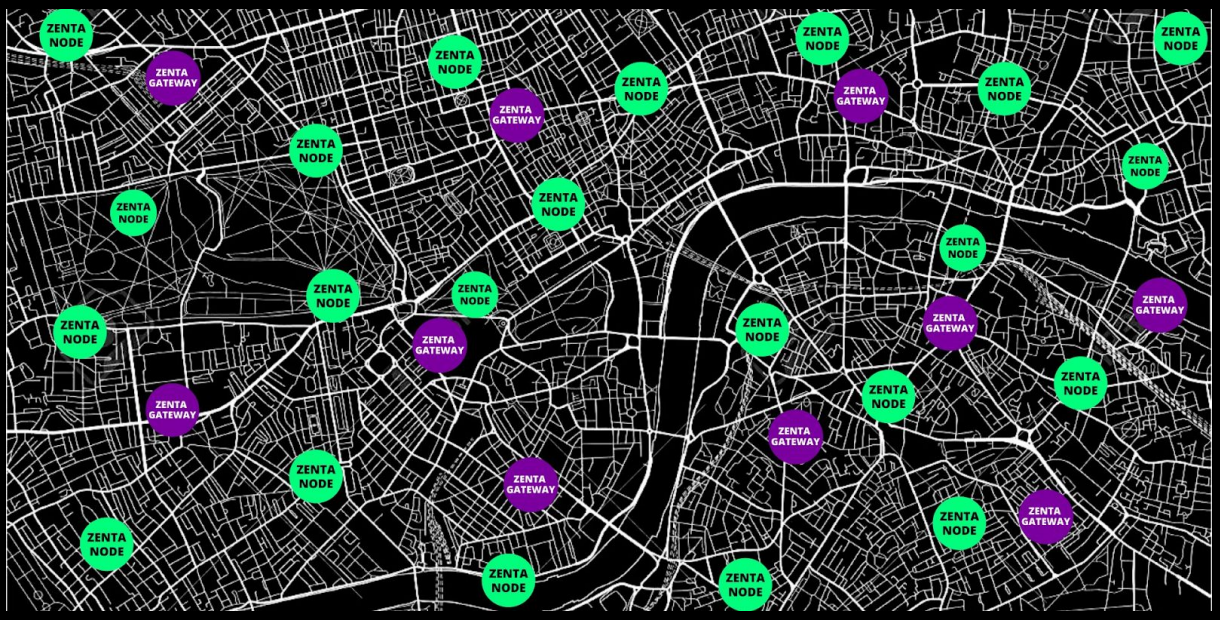
Zentavault aylık kullanım ücreti gerektirmez, bunun yerine veri yüklemek için yalnızca küçük bir işlem ücreti alınır. Zentavault bir dosya şifreleme ve dağıtım aracıdır.

12. İletişim

İletişim, iki kişinin birbirleriyle kolayca konuşabilmesi ve iletişim kurabilmesidir. Teknolojik platformlarda iletişim ilk önce telefonlarla sağlandı. Telefonlar tarihe büyük bir teknolojik gelişme olarak giriş yapmıştır, ancak teknolojinin hızı günden güne artmıştır ve bugün sayısız iletişim kaynağı mevcuttur. İlk zamanlarda, telefonlar gizliliğini ve özgürlüğünü koruyabiliyordu, ancak teknolojinin gelişimi bu süreyi kısalttı. Çünkü iki insan arasındaki iletişim ve konuşmalar başkaları

tarafından dinlenmeye başlandı. Bu nedenle, insanların mahremiyeti artık yok olmaya başladı. Ancak, yeni teknolojiler her geçen gün ortaya çıktıkça, insanların özgürlüğü ve gizliliği yeniden korunmaya çalışılıyor, ancak henüz bu tam olarak sağlanamadı. Çünkü bugün tüm konuşmalar ve yazışmalar bir şekilde birileri tarafından takip ediliyor. Ve ne yazık ki, konuşmamızın sadece karşı taraf ile aramızda kaldığını düşünmemize rağmen, telefonda ya da herhangi bir iletişim cihazıyla konuşurken durum gerçekte böyle değil.

13. Zentalk



Zentalk ultra güvenlikli, hibrit ve şifreli merkezi olmayan eşler arası(P2P) bir mesajlaşma uygulamasıdır. Zentalk, gizlilik ve güvenliğini Zentamesh ağ teknolojilerinin entegrasyonuyla sağlamaktadır. Zentamesh Ağı (Zentameshnet), mevcut en güvenli ve en güvenilir ağ varyasyonlarından biri olarak bilinir. Zentamesh Network teknolojisi güçlüdür, mükemmel yük dağılımına sahiptir ve sıfır merkezi yönetim içerir.

Zentamesh ağı, her bir düğümün ağ için veri aktardığı bir ağ topolojisidir. Zentachain .cjdns-, adres tahsisi için ortak anahtar şifrelemesi ve yönlendirme için dağıtılmış bir hash tablosu kullanarak şifreli bir IPv6 ağı uygular. Yapılandırmaya gerek yoktur ve mevcut ağları rahatsız eden birçok güvenlik ve ölçeklenebilirlik sorununu çözer. Tüm Zentamesh node' ları ağdaki verilerin dağıtımında işbirliği yapar. Zentalk kullanan her cihaz, Zentamesh ağında bir düğüm olarak görev yapar. Bu düğümler, dağıtılmış bir şekilde birbirleriyle bağlantı kurma özelliğine sahiptir.

Zentamesh ağı, bir sel tekniği veya bir yönlendirme tekniği kullanarak mesajları iletir. Yönlendirme ile, mesaj, hedefine ulaşana kadar bir Zentanode'dan diğerine atlayarak yol boyunca mesafe kateder. Tüm yollarının kullanılabilirliğini sağlamak

için ağ, ‘En Kısa Yol Köprüleme’ gibi kendi kendini iyileştirme algoritmaları kullanarak bağlantının sürekliliğine imkan verir ve bozuk yada arızalı yollar kendini yeniden yapılandırır. Kendi kendini iyileştirme, bir Zentanode bozulduğunda veya bir bağlantı güvenilmez olduğunda yönlendirme tabanlı bir ağın çalışmasına izin verir. Sonuç olarak, ağ kesinlikle güvenilirdir, çünkü Zentamesh ağındaki bir kaynak ve bir hedef arasında genellikle birden fazla yol vardır. Çoğunlukla kablosuz durumlarda kullanılsa da, bu kavram kablolu ağlara ve yazılım etkileşimine de uygulanabilir.

Gündelik yaşamda kullanılan yaygın örgü ağ teknolojilerine bir örnek kablosuz domotika (Z-dalga protokolü gibi) olabilir. Evinize yeni bir Zentanode kaydederseniz ve bunu yeni bir ampul gibi düşünürseniz, cihaz kontrol merkezi ile kendiliğinden konfigüre edilmiş ağ üzerinden eşleşir. Yaygın mesh ağları genelde kablosuzdur, ancak Zentamesh blockchain tabanlı bir ağ topolojisidir ve daha az alt yapısı mevcuttur.

Zentalk teknolojik gizlilik sağlar, bu sadece yüksek oranda şifrelenmiş Meta Verilerin kısa süre tutulduğu ve daha sonra otomatik olarak kurtarılamaz şekilde yok edildiği anlamına gelir. Bu, Zentamesh ağının ve mimarisinin entegrasyonu ile sağlanır. Zentalk, tüm mesajları ve verileri Zentamesh ağı üzerinden gönderir ve tüneller. Bu, gönderen ve alıcı arasında paylaşılan iletilerin gizliliğinin en üst düzeyde olmasını sağlar.

Zentamesh ağında, her Zentanode bir veya birden fazla düğüme bağlanır. Zentalk'ten bir mesaj gönderildiğinde ve veriler Zentamesh ağı üzerinden gönderildiğinde, mesaj istenen alıcıya ulaşana kadar bir Zentanode'dan diğerine geçer. Zentamesh ağındaki düğümlerin tasarımı sayesinde hangi düğümün hangi mesajı gönderdiğini ya da hangi mesajı aldığını bilmiyoruz. Bu, gönderen ile alıcı arasındaki iletişim için anonim olarak kalır. Zentalk kullanıcıları sadece tek bir mesaj ileterek ödüllendirilmeyeceklerdir. Zentanode sahipleri Zenta ile ödüllendirilecektir. Bu, bir Zentanode sahibi olmanız ve sürekli olarak çalıştırmanız gerektiği anlamına gelir; bu da çok enerji tasarruflu ve kullanışlıdır. Zentalk, ultra güvenli, şifreli bir mesajlaşma uygulamasıdır ayrıca ağın içindeki ve dışındaki her mesaj, Zentalk kullanıcısının gizliliği için istese de herhangi bir hata yapamayacak şekilde tasarlanmıştır. Zentalk ayrıca, kullanıcıların başka kullanıcılara saldırmasına veya herhangi bir saldırıya açık hale gelmesine neden olabilecek bir boşluk bırakmayacaktır. Zentalk farklı şifreleme türleri kullanacaktır, çünkü bazı şifreleme metodları korumasızdır, Zentalk için yalnızca güvenli olanları kullanacağız. Her şifrelemenin kendi rolü olacaktır ve kullandığımız tüm şifreler whitepaper' da listelenecektir. Zentalk, kuantum bilgisayar saldırılarına karşı gerçekten güvenli olan şifreleri kullanacaktır.

Zentalk Özellikleri:

- Zentalk, Google Play hizmetlerini gerektirmemektedir.

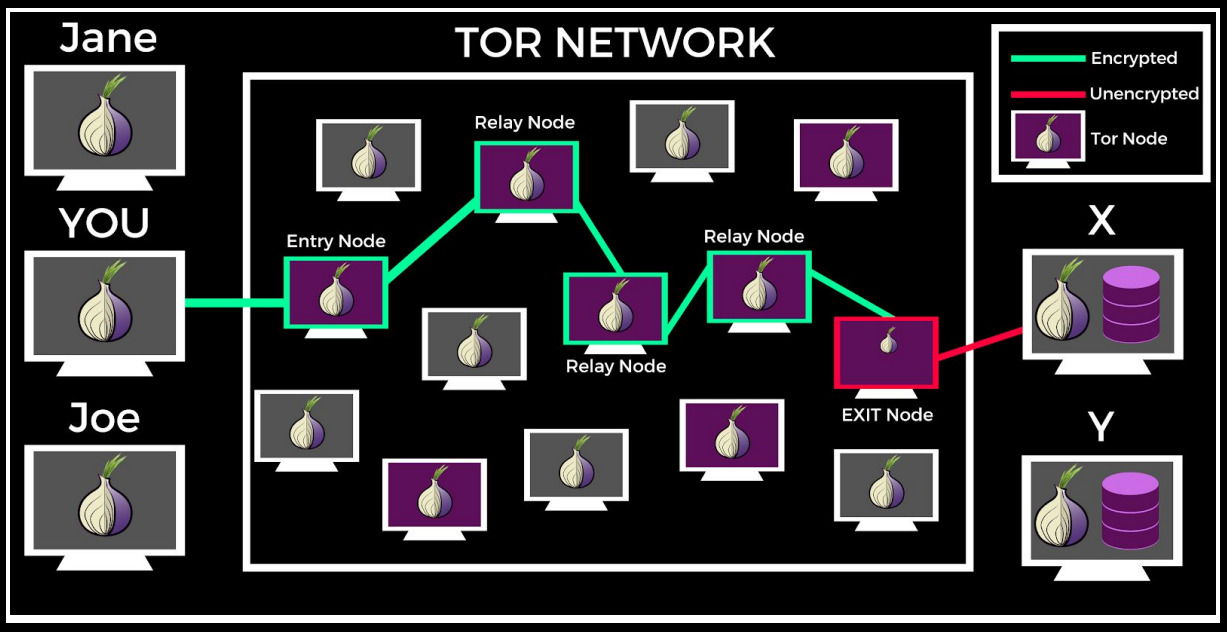
- Kişisel bilgi: Hayır
- Sunucu / Bulut Sunucuya sahip mi : Hayır
- IP Adresleri korunuyor: Evet, Tor-Network ile
- Mesajlar herhangi bir sunucuda saklanıyor mu : Asla
- Mesajlar kendi cihazında şifrelenmektedir: Evet
- Veriler kullanıcının kendi cihazlarında şifrelenir: Evet
- Kullanıcı hesabını kurtarma: Hayır
- Yedekleme: Hayır
- Çevrimdışı(İnternetsiz kullanım): Evet
- Google Takip edebilir mi: Hayır
- Veri Desteği: Evet
- Telefon Numarası: Hayır
- E-mail: Hayır
- Kayıt: Hayır
- Üçüncü kişi saldırısından koruma sağlar: Evet
- Grup Konuşması: Evet
- Anahtar Paylaşımı: Evet
- Haber paylaşımı: Evet
- Zentawallet: İlk başta Hayır /Sonradan Evet Konuşma & Ödeme (Sadece: Bitcoin, Ethereum, Zenta)
- Zentamesh ağı üzerinden Bitcoin ödemesi : Evet
- Tor Yönlendirme ile Bitcoin Ödemesi : Evet
- Zenta Ödülü: Evet (Zentanode sahibi olursanız)
- Hash-Algoritmaları: BLAKE2b
- Zentanode Hash-Algoritmaları: SHA-256
- Hibrit Şifreleme: Evet(RSA, AES, DHKE, EL-Gamal)
- Blok Anahtar Şifrelemesi: 128 Bit
- Anahtar Genişliği: 256 Bit
- RSS: Evet
- API: Evet
- Özel Node’ lar: Evet
- Özel Geçit(Gateway): Evet
- Zentanode Şifrelemesi: Evet
- Onion-Share: Evet
- Quantum dayanıklılığı: Evet
- Mesajları okuduktan sonra yok etme: Evet
- Tek Yönlü hash şifre imzası: Evet
- Diğer Uygulamalar Tarafından Takibi Durdur : Evet
- SIM Kart olmadan kullanma: Evet
- Bluetooth veya Wi-fi menzili içindeki Zentalk kullanıcısı, internet'e erişimi olmasa bile diğer cihazlar ve Zentanode üzerinden diğer kullanıcılarla iletişim sağlayabilir.

Birçok yeni özellik eklenmeye devam edecektir.

14. Zentalk & Tor Ağı

Tor anonim iletişimi sağlamak için kullanılan ücretsiz ve açık kaynaklı bir yazılımdır. Bu isim , orijinal yazılım proje adı "The Onion Router" ın kısaltmasından türetilmiştir. Tor, bir kullanıcının internet trafiğini ve yerini, ağ gözetimi veya trafik analizi yapan herhangi birinden gizlemek için 7000' den fazla röleden oluşan ücretsiz bir gönüllü ağ üzerinden yönlendirir. Tor kullanmak, kullanıcının internet aktivitelerinin izlenmesini daha da zorlaştırır: buna "Web siteleri, çevrimiçi mesajlar, anlık mesajlar ve diğer iletişim formlarını ziyaret" dahildir. Bununla birlikte, dünyanın çeşitli ülkelerindeki İnternet Servis Sağlayıcıları (ISS), kullanıcıların Tor'lara erişimini engellemek için genellikle hükümetleri tarafından ikaz edilir. Sonuç olarak, bu tür erişimin engellendiği ülkelerde kullanıcıların Tor ağına bağlanmasını sağlamak için Tor köprüleri geliştirilmiştir. Köprü rölelerinin bazılarını gizli tutarak, kullanıcılar genel Tor rölelerini engellemeye dayanan internet sansüründen kaçabilirler. Tor, bir çevrimiçi hizmetin Tor üzerinden ne zaman erişileceğini belirlemesini engellemez. Tor, kullanıcının gizliliğini korur ancak birinin Tor kullandığı gerçeğini gizlemez. Ancak köprüler, bir kişinin Tor kullandığı gerçeğini de gizler. Tor'un amacı, kullanıcılarının kişisel gizliliğinin yanı sıra, internet etkinliklerini izlenmekten koruyarak gizli iletişim kurma özgürlük ve yeteneklerini korumaktır. Bir kullanıcı Tor kullandığında, çevrimiçi veri toplayıcıları trafik analizi yapamaz ve kullanıcının Google Reklamları gibi internet alışkanlıklarına ilişkin verileri toplayamaz. Dolayısıyla, NSA gibi gözetim kuruluşları kullanıcıları gözlemleyemez. Tor, verileri birçok kez şifreler ve rastgele seçilen Tor röleleri, hedef IP adresi de dahil olmak üzere art arda oluşan sanal bir devre üzerinden gönderir. Bu nedenle, Zentalk mesajlaşma uygulamasını geliştirirken, kullanıcının mahremiyetini ve özgürlüğünü göz önünde bulundurduk. Zentalk, Tor protokolü sayesinde iletişimin tam anonimliğini garanti eder. Kullanıcılar, ikinci bir VPN sağlayıcısı veya Orbot kurmadan Zentalk'u kolayca açıp kapatabilecektir.

Tor-Ağı



15. Zentalk & Algoritma & Şifreleme

Kriptografi

Kriptografi veya kriptoloji, saldırgan olarak adlandırılan üçüncü tarafların arasında güvenli iletişim için bazı tekniklerin uygulanması ve incelenmesidir. Daha genel olarak, şifreleme, üçüncü tarafların bireylere ait özel mesajları okumasını engelleyen protokoller oluşturmak ve analiz etmekle ilgilidir;bilgi gizliliği, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliğinin çeşitli yönleri modern şifreleme için önemlidir. Modern şifreleme, matematik, bilgisayar bilimi, iletişim bilimleri disiplinlerinin kesişme noktasında bulunmaktadır. Şifreleme uygulamaları arasında elektronik ticaret, çip tabanlı ödeme kartları, dijital para birimleri, bilgisayar şifreleri ve askeri iletişim bulunur.

Şifrelemenin Tarihi

MÖ 600 dolaylarında: Spartalılar savaş sırasında gizli mesajlar göndermek için tırpan denilen bir cihaz kullandılar. Bu, tahta bir çubuğun etrafına sarılmış bir deri kayıştan oluşur. Deri şeridin üzerindeki harfler, açılmadığında anlamsızdır ve yalnızca alıcı doğru boyutta bir çubuğa sahipse, mesaj anlamlıdır.

60 M.Ö : Jül Sezar, karakterleri üç yerden değiştiren bir şifre icat eder: A, D, B, E, vb.

1553: Giovan Battista Bellaso, alıcının mesajın kodunu çözebilmesi için bilmesi gereken, -ortak kabul edilmiş- uygun bir şifreleme anahtar kelimesini kullanan ilk şifrelemeyi öngördü.

1854: Charles Wheatstone, tek olanlar yerine harf çiftlerini şifreleyen ve kırılması daha zor olan Playfair Şifrelemeyi icat etti.

1917: Bir Amerikalı, Edward Hebern, anahtarın dönen bir diske yerleştirildiği elektro-mekanik bir makine icat etti. Bir rotor makinesinin ilk örneğidir. Her yeni karakter yazıldığında değiştirilen bir tabloyu kodlamaktadır.

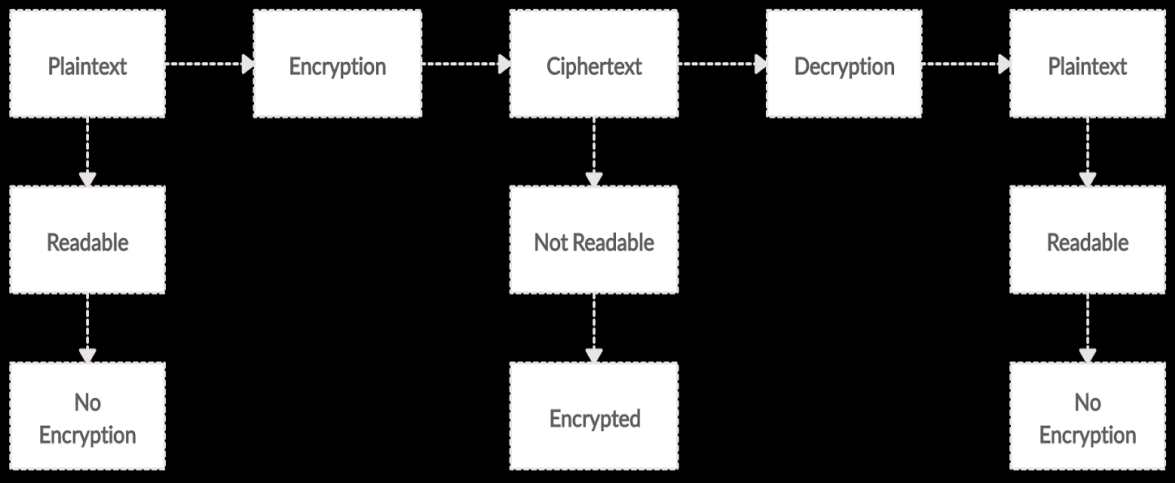
1918: Alman mühendis Arthur Scherbius Enigma makinesini ticari kullanım için icat etti. Hebern'in makinesi tarafından kullanılan bir rotordan çok, birkaçını kullanmaktadır. Dahisini tanıyan Alman ordusu bunu şifreli yayınlar göndermek için de kullanmaya başladı.

1932: Polonyalı kriptograf Marian Rejewski, Enigma'nın nasıl çalıştığını keşfetti. 1939'da Polonya bu bilgiyi Fransız ve İngiliz istihbarat servisleriyle paylaştı ve Alan Turing gibi kriptografların günlük olarak değişen anahtarı nasıl çözeceklerini bulmalarını sağladı. II. Dünya Savaşının kazanılmasında çok önemli rol oynadı.

1945: Bell Labs'dan Claude E. Shannon, "Kriptografinin matematiksel bir teorisi" adlı bir makale yayınlar. Bu modern şifrelemenin başlangıç noktasıdır.

Early 1970s: IBM, şirketin verilerini korumak için blok şifre tasarlayan bir 'şifreleme grubu' oluşturur. 1973'te ABD, bunu ulusal bir standart olarak kabul etti - Veri Şifreleme Standardı veya DES. 1997'de kırılana kadar kullanımda kaldı.

2000: DES, halka açık bir yarışmada bulunan Gelişmiş Şifreleme Standardı (AES) ile değiştirildi. Bugün, AES dünya çapında telifsizdir ve ABD hükümeti tarafından kullanılması onaylanmıştır.

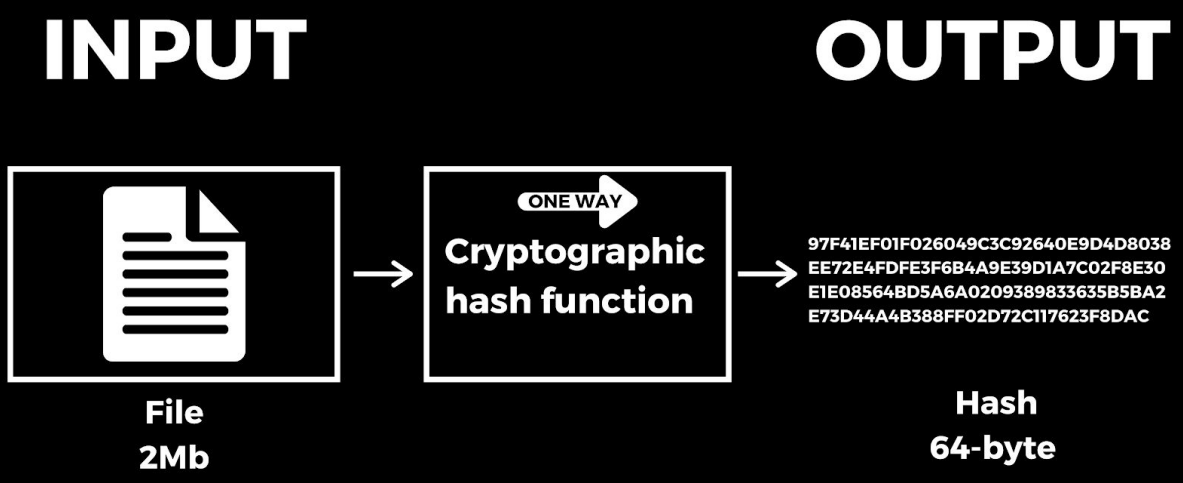


Hash Fonksiyonları

Hash fonksiyonları, modern şifreleme için yapı taşlarıdır. Bir hash fonksiyonu, rastgele boyutlu büyük verileri küçük sabit boyutlu verilere dönüştürmek için kullanılan bir şifreleme algoritmasıdır. Hash algoritmasının veri çıktısına hash değeri veya özet adı(digest) verilir. Hash fonksiyonların temel çalışma prensibi herhangi bir tuşa ihtiyaç duymaz ve tek yönlü çalışır. Tek yönlü işlem, girişi belli olan bir çıktıdan hesaplanması mümkün olmayan anlamına gelmektedir.

- Bir hash fonksiyonunun döndürdüğü değerlere hash değerleri denir.
- Kriptografik bir hash işlevi, bazı girdi verilerinin belirli bir hash değeri ile eşlendiğini kolayca doğrulayabilmenizi sağlar.
- Hash fonksiyonu, isteğe bağlı boyuttaki verileri sabit boyuttaki verilerle eşleştirmek için kullanılabilen bir işlevdir.
- Girdi verileri bilinmiyorsa, kaydedilen hash değerini bilerek yeniden oluşturmak zordur.
- Hash fonksiyonunun bir anahtarı yoktur.
- Uzun süreli güvenlik için 256 bit veya daha fazlası önerilir.
- SHA-1'in ciddi zayıf noktaları vardır o yüzden mümkünse kullanılmamalıdır.
- SHA-2 algoritmaları henüz kırılamamamıştır, ancak SHA-1 ile aynı prensibe göre çalışmaktadır.
- SHA256 / 512 Blake2b hash fonksiyonu ve diğerleri daha güvenli kabul edilir. (Gelecek 20-30 Yıl içinde kuantum direncine sahiptirler)

Hash-Fonksiyonu



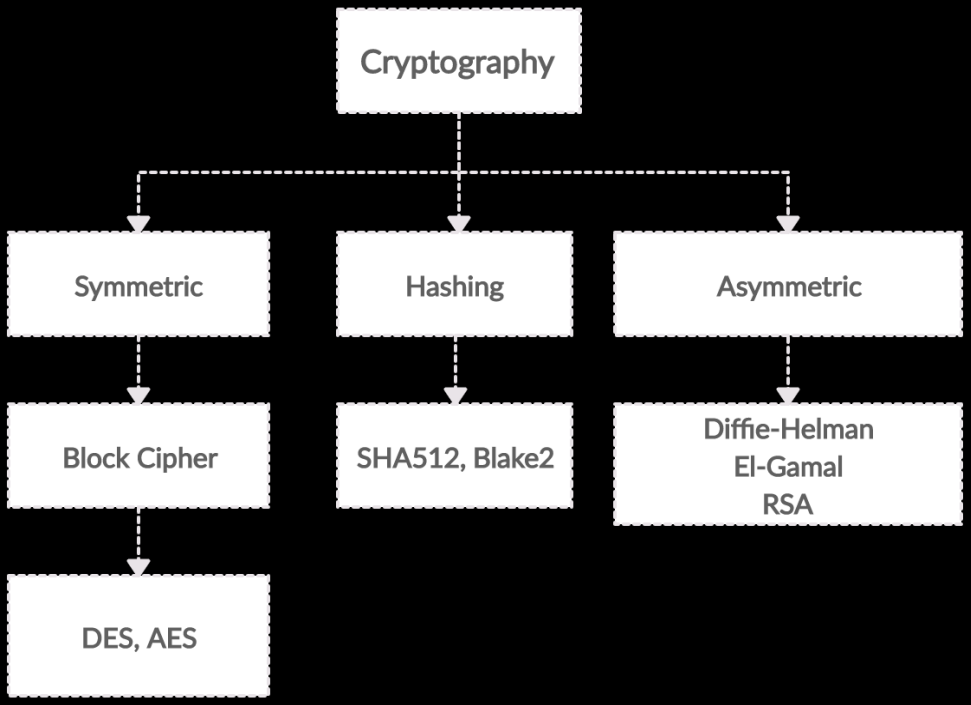
Şifreleme

Şifreleme, metnin veya başka herhangi bir veri türünün okunabilir bir formdan, başka bir varlık (yalnızca şifreyi çözme anahtarına erişimi olan bir kişi) tarafından çözülebilen şifreli bir sürüme dönüştürüldüğü yöntemdir. Şifreleme, özellikle ağlar arasında iletilen verilerin uçtan uca korunması için veri güvenliği sağlamada en önemli yöntemlerden biridir.

Şifreleme, bir tarayıcı ile bir sunucu arasında, şifreler ve diğer kişisel bilgiler dahil olmak üzere, gönderilen kullanıcı bilgilerini korumak için internette yaygın olarak kullanılır. Organizasyonlar ve bireyler ayrıca, bilgisayarlarda, sunucularda, telefonlar veya tabletler gibi mobil aygıtlarda depolanan hassas verileri korumak için yaygın olarak şifreleme kullanır.

Şifreleme nasıl çalışır

Şifreleme, bilgilerinizi korumak için algoritmalar kullanır. Ve sonra mesaj, mesajı bir anahtarla çözebilen alıcı tarafına iletilir. Her biri farklı karıştırma ve daha sonra bilgilerin şifresini çözme yöntemlerini içeren birçok algoritma türü vardır. Günümüzde yaygın olarak kullanılan şifreleme algoritmaları üç bölüme ayrılır: Hash Fonksiyonlar, simetrik, asimetrik.



Blok Şifresi

Bir blok şifresi, bir düz metin bit bloğunu alır ve genellikle aynı boyutta bir şifre metin bit bloğu oluşturur. Bloğun büyüklüğü verilen şemada sabittir. Blok büyüklüğün seçimi, şifreleme düzeninin gücünü doğrudan etkilemez. Şifrenin gücü anahtarın uzunluğuna bağlıdır.

Blok Şifre Şemaları:

- Kullanımda olan çok sayıda blok şifre şeması var. Birçoğu herkes tarafından bilinir. En popüler ve seçkin blok şifreler aşağıda listelenmiştir.

- Üçlü DES - Tekrarlanan DES uygulamalarına dayanan değişken bir şemadır. Hala saygın bir blok şifresidir, ancak mevcut olan daha hızlı blok şifrelere göre daha verimsizdir.

- Gelişmiş Şifreleme Standardı (AES) - AES tasarım yarışmasını kazanan Rijndael şifreleme algoritmasına dayanan nispeten yeni bir blok şifredir.

- IDEA - 64 bitlik blok büyüklüğünde ve 128 bit anahtar boyutunda yeterince güçlü bir blok şifresidir. Pretty Good Privacy (PGP) protokolünün erken sürümleri de dahil olmak üzere bir dizi uygulama IDEA şifrelemesi kullanmaktadır. IDEA programının kullanımının, patent sorunları nedeniyle sınırlı bir kabulü vardır.

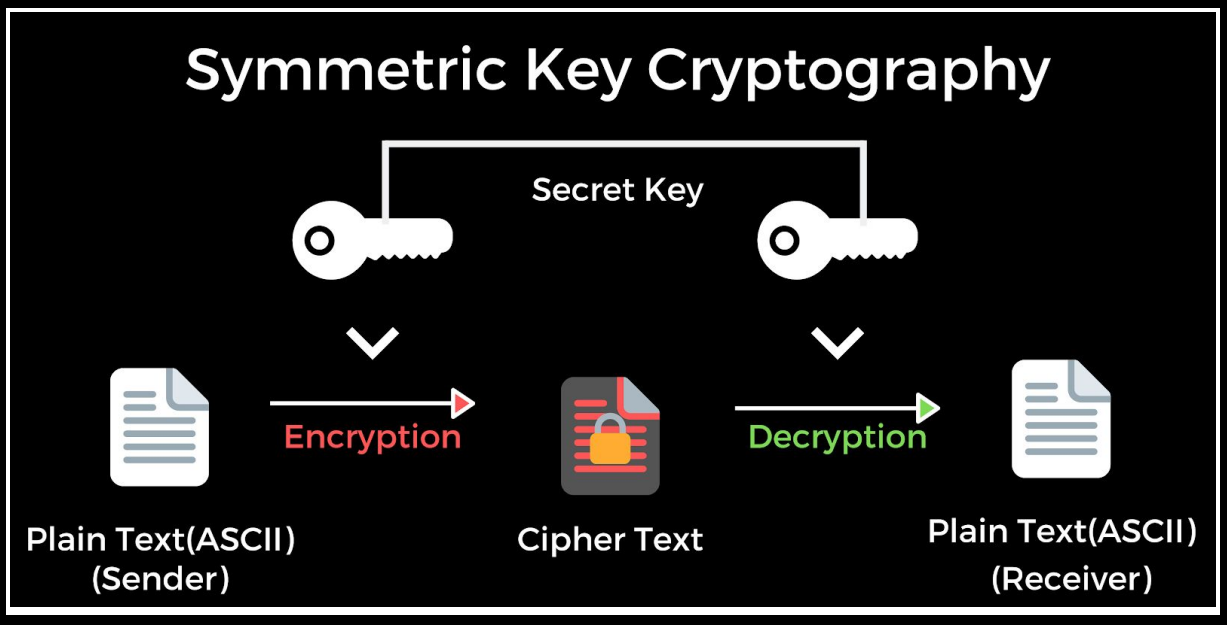
- Twofish - Bu blok şifre şeması, 128 bitlik bir blok büyüklükte ve değişken uzunluklu bir anahtar kullanır. AES finalistlerinden biriydi. 64 bitlik bir blok büyüklüğüne sahip olan önceki blok şifre Blowfish'ine dayanmaktadır.

- Serpent - Ayrıca AES yarışmasının finalisti olan, 128 bitlik bir blok büyüklüğüne ve 128, 192 ve 256 bit anahtar uzunluklarına sahip olan bir blok şifredir. Daha yavaştır ancak diğer blok şifrelere göre daha güvenli bir tasarıma sahiptir.

Simetrik Şifreleme

Simetrik şifreleme, elektronik bilgileri hem şifrelemek hem de şifresini çözmek için yalnızca bir anahtarın (gizli anahtar) kullanıldığı bir şifreleme türüdür. Simetrik şifreleme yoluyla iletişim kuran varlıklar, şifre çözme işleminde kullanılabilecek şekilde anahtarı değiştirmelidir. Bu şifreleme yöntemi, biri genel ve biri özel olan bir çift anahtarın mesajları şifrelemek ve şifresini çözmek için kullanıldığı asimetrik şifrelemeden farklıdır. AES (Gelişmiş Şifreleme Standardı) en çok kullanılan simetrik şifreleme algoritmalarından biridir.

Simetrik



AES Şifreleme

En yaygın kullanılan simetrik algoritma, aslen Rijndael olarak bilinen AES'tir. (Gelişmiş Şifreleme Standardı) ABD FIPS PUB 197'de açıklanan elektronik verilerin şifrelenmesi için 2001 yılında ABD Ulusal Standartlar ve Teknoloji Enstitüsü tarafından belirlenen standarttır. Bu standart, 1977'den beri kullanılmakta olan DES'in yerine geçmiştir. AES şifresi, 128 bitlik bir blok boyutuna sahiptir, ancak gösterildiği gibi üç farklı anahtar uzunluğuna sahip olabilir:

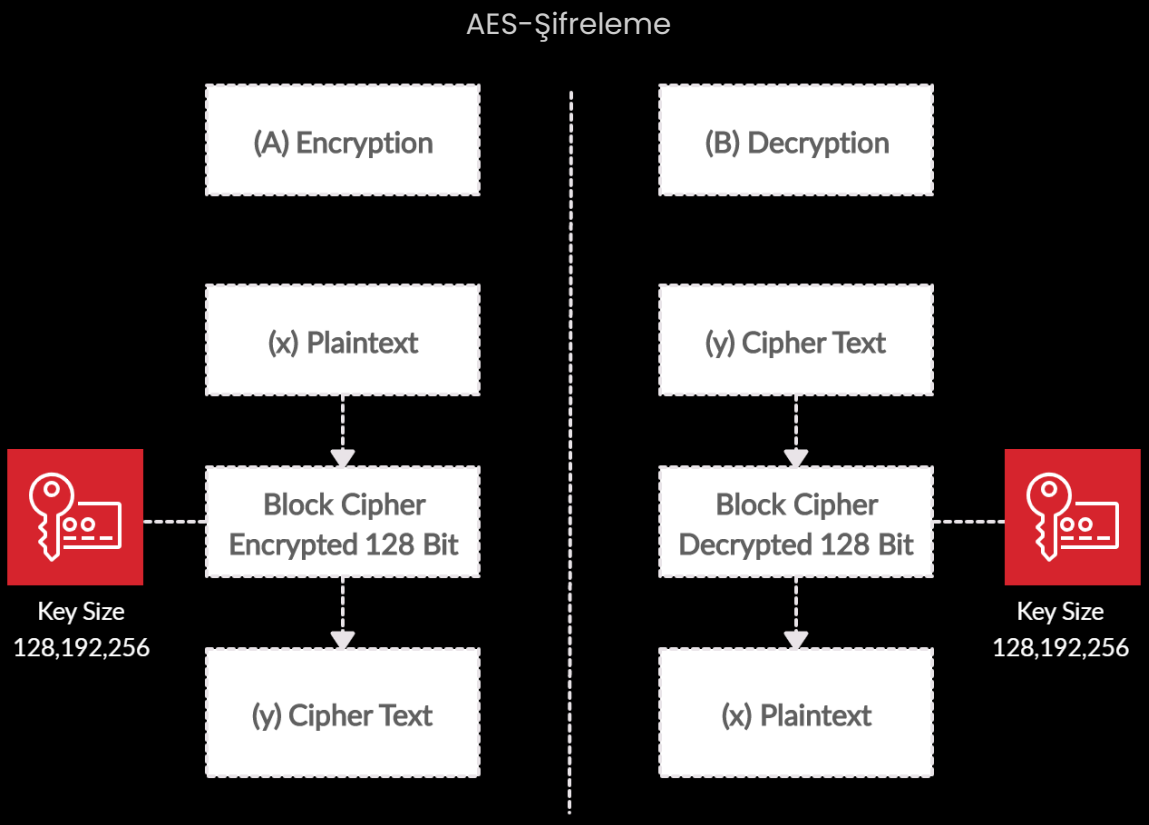
- AES - 128 Bit - (K)
- AES - 192 Bit - (K)
- AES - 256 Bit - (K)

Anahtar uzunluklarına göre tur -round (R) sayıları:

- 128 Bit = 10 (R)
- 192 Bit = 12 (R)
- 256 Bit = 14 (R)

1. Bugüne kadar AES şifrelemesinde hiçbir başarılı saldırı yoktur.
2. AES, yazılım ve donanımda çok verimli bir şekilde uygulanabilir.
3. Brute force saldırılarına karşı çok iyi ve uzun vadeli güvenlik sunar.
4. AES, 1990'ların sonlarından bu yana yoğun bir şekilde kullanılmaktadır.
5. Uygulamada, AES ile çoklu şifreleme yapmanın bir nedeni yoktur (DES bugün ayrıca TDES veya 3DES olarak da adlandırılan çoklu anahtar şifrelemeye ihtiyaç duyar).
6. Aynı gizli anahtar şifreleme ve şifre çözme için kullanılır.

7. Alice ve Bob her ikisi de aynı şifreleme yeteneklerine sahiptir, çünkü ikisi de aynı anahtara sahiptir, böylece Alice'in yapabileceği tüm eylemler (şifreleme ve şifre çözme gibi) Bob tarafından da yapılabilir.
8. Daha fazla tur daha güvenli bir sistem sağlar. Ancak aynı zamanda, daha fazla tur verimsiz, yavaş şifreleme ve şifre çözme işlemleri anlamına gelir.
9. 3DES' den daha güçlü ve daha hızlıdır.
10. C ve Java'da uygulanabilir bir yazılımdır.



AES ile anahtar değişimi sorunu

Simetrik anahtar (A) Alice ve (B) Bob arasında güvenli bir kanal üzerinden değiştirilmelidir. Bu nedenle, anahtar doğrudan en uygun yol olan normal bir bağlantı üzerinden gönderilemez ve farklı bir iletim şekli gerekir. 1000 çalışanı olan bir şirket gibi orta ölçekli ağlar için bile, güvenli bir kanal üzerinden üretilmesi ve değiştirilmesi gereken 2 milyondan fazla anahtara ihtiyaç vardır.

- E-ticaret uygulamalarında, Alice'in bir Zentanode siparişi vermek gibi belirli bir mesaj gönderdiğini kanıtlamak genellikle önemlidir.
- Sadece simetrik kriptografi kullanırsak ve Alice daha sonra satın alma konusundaki fikrini değiştirirse, her zaman Bob'un (satıcının) siparişi yanlışlıkla yarattığını iddia edebilir. Bunu önlemek "geri göndermeme"

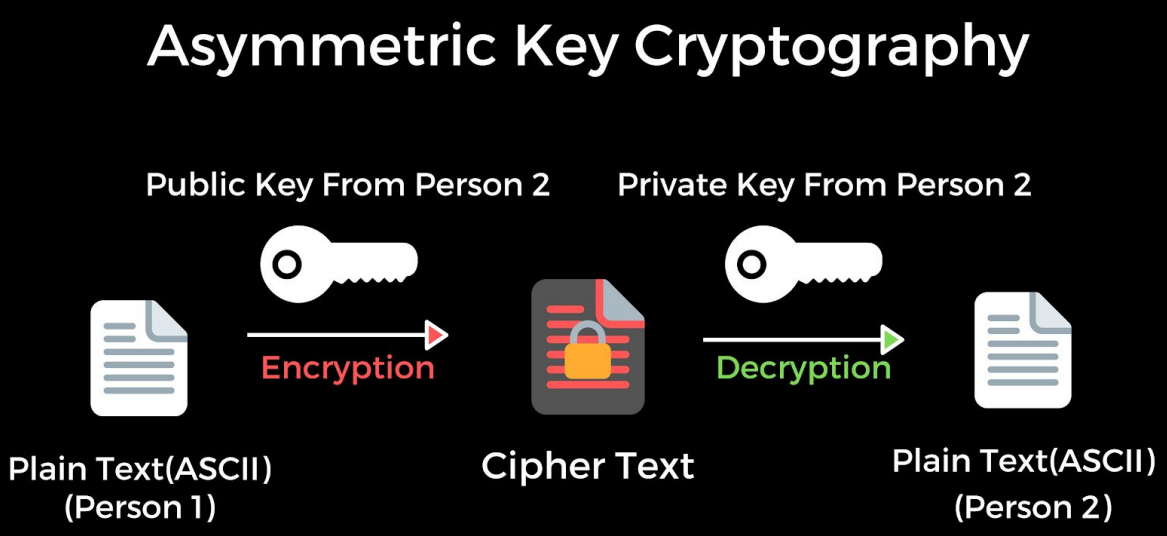
olarak adlandırılır ve asimetrik kriptografi (DHKE, El-Gamal, RSA) ile sağlanabilir.

Asimetrik Şifreleme

Açık anahtarlı şifreleme olarak da bilinen asimetrik şifreleme, biri genel diğeri özel olmak üzere iki farklı, ancak matematiksel olarak birbirine bağlı anahtar kullanır. Açık anahtar herkesle paylaşılabilir, ancak özel anahtarın gizli tutulması gerekir. RSA şifreleme algoritması, en yaygın kullanılan ortak anahtar algoritmasıdır, çünkü kısmen hem genel hem de özel anahtarlar bir mesajı şifreleyebilir; Bir mesajı şifrelemek için kullanılan zıt anahtarı, şifresini çözmek için kullanılır. Bu özellik, yalnızca gizlilik değil, aynı zamanda dijital imzaların kullanımı yoluyla elektronik haberleşme ve verilerin bütünlüğünü, güvenilirliğini aynı zamanda hesaplanamazlığını garanti altına almak için bir yöntem sunar.

- Asimetrik şifreleme, günümüzde birçok güvenlik uygulaması için arzu edilen bir araçtır.
- Asimetrik şifreleme Açık Anahtar Şifreleme (PKC) çalışma serisinde ele alınmaktadır.
- Tek yönlü fonksiyonlara da dayanan asimetrik algoritmalar vardır.
- Tek kullanımlık fonksiyonları olan sınıflar özellikle ilgilenmektedir: Hash ve kod tabanlı.
- Asimetrik algoritmalar, simetrik algoritmaların bilhassa güvenli olmayan kanallar ve dijital imzalar aracılığıyla anahtar değişimine olanak tanımadığı fırsatlar sunar.
- Yaklaşık 2005'ten bu yana “bilimsel” çalışmalarda asimetrik prosedürlere daha fazla ilgi duyulmaktadır.
- Bu yöntemlere duyulan ilgi için temel bir motivasyon, şu ana kadar asimetrik algoritmalara karşı kuantum bilgisayarlara dayalı hiçbir saldırı olmamasıdır.
- AES veya 3DES (TDES) gibi algoritmalardan çok daha yavaştır, bunun nedeni RSA'nın (ve diğer tüm asimetrik algoritmalar) gerektirdiği yüksek hesaplama çabasıdır.

Asimetrik



Rivest–Shamir–Adleman Şifreleme (RSA)

RSA (Rivest-Shamir – Adleman) ilk halka açık şifreleme sistemlerinden biridir ve güvenli veri iletimi için yaygın olarak kullanılmaktadır. Böyle bir şifreleme sisteminde, şifreleme anahtarı herkese açıktır ve gizli (özel) tutulan şifre çözme anahtarından farklıdır. RSA' da, bu asimetri, iki büyük asal sayıdaki ürünün faktoringinin(çarpanlarına ayırma) pratik zorluğuna dayanmaktadır(faktoring problemi). RSA kısaltması, 1977'de algoritmayı ilk kez halka açıklayan Ron Rivest, Adi Shamir ve Leonard Adleman'ın soyadlarının ilk harflerinden oluşur.

Bir RSA kullanıcısı, yardımcı değerle birlikte iki büyük asal sayıyı temel alan bir ortak anahtar oluşturur ve yayınlar. Asal sayılar gizli tutulmalıdır. Bir mesajı şifrelemek için genel anahtarı herkes kullanabilir, ancak yalnızca asal sayıları bilen bir kişi mesajı çözebilir. RSA şifrelemesini kırmak RSA problemi olarak bilinir. Faktoring problemi kadar zor olup olmadığı hala çözülemeyen bir soru olarak kalmaktadır. Yeterince büyük bir anahtar kullanılırsa, şu an için sistemi ele geçirecek yayınlanmış bir yöntem yoktur.

RSA Şifreleme ve Şifre çözme

Bir düz metin M'yi bir RSA genel anahtarı kullanarak şifrelemek için, düz metni yalnızca 0 ile N-1 arasında bir sayı olarak temsil eder ve sonra şifreli C'yi aşağıdaki gibi hesaplarız:

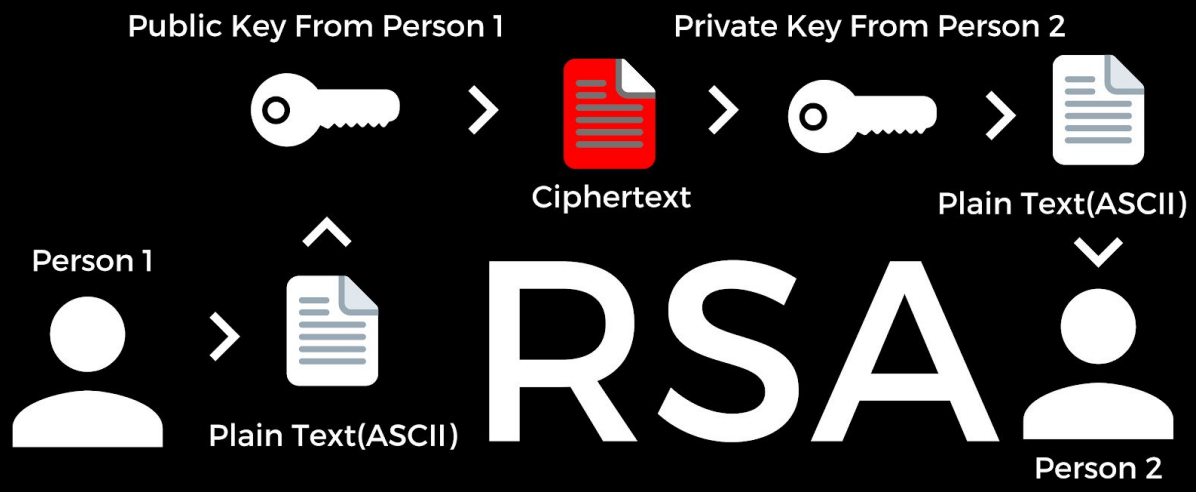
$$C = Me \bmod N$$

Şifre çözme RSA:

Bir RSA genel anahtarı kullanarak bir şifreleme C'nin şifresini çözmek için, basitçe M metnini şu şekilde hesaplıyoruz:

$$M = Cd \bmod N$$

RSA-Şifreleme



Diffie-Hellman

Diffie-Hellman algoritması bilinen en eski asimetrik anahtar uygulamalardan biridir ve çoğunlukla anahtar değişimi için kullanılır. Simetrik anahtar algoritmaları hızlı ve güvenli olmasına rağmen, anahtar değişimi her zaman için bir sorundur. Tüm sistemler için özel anahtarı almanın bir yolunu bulmalıyız. Diffie-Hellman algoritması bu konuda yardımcı olur. Diffie-Hellman algoritması güvenli bir iletişim kanalı oluşturmak için kullanılacaktır. Bu kanal, sistemler tarafından özel bir anahtar değişimi yapmak için kullanılır. Bu özel anahtar daha sonra iki sistem arasında simetrik şifreleme yapmak için kullanılır. Bu yüzden DH-Key-Pairs değişimini kullanıyoruz. Diffie-Hellman algoritması, ortadaki adam saldırısına(man-in-the-middle attack) karşı savunmasızdır.

Diffie-Hellman grupları, anahtar değişimi sürecinde kullanılan temel asal sayıların uzunluğunu tanımlamak için kullanılır. Üç tip Diffie-Hellman grubu vardır:

1. Bu en az güvenli gruptur ve sadece 768 bit anahtarlama gücü sağlar.
2. Bu grup 1024 bit anahtarlama gücünde orta seviyeye ayarlanmıştır.
3. Bu grup 2048 bit anahtarlama gücünde en üst seviyeye ayarlanmıştır.

Diffie-Hellman Protokolü

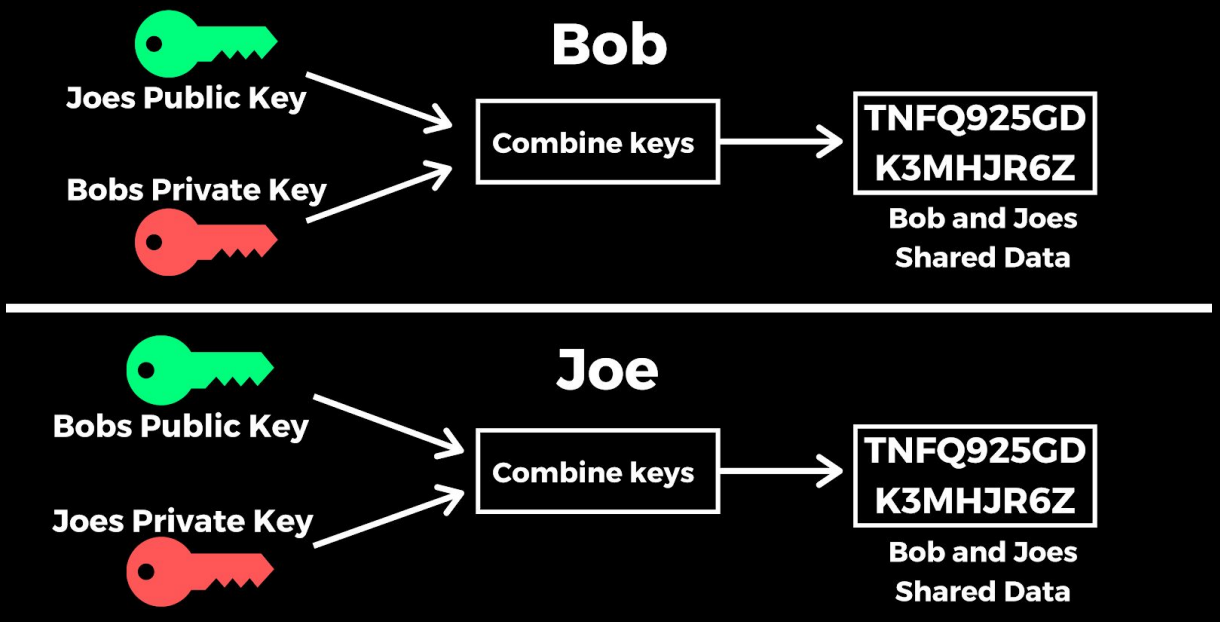
- Uzun süreli güvenliği sağlamak için asal sayıdaki Diffie-Hellman protokolü için p en az 2048 bit olmalıdır.
- Diffie-Hellman protokolü, anahtar değişimi için yaygın olarak kullanılan bir yöntemdir. Döngüsel gruplara dayanır.

Diffie-Hellman Hibrit Sistemleri

Hibrit oturum anahtarı sistemleri, bir oturum anahtarı geliştirmek için birden çok adımdan geçmek yerine, aşağıdakilerin gerçekleşmesi dışında, Diffie-Hellman sistemlerine benzer.

1. A kişisi, basitçe bir oturum anahtarı oluşturur, onu B kişisinin genel anahtarıyla şifreler ve şifreli mesajı B kişisine gönderir.
2. Daha sonra B kişisi, mesajın kendi özel anahtarıyla şifresini çözer, oturum anahtarını kendi tek tuşlu yazılımına veya telefonuna girer ve konuşma veya veri aktarımını daha hızlı, geçici, tek tuşlu modda başlatır.
3. Geçici, rastgele oturum anahtarını seçme işlemi, kullanıcılar için görünmez çünkü her biri kullanan şifreleme yazılımında yer alan matematiksel algoritmada gerçekleşmektedir.

Diffie-Hellman



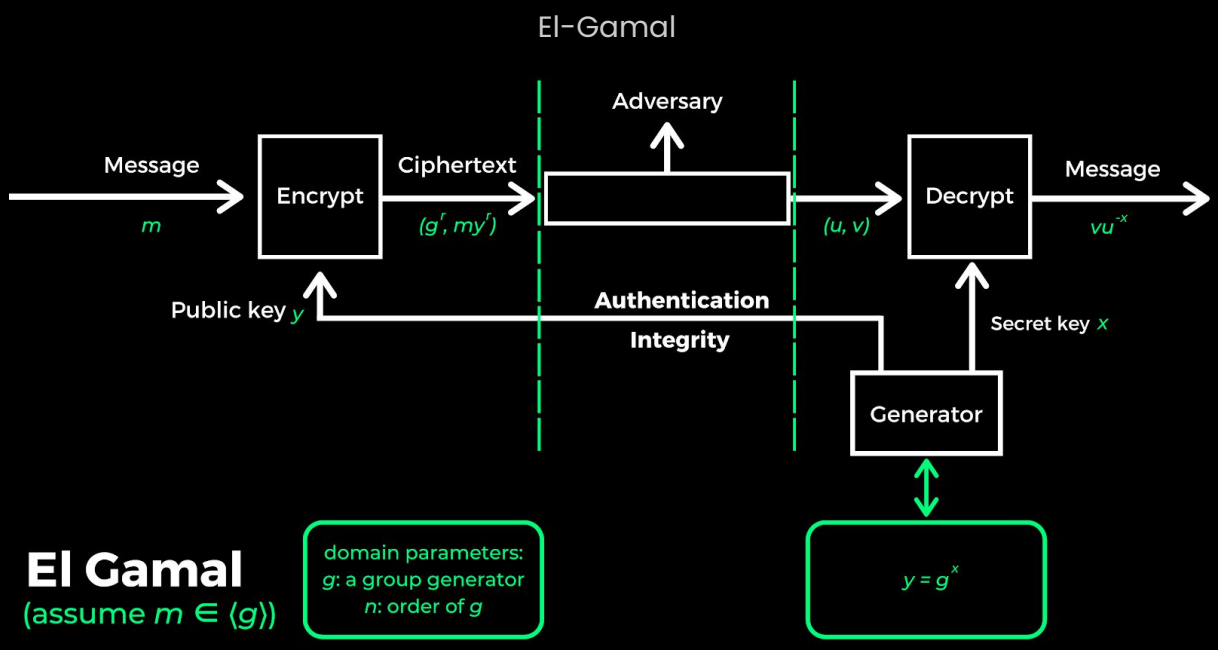
El-Gamal

El-Gamal şifreleme, açık anahtarlı bir şifreleme sistemidir. İki taraf arasında iletişim kurmak ve mesajı şifrelemek için asimetrik anahtar şifrelemesi kullanır. El-gamal algoritması, Ayrık Logaritma Problemi ve Diffie Hellman anahtar değişimine dayanan Taher El-Gamal tarafından icat edildi. El-gamal, iki özdeş mesajın şifrelenmesinin farklı şifreleme oranlarına neden olan olasılıklı bir şifreleme yöntemidir.

- El-Gamal, düz metnin iki katı büyüklüğünde şifreli metin kullanmanın dezavantajına sahiptir.
- Aynı düz metin şifrelendiğinde her seferinde farklı bir şifreleme metni verir.
- El-Gamal, şifrelemenin yanı sıra dijital imza için de kullanılabilir.
- El-Gamal döngüsel gruplara dayanır.
- El-Gamal şifrelemesi için, asal sayı p, en az 2048 bit olmalıdır.

El-Gamal Protokolü

- DHKE'den farklı olarak, asal sayıyı ve ilkel öğeyi seçmek için güvenilir bir üçüncü taraf gerekmez.
- İnşa aşaması sadece taraflarca bir kez yapılır.
- Her mesaj değişiminde şifreleme aşaması ve şifre çözme aşaması gerçekleştirilir.
- Alice'in sadece bir mesaj göndermesi gerekirken, Diffie-Hellman tabanlı protokol iki mesajın gönderilmesini gerektirir.

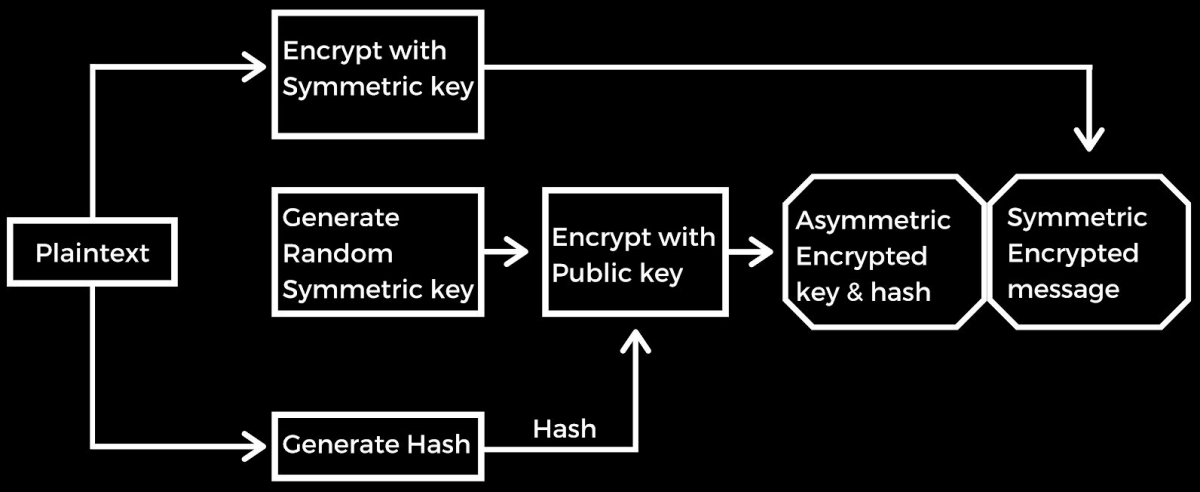


Hibrit Şifrelemesi

Hibrit şifreleme, iki veya daha fazla şifreleme sistemini birleştiren bir şifreleme modudur. Her şifreleme biçiminin güçlü yanlarından yararlanmak için asimetrik ve simetrik şifreleme kombinasyonunu içerir. Bu güçlü yönler sırasıyla hız ve güvenliktir. Hibrit şifreleme, genel ve özel anahtarlar tamamen güvenli olduğu sürece oldukça güvenli bir şifreleme türü olarak kabul edilir. Hibrit şifreleme şeması, asimetrik şifreleme şemasının uygunluğunu simetrik şifreleme şemasının etkinliği ile harmanlayan bir şemadır. Şifreleme yöntemlerinin kombinasyonu çeşitli avantajlara sahiptir.

- Kullanıcılar daha sonra hibrit şifreleme yoluyla iletişim kurabilirler.
- Asimetrik şifreleme, şifreleme işlemini yavaşlatabilir, ancak simetrik şifrelemenin eşzamanlı kullanımıyla, her iki şifreleme şekli de geliştirilir.
- Sonuç, genel olarak geliştirilmiş sistem performansı ile birlikte iletim işleminin ek güvenliğidir.
- Hibrit şifreleme yaklaşımları kullanılarak artan hesaplama karmaşıklığı, gizlilik, bütünlük ve özgünlük gibi şifreleme hedefleri gerçekleştirilebilir.

Hibrit Şifreleme



SHA-256

SHA-256, SHA-1'in (topluca SHA-2 olarak adlandırılır) ardışık hash fonksiyonlarından biridir ve mevcut olanların en güçlüsüdür. SHA-256, kodlama için SHA-1'den daha karmaşık değildir ve henüz hiçbir şekilde taviz vermemiştir. 256 bit anahtar, AES için iyi bir ortak işlevi görür. SHA-256, rastgele boyutta bir girdi alan ve sabit boyutta bir çıktı üreten bir fonksiyondur.

Ek olarak, SHA-256'nın oldukça iyi teknik parametreleri var:

- Blok boyutu göstergesi: 64 Bayt.
- İzin verilen maksimum mesaj uzunluğu: 33 Bayt.
- İletinin özet boyutunun özellikleri: 32 Bayt.
- Standart sözcük boyutu: 4 Bayt.
- Dahili pozisyon uzunluğu parametresi: 32 Bayt.
- Bir döngüdeki tekrar sayısı: 64.
- Protokolün (MiB / s) elde ettiği hız: yaklaşık 140

SHA-256 hash fonksiyonu Bitcoin ağı içinde iki ana yoldan kullanılır:

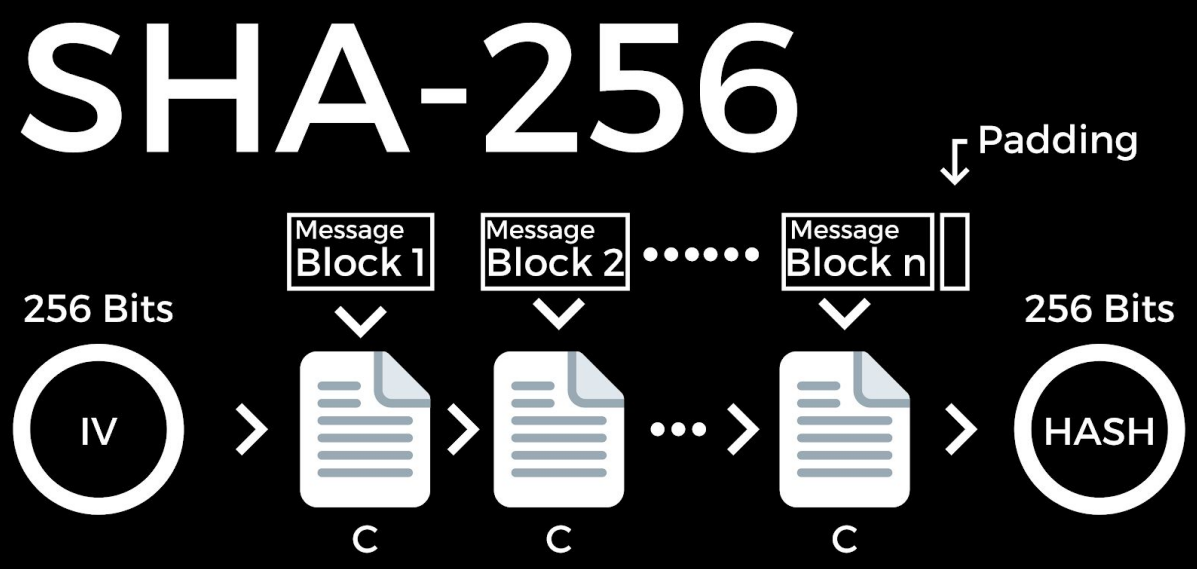
- Madencilik
- Bitcoin adreslerinin oluşturulması

Daha önemlisi:
Zamanla, bilgisayar işlem gücünün maliyeti azaldıkça siber saldırılar önemli ölçüde artmaktadır. 2025 itibariyle, mevcut dijital imzayı bugün olduğundan daha az güvenli hale getirecek. Bu nedenle algoritma seçimi önemli bir karar olacaktır. Bu gereklidir, çünkü geçici kısa vadeli güncellemeler güvenliği tehlikeye atabilir. Hiçbir hash algoritması, on yıl boyunca bile yüksek düzeyde bir güvenlik sağlayamaz.

Bu, kriptografların bir problemi bekleyip boşta oturacakları anlamına gelmez. SHA-3 olarak bilinen Sha-2 halefi zaten tamamlandı. Bu geçişi gerçekleştirme zamanı geldiğinde, çevrimiçi teknoloji endüstrisi SHA-3'ü bir sonraki seçenek olarak kullanabilecektir. Fakat belki de, o zamana kadar tamamen farklı bir algoritma olacak.

Desteklemek için yazılım geliştirmeye başlamadan önce yeni şifreleme standartlarını araştırmak ve test etmek yıllar alır. Sadece bir adım önde olduğumuzda, bir veya başka bir güvenlik seviyesi hakkında konuşabiliriz.

SHA-256



Blake2

BLAKE2 şifreleme hash fonksiyonu Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn ve Christian Winnerlein tarafından tasarlanmıştır.

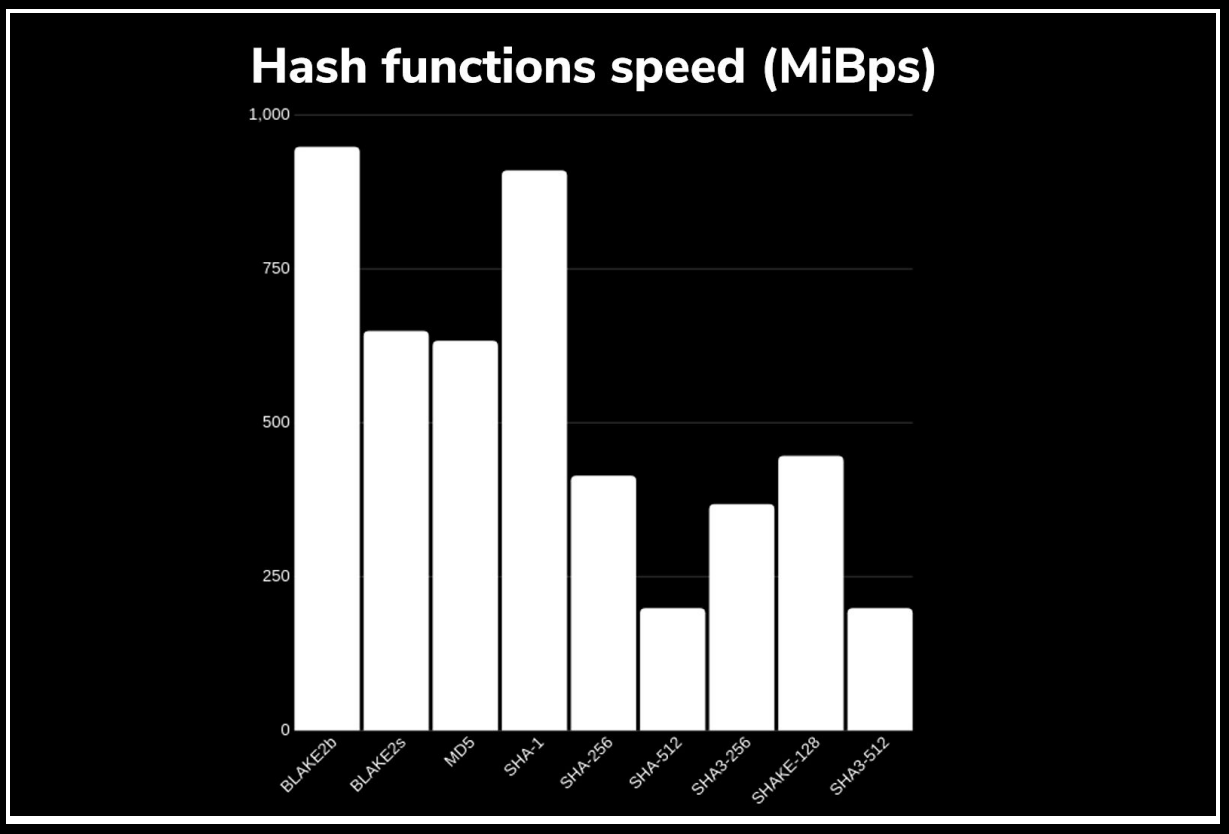
BLAKE2, MD5, SHA-1, SHA-2 ve SHA-3'ten daha hızlı bir şifreleme hash fonksiyonudur ve en az en son standart olan SHA-3 kadar güvenlidir. BLAKE2, yüksek hızı, güvenliği ve sadeliği nedeniyle birçok proje tarafından benimsenmiştir.

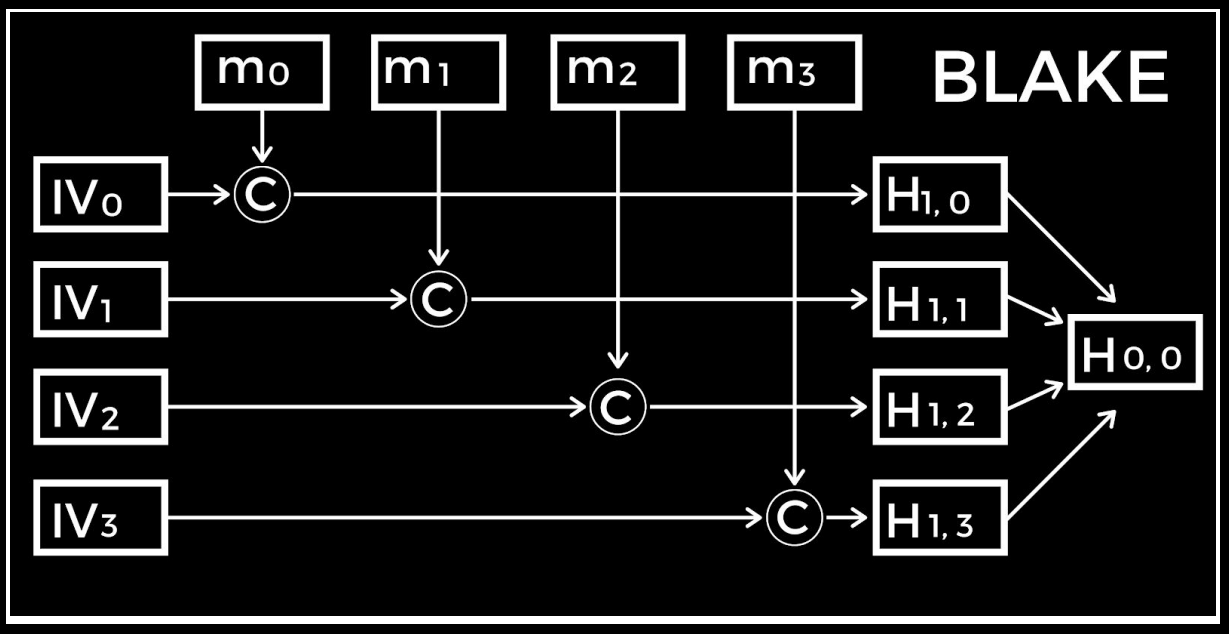
BLAKE2 iki farklı şekilde olur: BLAKE2b (veya sadece BLAKE2), NEON etkin ARMs dahil 64 bit platformlar için optimize edilmiştir ve 1 ile 64 bayt arasında herhangi bir boyutta özet üretir. BLAKE2s 8-32 bit platformlar için optimize edilmiştir ve 1 ile 32 bayt arasında herhangi bir boyutta özeti üretir.

BLAKE2'nin performansı BLAKE'den çok daha hızlıdır, özellikle de düşük tur sayısı nedeniyle. Uzun mesajlarda, BLAKE2b ve BLAKE2'nin sürümlerinin, sabitlerin, optimize edilmiş rotasyonların veya küçük endian dönüşümlerin olmamasından kaynaklanan tasarrufları göz ardı ederek yaklaşık % 25 ve % 29 daha hızlı olması beklenir. Paralel BLAKE2bp ve BLAKE2sp sürümlerinin 4 veya daha fazla çekirdekli bir CPU üzerinde çoklu iş parçacığı ile uygulandığında uzun mesajlarda BLAKE2b ve BLAKE2'lerden 4 ve 8 kat daha hızlı olması beklenir (çoğu masaüstü ve sunucu işlemcisi gibi: AMD FX-8150, Intel Core i5-2400S vb.) Paralel hash, daha önce gözlendiği gibi gelişmiş CPU teknolojilerinden de yararlanır.

Şema 1: EBACS'in "sandy" ölçümlerinden alınan çeşitli popüler hash işlevlerinin hız karşılaştırması. SHA-3 ve BLAKE2'nin bilinen bir güvenlik sorunu yoktur. SHA-1, MD5, SHA256 ve SHA-512, uzunluk genişlemesine karşı hassastır. SHA-1 ve MD5

kesişmelere karşı savunmasızdır. MD5, seçilen ön ek çarpışmalarına karşı savunmasızdır.





BLAKE2b'nin örnek parametre bloğu. Örnek olarak, 64 baytlık digest' larla BLAKE2b örneğini alıyoruz, yani, parametre digest uzunluğu 40, • a ayarlanır 256-bit anahtar, yani, parametre anahtar uzunluğu 20, • a ayarlanır tek yol input hepsi-55 string ayarlanır, • a kişiselleştirme hepsi-ee string ayarlanır. BLAKE2b verileri sırayla hash yapar, böylece ağaç parametreleri sıralı mod için belirtilen değere ayarlanır:

fanout ve maksimum derinlik 01 olarak ayarlanır, leaf maksimum uzunluk 00000000 olarak ayarlanır, node offset 0000000000000000 olarak ayarlanır, node derinlik ve inner hash uzunluk 00 olarak ayarlanır. BLAKE2b'nin bu örneği için parametre bloğu: 40200101 00000000 00000000 00000000 00000000 00000000 00000000 00000000 55555555 55555555 55555555 55555555

BLAKE2s için örnek parametre bloğu. Örnek olarak, 32 baytlık digest' lı• BLAKE2s' in bir örneğini alıyoruz., yani, parametre digest uzunluğu 20 olarak ayarlanır, • anahtar yok, yani, parametre anahtar uzunluğu 00 olarak ayarlanır, • tek yol input yok, ve kişiselleştirme yok, yani, sırayla tüm baytlar NULL olarak ayarlanır. BLAKE2s verileri sırayla hash yapar, böylece ağaç parametreleri sıralı mod için belirtilen değere ayarlanır: fanout ve maksimum derinlik 01 olarak ayarlanır, leaf maksimum uzunluğu 00000000 olarak ayarlanır, node offset 0000000000000000 olarak ayarlanır, node derinliği ve inner hash uzunluğu 00 olarak ayarlanır. Bu BLAKE2 örneği için parametre bloğu: 20000101 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Yapı & Terminoloji:

```
+--------------+------------------+------------------+
|              | BLAKE2b          | BLAKE2s          |
+--------------+------------------+------------------+
| Bits in word | w  = 64          | w  = 32          |
| Rounds in F  | r  = 12          | r  = 10          |
| Block bytes  | bb = 128         | bb = 64          |
| Hash bytes   | 1 <= nn <= 64    | 1 <= nn <= 32    |
| Key bytes    | 0 <= kk <= 64    | 0 <= kk <= 32    |
| Input bytes  | 0 <= ll < 2**128 | 0 <= ll < 2**64  |
+--------------+------------------+------------------+
| G Rotation   | (R1, R2, R3, R4) | (R1, R2, R3, R4) |
|  constants   | (32, 24, 16, 63) | (16, 12,  8,  7) |
+--------------+------------------+------------------+
```

Blake2b bayt boyutlandırma:

```
const (
    // The blocksize of BLAKE2b in bytes.
    BlockSize = 128
    // The hash size of BLAKE2b-512 in bytes.
    Size = 64
    // The hash size of BLAKE2b-384 in bytes.
    Size384 = 48
    // The hash size of BLAKE2b-256 in bytes.
    Size256 = 32
);
```

Şifreleme Sonuçları:

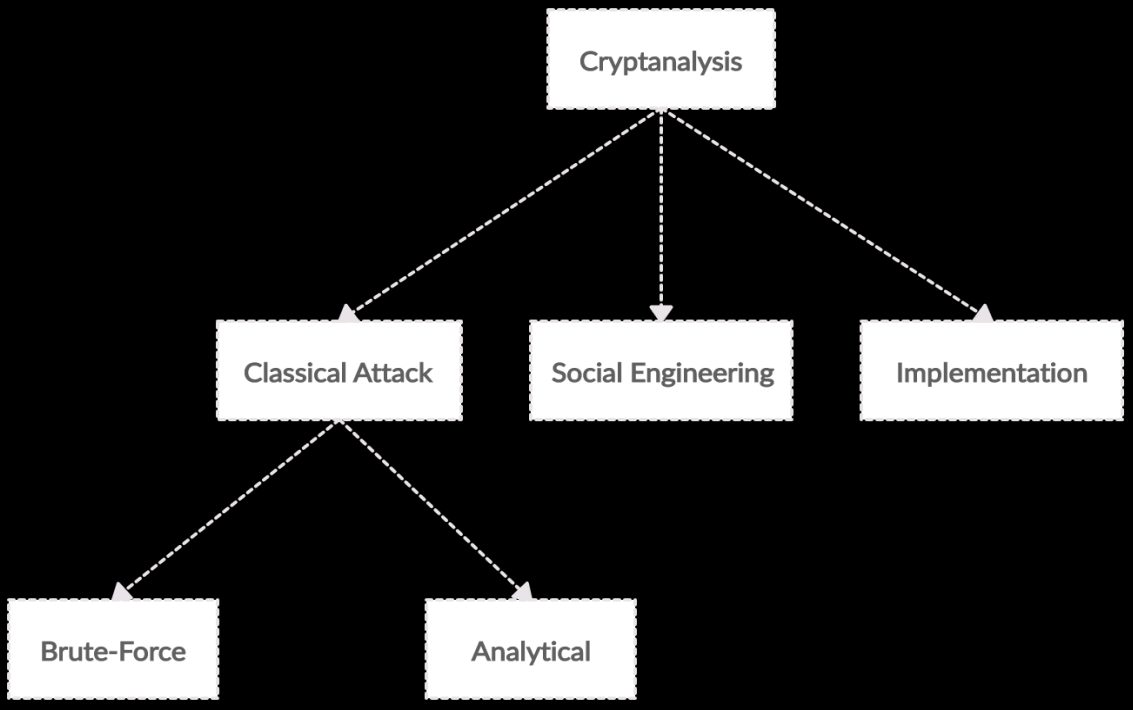
Neden tüm bu şifreleme mekanizmalarını, algoritmalarını ve bu çok bileşenli şifrelemenin hepsini ayrı ayrı ekledik ayrıca kullanmak için gerekli olan hash fonksiyonunu da yazdık, çünkü Zentameshnet, Zentalk ve Zentavult'taki tüm veriler ve IP adreslerin çok güvenli olduğunu, iyi korunduğunu ve üst düzey performans gösterdiğini sizlere sunmak istedik.

Daha da önemlisi, diğer şifreleme yöntemleri artık kullanılamaz çünkü şifreleme mekanizmaları bugün tamamen deşifre edilmiş durumda ve bitlerin gücünde bir eksiklik vardır. Ayrıca, bazı şifreleme algoritmaları, bazı uygulamalar için hız ve performans eksikliğine yol açar, uygulamalar için doğru şifreleme ve hash değerlerin kullanılması kesinlikle önemlidir. Diffie Hellman anahtar değişimi, (middle man attack)ortadaki kişi saldırısının, güvensiz kanaldan geçtiği için yapılan saldırılara karşı bir zayıflığı gösterir. El-Gamal şifreleme ve şifre çözme aşaması her mesajın değiştirilmesi ile gerçekleşir, ancak Diffie-Hellman protokolü iki mesaj gerektirir, böylece A kişisinin yalnızca bir mesaj göndermesi gerekir ve şifreleme ile şifre çözme aşaması her mesajın değişmesi şeklinde gerçekleştirilir. Hibrit şifreleme, iki veya daha fazla şifreleme sistemini birleştiren bir şifreleme modudur, Zentalk bu şifreleme sistemini de kullandığı için adını Zentalk hibrid mesajlaşma uygulaması olarak belirledik. Çünkü sistemin kendi başına çalışması ve üçüncü bir bulut tabanlı belleğe erişmemesi için ağ içinde ve dışında farklı şifrelemeleri sağlamalı ve El-Gamal imzalar için dijital bir çözüm olarak oldukça iyidir. Şifreleme hash fonksiyonu BLAKE2 genellikle kullanılır, çünkü diğer hash fonksiyonlarına göre daha hızlıdır ve merkezi olmayan uygulamalar için daha uygundur, bu yüzden Blake2 kullanmaya karar verdik. AES ile ilgili büyük bir sorun, simetrik bir algoritma olarak, hem şifreleyicinin hem de şifre çözücünün aynı anahtarı kullanma zorunluluğudur. Bu çok önemli bir anahtar yönetimi sorununa yol açar - tüm önemli gizli anahtarların, yol boyunca herhangi bir yerde dikkatsizce veya kasıtlı olarak tehlikeye atılma riski olmadan, dünyadaki yüzlerce alıcıya nasıl dağıtılabilir? Cevap ve çözüm, simetrik ve asimetrik şifrelemeyi birleştirmektir, bunlar AES ve RSA'nın güçlü taraflarıdır. Aynı zamanda her iki şifrelemede de güçlü bir bit gücü kullanmak önemlidir. SHA-256 hash işlevleri şu anda Zentanode Algoritmamızda kullanmak için yeterince güçlü ve AES şifrelemesi için en iyi seçenektir, ancak kuantum bilgisayarların gücü nedeniyle gelecekteki bir güncellemeye ihtiyacı olabilir ve yine burada bitlerin yeterince güçlü olması gerekir.

16. Kriptanaliz

Kriptanaliz, gizli bilgilere erişmeden, şifrelenmiş bilgilerin anlamının elde edilmesine yönelik yapılan çalışmalardır. Tipik olarak, bu sistemin nasıl çalıştığını

bilmek ve gizli bir anahtar bulmaktır. Kriptanaliz, kodu kırmak olarak adlandırılır. (Brute-Force) Şifreli metin genellikle bir şifreleme sisteminin elde edilmesinin en kolay kısmıdır ve bu nedenle kriptanalizin önemli bir parçasıdır. Hangi bilgilerin mevcut olduğuna ve ne tür şifrenin analiz edildiğine bağlı olarak, kriptanalistler bir şifreyi kırmak için bir veya daha fazla saldırı modelini takip edebilirler. Saldırgan veya üçüncü taraf bir kullanıcı, şifresi hariç, şifreleme sisteminin tüm ayrıntılarını bilse bile, bir şifreleme çözümü güvenli olmalıdır. Özellikle, saldırgan şifreleme ve şifre çözme algoritmasını bilse bile prosedür güvenli olmalı, ayrıca algoritma analitik saldırılara karşı da güvenli olmalıdır. Bir saldırgan her zaman bir şifreleme prosedürünün en zayıf noktasından yararlanır. Tek başına büyük bir anahtar odası şifrenin yeterince güvenli olduğundan emin olamaz.



- **Klasik Saldırı**

Klasik kriptanalizde, saldırganın izleyebileceği çeşitli hedefler vardır. En yaygın iki durum, saldırganın belirli bir şifre oranı y için düz metin x'i veya anahtar k'yı hesaplamak istediği durumlardır. Anahtar araştırmanın tamamında, şifre kara kutu olarak kabul edilirken, analitik saldırılar durumunda, şifreleme işleminin iç yapısı kullanılır.

- **Brute-Force Saldırı**

Brute-force saldırıları, bir eşleşme bulununcaya kadar olası tüm anahtar durumları için şifreleme algoritmasını çalıştırır.

Analitik Saldırı

Analitik saldırılar, şifreleme algoritmasının iç yapısını analiz ederek şifreleme sistemini kırmaya odaklanan saldırılardır.

Sosyal Mühendislik Saldırısı

Sosyal Mühendislik Saldırısı Manipülasyondur - kripto anahtarlarını elde etmek için kişilerarası etkilerden (sahte hesaplar gibi) yararlanılır. Kimlik avı saldırıları, sosyal mühendislik saldırısının en bilinen temsilcileridir.

Örnek: "Günaydın, Ben IT departmanı'ndan X. Acil bir güvenlik güncellemesi için şifrenize ihtiyacımız var."

Bir saldırgan, şifreleme sistemini aşmak için zincirdeki en zayıf halkayı arar. Bu nedenle, klasik kriptanalize direnen güçlü kriptografik algoritmalar tek başına yeterli değildir, sosyal mühendislik ve uygulama saldırıları da önlenmelidir.

- **Uygulama Saldırısı**

Yan kanal analizi gibi uygulama saldırıları gizli bir anahtar elde etmek için kullanılabilir. Bunlar saldırganın kriptosisteme fiziksel olarak erişebildiği durumlarda geçerlidir.

Kaç anahtar-boyut bite ihtiyacımız var?

Simetrik ve asimetrik prosedürler için anahtar uzunluklar çarpıcı biçimde farklıdır. Örnek olarak, 128 bit anahtarlı bir simetrik algoritma, yaklaşık 3072 bitlik RSA ile yaklaşık aynı güvenliği sunar. (RSA en popüler asimetrik yöntemlerden biridir).

Simetrik algoritmalar için tam anahtar araması kullanarak saldırı süresi:

1. 64 Bit'i kırmak için birkaç saat veya birkaç gün gerekir.
2. 128 Bitlik Uzun Terimler kuantum bilgisayarla kırılabilir.
3. 256 Bitlik Uzun Terimler kuantum bilgisayarlarla kırılmaz.

Güvenli sistemler için neye ihtiyacımız var?

Bir güvenlik sistemi veri, para veya bina gibi varlıkları korur. Şifreleme algoritmaları, dijital sistemlerin korunmasında genellikle merkezi ve merkezi olmayan bir rol oynar.

Güvenli sistemlerin kuralları ve simetrik algoritmaların kilit uzunlukları:

1. ifre kırmak, korunan şeylerin değerinden daha pahalı olacaktır.
2. Koruyucu değerler ve güvenlik amaçları başlangıçta tanımlanmalıdır.
3. Yalnızca kripto algoritmaları (örneğin, simetrik ve asimetrik şifreler ve hash fonksiyonlar) yada uzun zamandır genel olarak bilinen ve kapsamlı bir şekilde analiz edilen protokolleri kullanın.
4. Korsanın kuantum bilgisayarı yoksa, 128 Bit'in kırılması uzun yıllar alır.
5. 256 Bit: Kuantum bilgisayarlarla yapılan saldırılara karşı güvenlidir.
6. 128, 192 ve 256 bit anahtar uzunluklu AES Şifrelemesi brute force saldırılarına karşı güvenlidir.
7. RSA'ya ihtiyacımız vardır. Veya DHKE Protokolü, güvenli olmayan bir kanal bağlantısındaki anahtarları değiştirmek için bir zorunluluktur. Simetrik anahtarın şifresi çözüldüğü anda, her iki taraf (A) ve (B), bunu simetrik şifreleme ve mesajların şifresini çözmek için kullanabilir.
8. RSA, El-Gamal veya 3DES gibi simetrik veya asimetrik algoritmalarla verileri şifreleyin.

17. Zentamesh Ağı & Zentanode' lar

Node' ları Anlamak

Düğümlerin(Node) fikirleri, paket değiştirme teorisi ve dağıtılmış ağlar kavramının benimsenmesiyle popüler hale geldi. Bu bağlamda, düğümler dağıtılmış bir ağ üzerinden farklı yollar boyunca bilgi alabilen, depolayabilen ve gönderebilen ağ geçitleridir. Her düğüme ağ içinde eşit bir konum verilmiştir, bu da herhangi bir düğümün kaybının ağa zarar vermeyeceği anlamına gelir.

Zentameshnet neden daha iyi?

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 etrafına yayabilir ve hızlıca yönlendirilebilir. Veri yönlendirilir ve ağ hala işlevseldir. Mesh ağlar hem kablolu hem de kablosuz ağlara uygulanabilir, Zentalk ise mesh bir WLAN (Kablosuz Yerel Erişim Ağı) kurar. Bu MWLAN, Zentanode Meshed WiFi kullanımı sayesinde elde edilir. Bu, Zentalk üzerinden çevrimdışı iletişim için gerekli olacaktır.

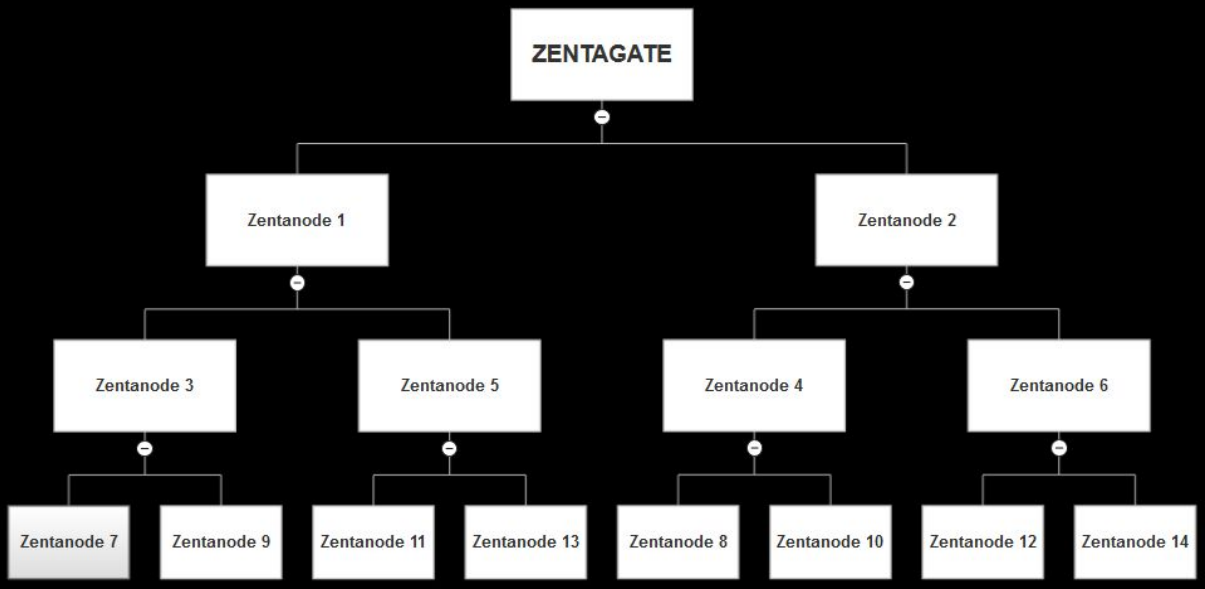
Bu, bir Zentanode sahibinin internet bağlantısı kurabilecek ve paylaşabilecek, ayrıca internet erişimi olmayan cihazlarla iletişim kurabilecek anlamına gelmektedir(çevrimdışı -çevrimdışı). Bu, çok az veya hiç altyapı olmasa bile gerçekleştirilebilir. Zentanode sahipleri Zenta ile ödüllendirilecektir. Düğümler cep

telefonları, yönlendiriciler, anahtarlar, köprüler ve ağ geçitleri gibi aktif ağ bileşenleridir.

Ağdaki herbir Zentanode bir bağlantı noktasıdır. Bu, yeniden dağıtım noktası veya veri aktarımındaki bir son nokta olabilir. Gönderimleri diğer ağ düğümleri için bulma, işleme ve iletme özelliğine sahiptir. Bir ağ düğümü, diğer ağ elemanlarına en az iki genellikle de daha fazla bağlantıya sahiptir.

Zentameshnet'teki her Zentanode ayrıca Zentamesh ağını büyütmek için Ağ Geçidi görevi görebilir. Kullanıcı ayrıca kendi Zentanode'u ile bağlantı kurmak için ağını bir pin koduyla kapatabilir. Her Zentanode kendi kimliğine sahip olacaktır.

Bir Zentanode'un rolü cep telefonunda, tablette veya bilgisayarda Zentalk messenger dApp çalıştıran bir cihaza bağlanacaktır.



Zentamesh teknolojsini kullanmak için 11 sebep:

1. Ağ istikrarı

(Kablosuz) Mesh ağındaki veriler, Zentanode'lardan biri veya birkaçı hatalı veya arızalı olsa bile diğer Zentanode'lar üzerinden iletilebilir, veriler ekosistemdeki diğer Zentanode'lar üzerinden yönlendirilir.

2. Yüksek bant genişliği

Zentamesh ağları, daha yüksek bir bant genişliğine izin vererek 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, Zentamesh ağının çoklu atlama mekanizması, kullanıcı iletişiminin birkaç Zentanode'dan geçmesi gerektiğini belirler.

4. Zentanode Mesafesi

- Ne kadar çok Zentanode kullanıcısı olursa, kablosuz Zentamesh ağı o kadar geniş ve hızlı olur.
- Tek bir Zentanode menzili şu anda internet erişimi olmadan 25-50 Km (Daha Fazla Düğüm = Daha Fazla Aralık)
- Zentanode kullanıcısı, Zentanode'unu kendi kullanıcı ağ geçidi(Zentagateway) olarak da çalıştırabilir.
- Zentanode olmadan, menzil Wi-fi Bağlantısı üzerinden yaklaşık 100 metre olacaktır.

5. Zentameshnet ile Veri Transferi

- Zentameshnet ağında ilk önce Wifi ve BLE bağlantısı üzerinden maksimum 15 Mb veri ve dosya aktarmak mümkün olacaktır.
- İnternet bağlantısıyla 150 Mb'a kadar, indirme hızı saniyede 17.88 MB olacaktır.

6. Zentanode Hash (H) ve Şifreleme (E)

- SHA256(H), AES(E), RSA(E), Blake2b(H), Hibrit(E)
- Zentanode Hash -Algoritmaları: SHA-256
- SLL

7. Çalışma frekansları:

- Avrupa- 868MHz
- US, Kanada & Meksika - 902MHz
- Latin Amerika & SE-Asya - 922MHz

8. Mevcut ağlar:

- IEEE 802.11,(Wifi) Bluetooth, LTE, 4G, 5G

9. Wifi Bağlantısı

- Çoğu kablosuz ağ için hali hazırda bulunan WiFi standartlarına (802.11a, b ve g) güveniyorlar.
- Deep sleep(Uyku Modu): Evet

10. Bluetooth

- Düşük Enerji

11. Zentagateway

- AES 128

18. Zentavault

Zentavault, Zentachain tarafından üretilen ikinci dApp. Zentavault, yüksek oranda şifrelenmiş ve dağıtılmış bir depolama hizmeti olarak tasarlanmış ultra verimli bir dApp'dir. Bu servis Zentachain platformunda barındırılacak olup ZentaChain'in dApp'ları asla merkezi sistemlere güvenmez. Ve kesinlikle kullanıcıların meta verileri için hiçbir yedekleme veritabanına sahip olmayacaktır. Bunu yaparak, Zentavault gizlilik, anonimlik ve ticari performansını üst seviyede tutacaktır.

Zentavault aylık kullanım ücreti gerektirmez, bunun yerine veri yüklemek için yalnızca küçük bir işlem ücreti alınır. Zentavault bir dosya şifreleme ve dağıtım aracıdır. İçeriği seçtikleri şekilde şifrelemek, depolamak ve paylaşmak için kullanıcılar tam kontrol sahibi olacaktır. Zentavault ile, verilerinizin IPFS olarak da adlandırılan, Nesneler Arası 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'deyken, şifreli hash veya hash kimliği olarak bilinen benzersiz bir tanımlayıcı atanır. Bu, kullanıcının verilerini bulmak veya iki taraf arasında paylaşmak için kullanılabilir. İçeriğiniz IPFS'ye gömüldükten sonra, başkalarına içerik bulma veya paylaşmanın bir yolunu sağlayan bir hash kimliği atanır. IPFS gibi eşler arası hiper medya protokolü teknolojilerini kullanarak, Zentavault daha hızlı, korumalı ve erişilebilir bir dosya depolama ve aktarma hizmeti sağlayabilir.

IPFS (Nesneler Arası Dosya Sistemi)

Modern internet, çağımızın çığır açan teknolojilerinden biri olmasına rağmen, 1990'lı yıllardaki kuruluşundan bu yana bazı kısıtlamaları olduğunu göstermiştir.

Teknolojik gelişmeler ilerledikçe, her türlü teknolojinin de ya güncelleme ya da kavramsal olarak yeniden şekillendirilmeye ihtiyaç duyduğu görülmüştür. HTTP protokolünde durum bu şekildedir.

Son zamanlarda, HTTP protokolünün "göreve hazır" olduğu gösterilmeyen alanlar olan gizlilik, güvenlik ve hız konularını ele alacak çözümlere olan talebin arttığını gördük. Neyse ki IPFS, söz konusu sorunlara çözüm sunan bir fikir olarak ortaya konulmuştur.

Nasıl çalışır?

Buna bir BitTorrent yığını 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 erişime olanak 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 değişmezlik ve içerik çeşitliliği 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 sunar. 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 bulmacasıyla oluşturulmuş bir ortak anahtarın kriptografik hash3 olan bir Node kimliği ile tanımlanır. Düğümler ortak ve özel anahtarlarını saklar (bir parola ile şifrelenir). Kullanıcılar, her lansman sırasında "yeni" bir düğüm kimliğini başlatmakta özgürdürler, ancak bazı kazanılmış ağ avantajlarını kaybederler, düğümlerin aynı kalması tavsiye edilir.

IPFS Ağı

IPFS düğümleri, ağdaki yüzlerce başka düğümle internet üzerinden düzenli olarak iletişim kurar. IPFS ağ yığını özellikleri:

- İletim: IPFS herhangi bir aktarım protokolünü kullanabilir ve WebRTC Veri Kanalları (tarayıcı bağlantısı için) veya uTP (LEDBAT) için en uygunudur.
- Güvenilirlik: IPFS, temel ağlar sağlamazsa, uTP (LEDBAT) veya SCTP kullanarak güvenilirlik sağlayabilir.
- Bağlanabilirlik: IPFS ayrıca ICE NAT geçiş tekniklerini kullanır.

- Bütünlük: isteğe bağlı olarak bir hash sağlama toplamı kullanarak mesajların bütünlüğünü kontrol eder.
- Doğrulama: isteğe bağlı olarak, gönderenin genel anahtarıyla HMAC kullanarak mesajların doğruluğunu kontrol eder.

IPFS Yönlendirme

Yönlendirme için IPFS, S / Kademlia ve Coral'ı temel alan Dağıtılmış Özensiz Hash Tabloları kullanır. Amacı:

1. Düğümlere eklenen verileri duyur
2. Belirli düğümler tarafından istenen verileri bul

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

Objects Merkle DAG

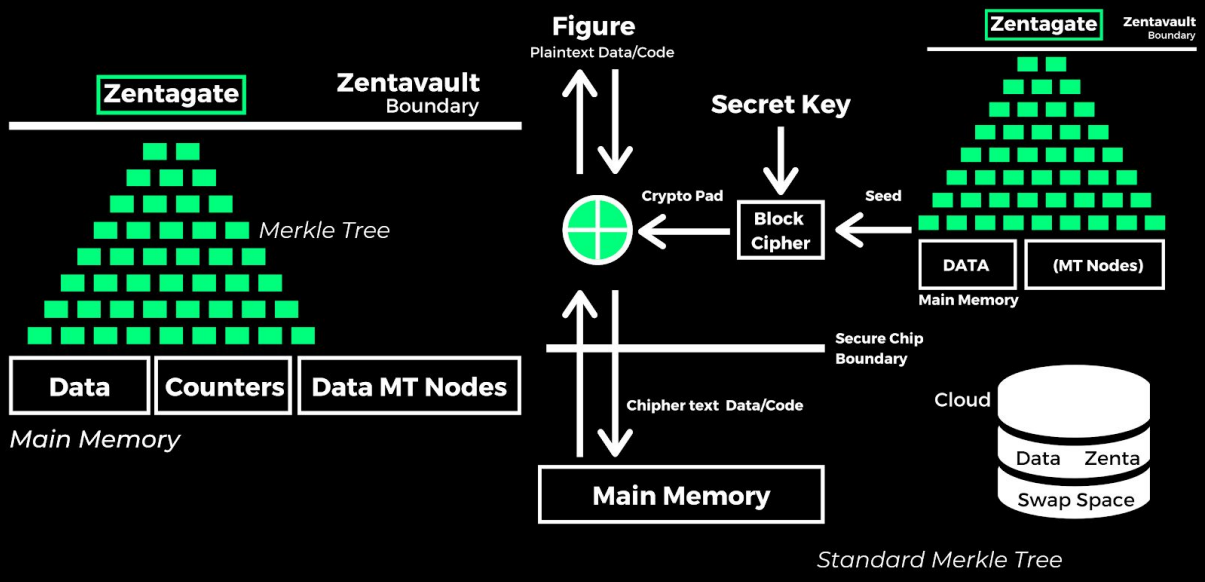
Merkle DAG (Merkle Yönlendirilmiş Asiklik Grafiği), Nesneler Arası(Interplanetery) Dosya Sistemindeki nesne dosyalarının sırasını korumak için kullanılır. Merkle DAG, dosyaların bir hash kimliği olarak bilinen benzersiz şifreli hash değerleri ile birbirine bağlanmasına izin verir. Hash kimliği tüm hash kimlik nesne linklerini içerir. Merkle DAG, aşağıdaki gibi IPFS'ye faydalı özellikler sunar:

- İçerik koruması: Merkel DAG, IPFS'deki tüm içeriğin güvenliğini, emniyetini ve bütünlüğünü garanti eder. IPFS'de depolanan veya barındırılan herhangi bir nesne zarar görmüş veya başka bir şekilde bozulmuşsa, Merkle DAG kök hashini otomatik olarak değiştirir.

- Verimlilik için tekrardan kaçınma(Aynı veriyi iki kez depolamaz): IPFS'de içerik tutan tüm nesneler sıralanır, çoğaltılan nesneler tanınır ve silinir. Bu, içeriğin IPFS'de birden çok kez tekrarlanmasını engeller.

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

19. Zentagate



Adresten Bağımsız Seed Şifrelemesi Kullanma

Bellek şifrelemenin amacı, güvenli işlemci sınırı dışında depolanan tüm verilerin ve kodların anlaşılmaz bir biçimde olmasını ve depolanan gerçek değerler hakkında hiçbir şeyin açığa çıkmamasını sağlamaktır. Aşağıdaki şema, sayaç mod şifrelemesinde bunun nasıl elde edildiğini göstermektedir. Bir blok belleğe tekrar yazıldığında, bir seed blok şifresi (örneğin, AES) ve sadece işlemci tarafından bilinen gizli bir anahtar kullanılarak şifrelenir.

Şifreli seed bir kriptografik takım olarak adlandırılır ve bu takım, 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 seed şifrelemek için kullanılan aynı takımın üretilmesi için şifrelenir. Blok çip üzerine ulaştığında, takım 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. Blok çip üzerine ulaştığında, takım bir başka bit XOR değeri bloğu orijinal düz metin biçimine geri yükler. Matematiksel olarak, eğer P şifresiz metin ise, C şifreli metindir, E blok şifreleme işlevidir ve K gizli anahtardır. şifreleme C = P EK (Seed) gerçekleştirir. Her iki tarafı da EK (Seed) ile XOR işlemi yaparak, şifre çözme şifresiz metin P = C EK (Seed) sonucuna varır.

IPFS Dosyaları

IPFS ayrıca sürümlü bir dosya sistemini Merkle DAG'in üstüne modellemek için bir nesne kümesi tanımlar. Bu nesne modeli Git'in kullandıklarına benzer:

1. lok: değişken boyutlu bir veri bloğu.
2. liste: bloklar veya başka listeler topluluğu.
3. ağaç: bloklar, listeler veya diğer ağaçlar topluluğu.
4. commit: bir ağacın sürüm geçmişindeki bir anlık görüntü.

Neden IPFS' e ihtiyaç duyarız?

- **Bant Genişliği**

Sadece bir merkezi konumdan verilere erişebilmek, dezavantajlara sahip olabilir. Bir dosyayı insanlarla dolu bir odayla paylaşmak istediğinizi hayal edin. Bu dosyayı muhtemelen sizden uzakta bir yere (internetin omurgası) bulunan ve yolda birkaç sunucuya yönlendirilmiş merkezi bir sunucuya yüklersiniz. Diğer insanlar daha sonra bu uzak sunucuya tekrar bağlanıp bu dosyaya erişebilirler.

Özellikle resim ve video gibi büyük dosyalarda, bu dosyayı muhtemelen sizinle aynı yerel ağa bağlı olan insanlarla dolu bir odayla paylaşmak için çok fazla bant genişliği kullanılmasına neden olabilir. IPFS ile bu dosya, yerel ağ 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, özellikle depolama maliyetinden çok, daha yavaş azalan bağlantı hızı maliyetine bakıldığında önemlidir. Bu eğilim devam ederse, kullanıcılar çok daha fazla veri depolayabilecek ve böylece ağ kullanımlarını artıracaktır. Ancak bant genişliği aynı hızda gelişmiyorsa, bağlantı hızı gittikçe yavaşlar. Güvenlik de artar - örneğin, DDoS saldırıları, IPFS'nin sahip olmadığı merkezi bir dağıtım sistemine saldırmaya bağlı oldukları için işe yaramaz. Hız, artan bir başka faktördür. Dağıtılmış bir ağda, bir şey talep eden her node, onu tek bir merkezi konum yerine kendisine en yakın olan node'dan ister.

- **Gecikme**

İlgili bir diğer sorun gecikmedir. Işık hızı sabit olduğundan ve değiştirilemediğinden gecikmeyi azaltmanın tek yol, verileri kullanıcıya daha yakın bir noktadan sunmaktır. Bu nedenle büyük bulut servis sağlayıcıları bölgelere göre depolama

yerleri sunmaya başlamıştır. IPFS, istenen verilere hizmet veren bilgisayara olan mesafeyi mümkün oldukça azaltmayı amaçlamaktadır.

Offline Olma

Gün içinde birçok hizmet kullanıyoruz ve yalnızca çevrimiçi olduğumuzda yoğun olarak çalıştığımız hizmetlere güveniyoruz. Aynı odadaki diğer kişilerle birlikte bir belge üzerinde birlikte çalışmak veya telefonunuzdan dizüstü bilgisayarınıza veri aktarmak istiyorsanız, bunu yalnızca internetin omurgasının merkezi sunucularına bağlıysanız yapabilirsiniz. Bant genişliği veya yığılma, 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 değiştirme olanağı sunar.

- **Sansürleme**

Her şey bir P2P ağından ziyade bir merkezi sunucuda saklanır ve çalıştırılırsa, verilere veya hizmetlere erişim sansürlenebilir veya kısıtlanabilir. Buna bir örnek, Mısır hükümeti, protestocular arasında iletişimi ve organize olmalarını engellemek için 2011 yılında Arap baharı boyunca internete erişimi tamamen kesti. Bağlantılı olarak P2P IPFS, bu sansürü imkansız hale getirmeyi umuyor.

- **Devamlılık**

Herkes daha önce bir 404 hatasıyla karşılaşmıştır Bu, silindiği veya kaldırıldığı için gerekli içeriğin bulunamadığı anlamına gelir. Örneğin, sağladığınız içerik için gerekli olduğundan, bu içeriğe bağlanmak istiyorsanız bu çok büyük bir problem olabilir. Genel olarak, web'de toplanan bilgilerin çoğunun erişilebilir olması ve birisinin bazı web sitelerini isteyerek veya yanlışlıkla kapatması nedeniyle silinmemesi toplum için faydalı olacaktır. IPFS ile bağlantılı içeriğin bir sürümünü kendiniz kaydedip barındırabilirsiniz ve bu şekilde, orijinal ana bilgisayarlar artık barındırmasa da, bu içeriğin kullanıcılar tarafından her zaman kullanılabilir olmasını sağlanır. Asıl fikir, hiçbir içeriğin kaybedilmediği kalıcı bir ağ oluşturmaktır çünkü içeriğin tamamı birçok kişi tarafından barındırılmaktadır.

- **Güvenlik**

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

- **Kendinden Sertifikalı Dosya Sistemleri - SFS**

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

Sunucularda ortak bir şifre bulunur ve istemciler sunucunun kimliğini doğrulamak ve güvenli bir iletişim kanalı oluşturmak için sunucu ortak şifrelerini kullanır. SFS, müşterilerin daha önce hiç duymamış olsalar bile, sunucuların kimlik doğrulamalarına izin vermek için, “self-certifying yoladı (kendini doğrulayan yoladı)” kavramını ortaya koyar.

Bir kendinden sertifikalı yoladı, sunucunun genel şifresinin hash değerini içerir, böylece istemci, resmi 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 yoladı aşağıdaki sözdizimine uyar: /sfs/location:hostid/real/pathname, burada ‘’location’’, dosya sistemini dışa aktaran sunucunun adı (IP adresi veya DNS Adı) ve ‘’hostid’’ sunucunun ortak şifresini ve diğer bazı bilgileri içeren bir dizenin hash’ idir. SFS, yoladının kullanıcı tarafından nasıl elde edildiği ile ilgilenmez; bir kullanıcı sonunda mevcut bir PKI (Açık Anahtar Altyapısı) kullanarak ana bilgisayar kimliğini alabilir. Öte yandan, ilgilendiği dosyalar için kendinden onaylı bir yoladı alındığında, kullanıcıların herhangi bir şifreyi 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 çıkarmıştır: uzaktaki sistemleri aşağıdaki şema ile ele almak:

/sfs/<Location>:<HostID>
Burada Location sunucu ağ adresidir ve
HostID = hash(public_key || Location)

Böylece SFS dosya sisteminin adı sunucuyu doğrular

Yukarıda okuduğunuz gibi, web zaten işlev görüyor gibi çalışacak 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 (InterPlanetary Linked Data) adı verilir.

Zentachain olarak Zentachain Lab'ı kalıcı olarak güncelleme hakkını saklı tutmaktayız çünkü teknoloji çok hızlı bir şekilde gelişmektedir dolayısıyla daima güncel ve en iyi standarda sahip olacağımızdan emin olmamız gerekir.

REFERANSLAR

Adnan Abdul-Aziz Gutub, Farhan Abdul-Aziz Khan, Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems, 2012 International Conference on Advanced Computer Science.

Shankar Dhakar, Ravi & Kumar Gupta, Amit & Sharma, Prashant, Modified RSA Encryption Algorithm (MREA), 2012 2nd International Conference on Advanced Computing and Communication Technologies(ACCT), pp. 426-429, 2012.

Nishtha Mathur and Rajesh Bansode, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, Procedia Computer Science 79, pp. 1036 – 1043, Elsevier, 2016.

Koorosh Goodarzi, Abbas Karimi, Cloud Computing Security by Integrating Classical Encryption, Procedia Computer Science 42, pp. 320 – 326, Elsevier, 2014.

Shilpi Gupta and Jaya Sharma, A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman, 2012 International Conference on Computational Intelligence and Computing Research, IEEE, 2012.

R. Rizk, Y. Alkady, Two-phase hybrid cryptography algorithm for wireless sensor networks, Journal of Electrical Systems and Information Technology Vol 2, Issue 3, pp. 296-313, 2015.

Koorosh Goodarzi, Abbas Karimi, Cloud Computing Security by Integrating Classical Encryption, Procedia Computer Science 42, pp. 320 – 326, Elsevier, 2014.

M. Indra Sena Reddy and A.P. Siva Kumar, Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm, Procedia Computer Science 85, pp. 62-69, Elsevier, 2016.

Wang Rui; Chen Ju; Duan Guangwen, 'A k-RSA algorithm,' Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.21,24, 27-29 May 2011.

Liang Wang, Yonggui Zhang, A New Personal Information Protection Approach Based on RSA Cryptography, IEEE, 2011.

Christof Paar, Jan Pelzl, "Understanding Cryptography", SpringerVerlag Berlin Heidelberg, pp. 3-9, 30-31, 2010.

Assad Ibraheem Khyoon,"Modification on the Algorithm of RSA Cryptography System" 2006.

Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, Procedia Computer Science 54, pp. 73-82, Elsevier, 2015.

Diffie: Whitfield Diffie and Martin Hellman, ``New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976.

Vitalik Buterin. Ethereum 2.0 mauve paper. 2016

Polkadot:
https://polkadot.network/PolkaDotPaper.pdf

Cosmos:
https://cosmos.network/cosmos-whitepaper.pdf

ABCI:
https://github.com/tendermint/abci

Bitcoin:
https://bitcoin.org/bitcoin.pdf

BitShares:
https://bitshares.org/technology/delegated-proof-of-stake-consensus

Computer Networks:
https://digitalescobar.wpcomstaging.com/wp-content/uploads/2018/12/DigitalEscobar.com-Computer-Networks-A-Systems-Approach-by-Larry-L.-Peterson-Bruce-S.-Davie-.pdf

AES Encryption:
https://townsendsecurity.com/sites/default/files/AES_Introduction.pdf

Blake2:
https://blake2.net/

Hybrid Encryption Algorithm:
https://pdfs.semanticscholar.org/d518/9533fd596a5cbc39864d21a5ef4e0156359d.pdf

A hybrid encryption algorithm based on RSA and Diffie-Hellman:
https://ieeexplore.ieee.org/document/6510190

IPFS:
https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

Ietf.org:
https://en.wikipedia.org/wiki/History_of_cryptography

Diffie–Hellman:
https://www.math.brown.edu/~jhs/MathCrypto/SampleSections.pdf

Crypho Security Whitepaper:
https://www.crypho.com/downloads/crypho_security_whitepaper.pdf

On the Security of ElGamal Based Encryption:
https://www.researchgate.net/publication/221010812_On_the_Security_of_ElGamal_Based_Encryption

Descriptions of SHA-256, SHA-384, and SHA-512:
http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf

A Review on Hybrid Encryption in Cloud Computing:
https://www.semanticscholar.org/paper/A-Review-on-Hybrid-Encryption-in-Cloud-Computing-Kumar-Badal/ad6ba7c05455b4b1416e19b52aa42ec050a5dd74