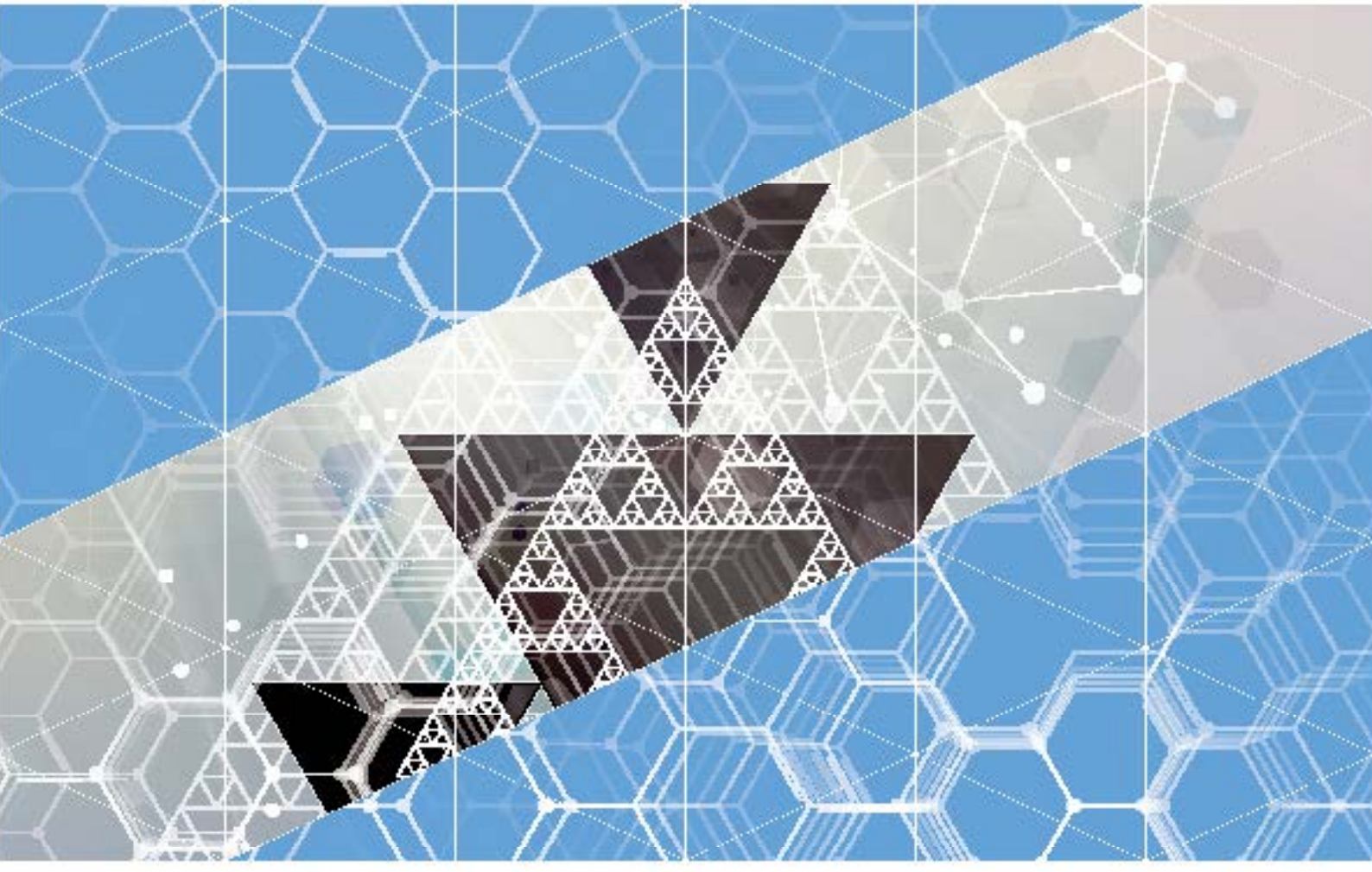
SAFE мрежата – въведение

Кратко представяне на първата напълно автономна мрежа за данни в света



Март 2018

SAFE Network

SAFE мрежата – кратко въведение

Технологичният напредък е един вечен процес на автоматизация и абстракция. Трудни и сложни задачи се опростяват чрез софтуер и машини, докато накрая не се приемат за даденост. Междувременно технологията върви напред, преодолявайки нови бариери по пътя на развитието си.

Един пример за този процес са т.нар. изчислителни услуги в облак /cloud computing/. Задачата за осигуряване на сървър, която преди беше специализирана, сега е толкова проста, че всеки може да я направи. Сложността вече не е бариера. В крайна сметка машините ще станат много по-добри в подсигуряването на други машини, отколкото са хората, и в този момент може да има предимство автоматизирането на задачата като цяло. Всъщност, това вече започва да се случва.

Ако ние вземем този процес и го придвижим една стъпка по-напред и автоматизираме цялата мрежа, правейки я автономна, способна да съхранява, да защитава и да доставя данни, без да има изобщо човешка намеса? И какво ще стане, ако данните върху тази мрежа се съхраняват и пренасят при условия на пълна сигурност, осигурена чрез най-модерните техники на криптиране, които са на разположение? И какво ще стане, ако потребителите на тази платформа могат да бъдат по желание или публични или анонимни?

Сред очевидните ползи би било и повишеното доверие в сигурността и непокътнатостта на всички данни. Без присъствието на трети страни, които да въвеждат грешки и сериозни бариери поставени пред хакерите, които искат да откраднат, корумпират или компрометират данни, децентрализираните „ненадеждни" системи например, ще станат безценни в много приложения в „интернета на нещата", като да речем автомобилите без шофьори, където всякакъв срив или кибернетична атака биха били животозастрашаващи. Това ще предложи много по-нужна алтернатива на настоящия интернет, доминиран от шепа огромни и мощни корпорации и използван от правителствата, за да ни държат под око. Това е мощна динамика която назрява за промяна.

Но най-вече, такава система ще бъде опростена, без да съществува абстрактността от сложността на управляваните данни. Тази смяна на парадигмата ще бъде сериозен заряд в ръцете на всички видове индустрии. След като разработчиците вече няма да се тревожат за ниското ниво на съхранение, маршрутизиране и изчисляване, един цял нов набор от приложения могат да бъдат изградени. Приложени независими от данните, които използват. Това ще даде силен начален тласък на зараждащата се икономика на личната информация, в която индивидите решават кой може да вижда какви са детайлите, които касаят лично тях, с каква цел и с какво възможно финансово възнаграждение.

Такава система е и визията на MaidSafe, шотландска софтуерна компания, която работи в сферата на децентрализираната компютърна мрежа. SAFE (Secure Access For Everyone/Безопасен достъп за всеки) Network е автономна, равноправна / peer-to-peer / мрежа, създадена чрез свързване на компютрите и смартфоните на потребителите заедно. Тя е проектирана да разрешава много от настоящите технически, управленски и обществени проблеми с централизирани мрежи: липса на конфиденциалност и сигурност на данните, цензура и масирано консолидиране на контрола от

няколко силни действащи лица.

Този документ очертава как SAFE мрежата е изградена, за да се постигнат тези цели. Макар че е малко техническо на места, той е предназначен до голяма степен да бъде като учебник за начинаещи. Четейки го, дори тези с много малко техническо знание, трябва да могат да получат едно разбиране за това какво е SAFE мрежата. Междувременно, за тези, които искат по-голяма задълбоченост, има много указания къде могат да намерят повече от съответната информация.

1. Заявление за намерение

Световната интернет мрежа днес е много далеч от това, което първоначално е създадено от сър Тим Бърнърс-Лий и неговите колеги преди по-малко от три десетилетия. Неимоверно по-мощна и разпростираща се, отколкото тези учени някога биха си представили, че мрежата може да бъде. За съжаление тя също така служи и за централизиране на властта, богатството и контрола. Две корпорации, Google и Facebook, сега контролират 70 процента от разходите за онлайн реклама в момента, в който се пише това ръководство, и вероятно е много повече, когато вие го четете.

> Централизираното съхранение на данни върху корпоративни сървъри осигурява една неустоима „каца мед" за всяка т.нар. „черна шапка", която търси вариант да се докаже.

Навсякъде другаде, гигантски търговци като Amazon например, използват своя мащаб, политическо влияние и международен отпечатък, за да унищожат местната конкуренция, създавайки виртуален монопол в много сфери, и тези същите компании са също така и най-големите доставчици на облачни услуги, които все повече използват всички наши данни. Накъдето и да погледнете, историята е една и съща: централизация, консолидация, хомогенизация и монополизиране.

Тази централизирана търговска инфраструктура също така предоставя и перфектната вече готова рамка за наблюдение от правителството, както Едуард Сноудън разкри така драматично преди няколко години. И тъй като ние ставаме все по-зависими от нея, тази инфраструктура става все по-пикантна цел за враждебно настроените държавни субекти, които не само я използват, за да разпространяват дезинформация и раздори, но също така могат да извадят от строя критична инфраструктура с добре таргетирани DDoS /атака за отказ на услуга/ и злонамерени атаки с правдоподобно отричане и без да е нужно да направят и една стъпка на чужда земя.

Разбира се, ние не трябва да се притесняваме единствено от хакери, разполагащи с добри ресурси и подкрепени от правителството. Централизираното съхранение на данни върху корпоративни сървъри осигурява една неустоима „каца мед" за всяка т.нар. „черна шапка", която търси вариант да се докаже. Телекомуникационният гигант в Обединеното кралство, TalkTalk, беше хакнат от няколко тийнейджъра – буквално в една задна стаичка – и това се случва още преди да започнем да говорим за Yahoo, Equifax, Target, Tesco Bank и много други. Казано с прости думи: нашите данни – което означава нашите онлайн идентичности, основата на начина по който оперираме в съвременния свят, нашите „дигитални души" – не са в безопасност на сървърите на компаниите. Въпреки всичката си слава, интернет е разрушен. Той се е отдалечил доста от оригиналната си визия. В момента той е машина за цензура, пропаганда и централизиран контрол, който се храни с нашите лични данни. Той би могъл и би трябвало до е нещо много по-добро от това.

Решението на MaidSafe е да създаде сигурна, автономна, ориентирана към данните, равноправна /peer-to-peer/ мрежа като алтернатива на настоящия модел, ориентиран към сървър. Вместо да има централен сървър или център за данни, индивидуалните файлове се разделят на части, шифроват се и се разпространяват из мрежата. Потребителите разполагат с пълен контрол върху файловете, които създават. Те са устойчиви на DDoS /атака за отказ на услуга/, зловредни и хакерски атаки и не могат да бъдат централно кооптирани и контролирани от монополистични кооперации и правителствени интереси. Като платформа, такава мрежа би могла да постави началото на цели нови бизнес модели, както старият интернет направи в началото на века.

Все повече и повече хора споделят това виждане, включително и самият сър Тим, и някои от нас работят усилено, за да го превърнат в реалност.

Разкажи ми повече (линкове за кликване)

Автономни мрежи за данни и защо светът се нуждае от тях (MaidSafe блог)
Силата на тълпите - Част първа: Проблемът (MaidSafe блог)
Тим Бърнърс-Лий за бъдещето на мрежата: „Системата се проваля" (Guardian)
Една децентрализирана мрежа ще върне силата на хората онлайн (Techcrunch)
Отделна мрежа за предприятията и индустриален интернет за нещата (Meshdynamics)
Парадигмата се сменя заради децентрализираната мрежа (Ruben Verborgh блог)

2. Кратка история на децентрализираните мрежи

Децентрализираните или peer-to-peer (P2P) мрежите не се нещо ново. След пускането на Napster на първи юни, 1999 година, те главоломно превземат света, най-вече заради споделянето на файлове. Тези мрежи позволяват на потребителите от цял свят да се свързват едни с други и да споделят данни като филми, книги и музика. През 2010 година, повече от половината от целия интернет трафик се приписва на P2P.

Но използването на тези технологии не се ограничава просто до споделяне на файлове. Freenet стартира през март, 2000 година, позволявайки на хората да публикуват децентрализирани уебсайтове (Freesites). Freesites не се съхраняват на централни сървъри, но вместо това се разпределят из машините на потребителите на кодираната мрежа.

Малко след това е създаден BitTorrent протоколът от Брам Коен. BitTorrent бил и все още е особено подходящ за прехвърлянето на файлове в P2P модел, позволявайки едновременно сваляне от множество пиъри.

Следващата значима разработка пристига след финансовия крах през 2008 година, който почти накара глобалната икономика да падне на колене. През 2009 година Сатоши Накамото пуска на пазара Bitcoin и дава на света една децентрализирана дигитална валута, която не се контролира от банка, правителство или институция. Блокчейн – основният камък, който записва всички Bitcoin транзакции – беше нещо съвсем ново, разрешаващо с един удар трудния и отдавнашен проблем за създаване на безверен източник за истината на транзакциите. Връзките между Bitcoin възлите не са шифровани, но собствеността на мрежовите „адреси" могат да бъдат доказани чрез използването на частни криптографски ключове в Public Key Infrastructure (PKI) /Инфраструктура за публични ключове/. От тук идва и терминът криптовалута.

SAFE мрежата е следващата голяма стъпка в еволюцията на P2P мрежите, комбинирайки визията за децентрализирано споделяне на файлове и уеб сайтове, заедно с вътрешна крпитовалута -Safecoin- и няколко допълнителни иновации за повишаване на сигурността, неприкосновеността, изпълнението и стабилността. MaidSafe (компания, базирана в Айр, Шотландия) проучва и разработва този проект от 2006 насам. Целта е да се разработят и да се активират следните характеристики:

- Пълно съхранение на криптирани данни и споделяне на файлове със 100 процента непокътнатост на данните.
- Способност да се влиза в мрежата анонимно, използвайки инфраструктурата с публичен ключ.
- Способността да се създават услуги за комуникация и публикуване, устойчиви на цензура.
- Увереност в това, че всички данни са 100 процента безсървърни, криптирани и

децентрализирани.

- Увереност в това, че мрежата е автономна и самолекуваща се.
- Елиминиране на нуждата от централизирани сървъри и тракери.
- Инкорпориране на бърза и мащабна криптовалута която да позволява обмена на стойност, освободена от таксите за транзакция.

Комбинирането на тези характеристики дава на потребителите свободата безопасно да съхраняват данни върху мрежата. SAFE също така им позволява безопасно да споделят данни с другите и да публикуват уебсайтове, използвайки защитени комуникационни канали. Нови браузъри и уеб приложения комуникират с мрежата чрез Application Programming Interfaces (APIs) /Програмни интерфейси за приложения/, които дават възможност да се подобри поверителността, както и високо защитени форми на имейли, съобщения, сърфиране; Domain Name System (DNS) /Система за имена на домейни/; чатове; и всякакви други технологии, които понастоящем се използват в интернет.

Разкажи ми повече (линкове за кликване)

Napster (Wikipedia)
Freenet (Wikipedia)
BitTorrent (Wikipedia)
Bitcoin: A Peer-to-Peer Electronic Cash System (Whitepaper)

3. Напълно автономна мрежа за данни

В основата си, SAFE е една „автономна „мрежа за данни". Това означава, че тя е в състояние да управлява и оптимизира работните товари, маршрутизацията, излишъкът в системата, аутентификацията, контрол на достъпа, и други мрежови задачи и такива за съхранение, без каквато и да е човешка намеса. За разлика от настоящия интернет, инфраструктурата на SAFE не е дефинирана от група външни сървъри, виртуални машини /Virtual Machines (VMs)/, притежавани места за съхранение и идентифицируеми възли. За разлика от блокчейните, тя е проектирана да съхранява и управлява данни на живо, а не указатели към данни и да извършва транзакции в реално време. И за разлика от BitTorrent, не разчита на централизирани компоненти в мрежата, за да локализира и проследява файлове.

> Няма абсолютно никаква човешка намеса, освен потребителите, които стартират самоконфигуриращият се, самолекуващ се софтуер.

Промените, до които ще доведе една напълно автономна мрежа, която се грижи за всички аспекти на подсигуряването, управлението и трансфера на данни, се простират надалеч. Няма хора, които да определят цените, няма променящи се конфигурации, които да накарат нещата да проработят, няма данни, които се дърпат на диск, няма как да се излъжат правилата, които управляват възлите – абсолютно никаква човешка намеса, освен потребителите, чиято единствена задача е да стартират самоконфигуриращият се, самолекуващ се софтуер, заедно с други потребители, които вършат същото нещо. Мрежата решава какви са цените, наградите, как се защитават данните, комуникациите и изчисленията. Ние през това време може да правим нещо доста по-полезно с времето си!

Мрежата SAFE замества три от седемте мрежови слоя на OSI модела за подобряване на сигурността, неприкосновеността и автономността.

Двете страни на мрежата - Клиенти и Трезори (Хранилища)

Мрежата SAFE може да се разглежда като защитен, кодиран слой, който се намира на върха на настоящия интернет, позволявайки съхранението и работата в мрежа на автономни данни чрез заместване на три от седемте мрежови слоя на OSI. Тя има два основни компонента: Трезори (Хранилища) и Клиенти.

KEEP IT SIMPLE!

SAFE мрежата се състои от машините на нейните потребители, свързани заедно от софтуер. Има два основни вида възли: Клиенти и Трезори. Клиентският софтуер позволява на потребителите да имат достъп до мрежата, докато Трезорите предоставят съхранение, маршрутизиране и сигурност на данните и начин на печелене на Safecoin валута. Един компютър може да бъде и двата вида възела по едно и също време.

Ядрото на SAFE мрежата е образувано от възли, наречени Трезори. Трезорите са програми, които хората (фермерите) управляват на своите компютри, свързвайки устройствата към всеки друг използващ съществуващ протокол като например TCP UDP и pTP. Трезорите позволяват на потребителите да разрешат на SAFE мрежата да съхранява данни на техните устройства, потенциално печелейки Safecoin валута когато правят това (виж глава 7). Трезорите също така управляват данните и маршрутизирането им из мрежата, предаването на съобщения и подсигуряват валидността на събития, възникващи в мрежата.

WHAT DOES THAT MEAN?

Трезори – възлите, които изграждат SAFE мрежата се наричат Трезори. Състоят се от софтуер, който върви върху устройствата на потребителите и комуникира с другите Трезори. Трезорите също така съхраняват данни във формата на криптирани парчета, срещу което те могат да печелят Safecoin чрез фермерство, когато се свалят тези данни от други потребители.

Клиент – програма, която позволява на потребителите да се свързват към мрежата и да се възползват от нейните услуги. Понастоящем това се осъществява чрез Peruse браузъра.

Peruse – браузър за сърфиране в SAFE мрежата.

Фермерство – действието, чрез което се печелят Safecoin чрез предоставянето на капацитет за съхранение, изчисления и интернет трафик, които изграждат мрежата.

Safecoin – валутата на SAFE мрежата, която се печели чрез съхраняване на данни, харчи се за закупуване на място в мрежата и подлежи на размяна между потребителите на мрежата като дигитален кеш.

Трезорът

Софтуера на Трезора е малък изпълним файл, който свързва машината на потребителя към SAFE мрежата. Той управлява съхраняването на късовете данни върху компютъра на потребителя и по този начин предоставя капацитет за съхранение на мрежата. Той също така маршрутизира и кешира криптираните късчета данни из мрежата, използвайки така изцяло криптираните връзки към други Трезори.

Чрез маршрутизиране и съхраняване на данни, Трезорите образуват сърцето на SAFE мрежата. Трезорите са логически събрани в малки групи, всяка от които е отговорна за грижата за съхраняваните данни в определен обсег от адреси, тези малки групи се наричат Секции (виж глава 4).

Формирането, сливането и разделянето на тези групи от възли се случва по напълно автоматичен начин. Същото важи и за маршуритизирането на късовете информация из мрежата. Няма централни сървъри или агенти (както BitTorrent тракерите), които да са нужни за формирането на тази мрежа. Трезорите следват набор от правила за създаване и поддържане на мрежата, която не изисква централен орган, който да контролира процедурите. Трезорите имат „personas" /персонажи/, които да им помагат да управляват различните задачи (виж глава 8).

Включването на Трезор в SAFE мрежата се нарича фермерство, тъй като потребителите се грижат за данните, докато те се използват и в този момент те могат да получат заплащане за своите усилия.

Включването на Трезор в SAFE мрежата се нарича фермерство, тъй като потребителите се грижат за данните, докато те се консумират и в този момент те могат да получат заплащане за своите усилия.

Клиентът

Точно както не е нужно да управлявате уеб сървър, за да използвате мрежата, не е нужно да управлявате и Трезор, за да имате достъп до SAFE мрежата. Обикновените потребители взаимодействат с мрежата чрез клиента. Това е част от софутера, който в момента е вграден в Peruse браузъра, който позволява да се осъществеюи сигурна връзка с Трезорите, които изграждат SAFE мрежата, докато се скриват IP адресите на потребителите от самата мрежа. Всеки потребител (дори да не е влязъл в системата) е способен да изисква (GET) безплатно данни от мрежата. Например, потребителите могат да сърфират в safe://сайт или да свалят песен или филм, публикувани като публични, и това няма да им струва нищо. Само когато потребителят иска да съхранява (PUT) данни в мрежата, тогава е нужен акаунт с малко количество Safecoin в него.

Кажи ми повече (линкове за кликване)

На прага на автономните мрежи (Enterprise Networking Planet)
Автономни мрежи (MaidSafe whitepaper)
Внедряване на Хранилище в SAFE мрежата (Github)
OSI модел на мрежовите слоеве (Wikipedia)
Клиентска библиотека на SAFE (Github)
Peruse браузър (Github)

4. Архитектурата на SAFE мрежата

Основна цел на MaidSafe е потребителите да могат да сърфират, създават и споделят файлове също толкова лесно както го правят в настоящия интернет, но с доста повишена защита на личните данни, сигурност и контрол върху данните им. SAFE мрежата е проектирана така че да е лесна за използване и от разработчиците, като за тях това е просто малък скок от това, което им е познато по отношение на използваните интерфейси за приложения /APIs/. Все пак, онези, които желаят да изпълняват по-сложни задачи на ниво система, ще имат нужда да се разровят по-дълбоко в нейната архитектура. Очевидно има някои големи разлики между традиционната връзка клиент-сървър и децентрализираните системи. Тази глава предоставя кратко въведение по темата.

Секции
Първата стъпка в разбирането на архитектурата на SAFE мрежата е да се да се хвърли един кратък поглед върху хеш-таблиците на разпределение (distributed hash tables /DHTs).

KEEP IT SIMPLE!

За да намерите данни върху децентрализирана разпределена мрежа имате нужда от карта. Хеш-таблиците за разпределение (DHT) изпълняват тази функция като предоставят издирваща услуга за локализиране на данни. Данните се съхраняват според уникална особеност – техният хеш. Той е същият както и неговият мрежови адрес. SAFE мрежата се дели на Секции с малки групи възли (Трезори) отговорни за управлението на данните в една Секция. Колкото повече възли има в мрежата, толкова повече Секции ще има, и толкова по-устойчива става на сривове или атаки.

Петър Маймунков и Давид Мазирес пускат на пазара разпределителната хеш таблица Kademlia през 2002 година. Идеята е, че възлите в мрежата покриват основния мрежов слой с различна система на възлова идентификация. Така че възелът (в този случай Трезор) може да има IP адрес 96.251.182.97, докато той използва 17846cb8a4b53c9e44c616d2415a15984283eee975a1dac8f488dd91d0aed1cd като уникален 256-битов адрес в XOR пространството.

Изключително битовия OR (XOR) има характеристиката всеки адрес да има уникално разстояние към който и да е друг адрес в целия обхват на адресите. XOR дистанцията няма отношение към физическата дистанция. Всъщност две отделни файла с информация върху мрежата могат да бъдат с много близък XOR-wise но да се намират на машини, разположени на двата края на света.

MaidSafe излезе с подобрение на Kademlia чрез разделяне на целия обсег от 256-битови адреси в т.нар. 'Disjoint Sections' /Разединени Секции/, или Секции накратко. В цялото 256-битово адресно пространство има 2256 -1 възможни адреса, което е изключително голям брой, който трябва да се управлява, но може да бъде разделено на по-малки Секции на база на адреса, като всяка Секция се управлява от малка група от Трезори.

WHAT DOES THAT MEAN?

Разпределителна хеш-таблица – карта на пътя към данните съхранявани върху разпределящата мрежа.

XOR нетуъркинг – начин за случайно разпределяне на физическото местоположение на данните върху разпределителната мрежа и подсигуряването на всяко местоположение да е уникално.

Секция – подгрупа на всички адреси на мрежата. Данните, съхранявани на всяка Секция биват контролирани от специална група възли (Трезори).

Размер на групата – параметър, определящ минималния брой възли, които могат да контролират една Секция.

Bootstrapping /самозареждане/ – стартиране на SAFE мрежата чрез свързване на минимален брой възли заедно. Самозареждането също така се използва за въвеждане на нов възел (Трезор) присъединил се към мрежата.

Bootstrap сървъри – малък брой сървъри, управлявани от MaidSafe върху които се свързват новите Трезори (чрез proxy) когато се присъединят към мрежата. Техните IP адреси са предварително зададени в софтуера на Трезора.

Хеш функция – функцията, използвана, за да картографира данни от произволен размер до данни с фиксиран размер (например 256-битов низ от знаци) се нарича хеш. Всяка промяна в оригиналните данни ще даде резултат в абсолютно различен хеш. SAFE използва SHA-3 хеш функция.

Датачейн (Datachain) – записване на членството в Секциите и мрежовите събития, които се държат от всеки Трезор в тази секция.

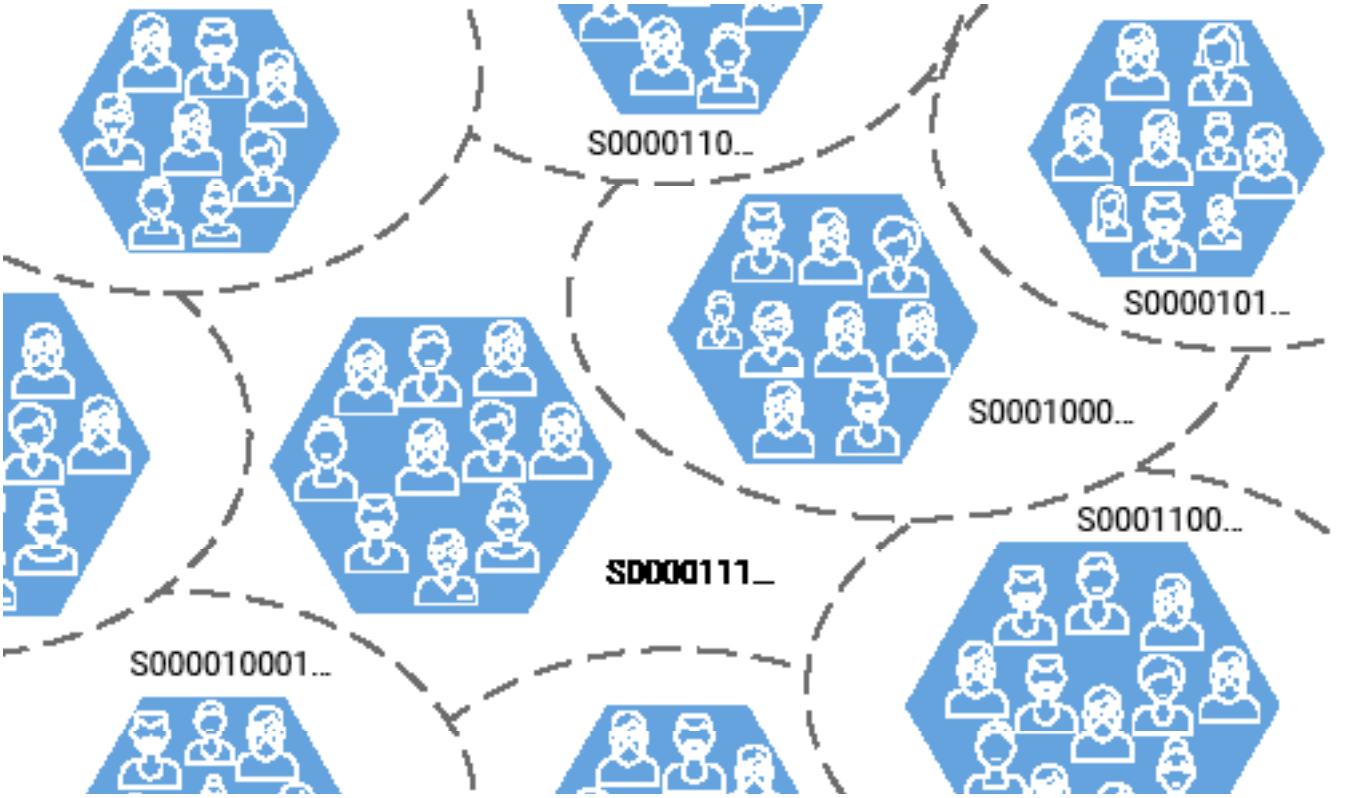
При присъединяване или връщане в SAFE мрежата, един Трезор не може просто да избере свой собствен XOR адрес. Вместо това, то трябва да изчака Секцията да го избере и да го направи част от мрежата. Когато това се случи, Трезора получава маршрутизираща таблица от Секцията и научава диапазона на адресите на данните, за които тя е отговорна.

Данните, съхранявани на SAFE мрежата първо се разделят на късове, хешират се и след това се кодират. Тези късове се прокарват през хеширащ алгоритъм, за да достигнат до създаването на уникален 256-битов код или хеш за всеки един къс. Само късовете, които са абсолютно идентични ще имат същата хеш стойност. Този хеш служи като XOR адрес в мрежата, където тези късове ще бъдат съхранявани, което от своя страна определя групата на Трезорите, които ще го управляват.

> "Хеша на къс информация служи като XOR адрес в мрежата, където този къс ще бъде съхраняван, което от своя страна определя групата на Трезорите, които ще го управляват."

И така късовете с хешове, които са в рамките на определен

Всяка Секция (обсег от XOR адреси) се управлява от група от Трезори. Най-надеждните Трезори в групата се наричат „Старейшини" /Elders/. Старейшините имат право на глас и комуникират със старейшините в съседните Секции.



диапазонов адрес (да речем от 000010... до 000011...) ще бъдат защитени и съхранени от групата на Трезорите, които управляват тази определена Секция. Членството в тази група ще се промени с времето тъй като непрекъснато има възли, които се разкачват или се свързват отново към мрежата. Когато мрежата е самозареждаща се, минимум осем Трезора са отговорни за целия 256-битов обсег на адреса (2256 -1 адреси). При присъединяването на повече Трезори, групата ще се раздели на две. И ако тези нови групи привлекат нови Трезори, те също ще доведат до повтаряне на този процес. Затова с 1 000 групи, пространството на адресите се разделя на 1 000 Секции. С 100 000 групи, то се разделя на 100 000 Секции, и т.н.

Ако групата от Трезори управляващи определена Секция, нараснат значително повече от средното (усредненият модел е около 12 Трезора), по принцип тя ще се раздели на две по-малки групи, като всяка от тях управлява по-малък Сектор (диапазон от адреси). Обикновено това се случва преди членството в групата да надвиши 22 Трезора.

По същия начин, ако Трезори напускат групата и броят им спадне под зададено ниво, което е определено като параметър за размер на групата, тогава Секцията ще се подтикне да търси сливане с подобна група (някоя, която се управлява от близък Сектор). Понастоящем, размерът на групата е 8.

Консенсус и кворум

Групата на Трезорите управляваща Раздел винаги ще се опитва да постигне консенсус помежду си за всяко състояние или действие. Те също така „подписват групово" съобщения, които пътуват из по-широката мрежа, така че други Трезори в други групи да могат криптографски да проверяват всяко съобщение и действие. Тези групови подписи се съхраняват в Датачейн (верига от данни), която е защитена и се поддържа от всички Трезори в групата. Всички събития, като например образуването на групата, разделянето и сливането се записват и се съхраняват по този начин.

За да се случи нещо в мрежата, например съхраняване на късове данни на мрежовия адрес, групата от Трезори отговорна за този адрес трябва да реши че действието е законно и валидно. Ако размерът на изисквания кворум (например, 5 от 8 Хранилища) се достигне, действието ще продължи. Запис на всички такива събития се пази в контейнер, който се нарича Датачейн („верига от данни"). Всеки нов Трезор, който се присъединява към групата, може да прочете веригата от данни. Групите, също така споделят информация относно събитията и настоящото състояние на други групи, които се намират близо до тях.

Всички събития в групата са криптографски проверими от всеки Трезор, който се присъедини към групата. Тези събития също така се съхраняват от други близки групи (като се измерват в XOR разстояние) в мрежата. Така че групата от възли, управляваща Секция S (0000110) знае и всички възли в групата управляваща също и SS (0000111). Тя също има достъп до част от Датачейна (веригата от данни), съдържаща цялата информация за тази група. И тъй като те държат записите на състоянието на Секциите, Датачейна позволява на мрежата сама да се възстанови в случай на сериозен срив.

Колкото по-близо е Трезора до определено адресно пространство на SAFE мрежата, толкова повече информация има то за данните съхранени на този адрес. И логично, колкото по-отдалечен е един Трезор, толкова по-малко информация има той. Освен когато мрежата е много малка (по-малка от 22 Трезора), няма Трезор в SAFE мрежата с пълен преглед върху мрежата. Колкото по-голяма става мрежата, толкова по-защитена става тя, защото всеки отделен Трезор ще оказва влияние върху все по намаляващ диапазон от адреси.

Действие или събитие, което се случва в Секция, е валидно само ако кворума на групата го е одобрил. Промяна на състояние трябва да бъде подписано от определена част от тази група, известна като размер на кворума. Трезорите следват определени правила, които са определени от размера на кворума. В група от осем Трезора, са нужни пет, за да се одобри едно действие (като например искане от страна на Клиента да съхрани къс данни); в този случай, размерът на кворума е 62.5 процента.

Забележете, че няма външни проследяващи или мениджъри, включени в което и да е от решенията на тези групи. Група от Трезори (без значение колко малка или голяма е) оперира по един напълно автономен начин в рамките на мрежата.

> Няма Трезор в SAFE мрежата с пълен преглед над мрежата.

Кажи ми повече (линкове за кликване)

Преглед на техниките за сигурност на DHT (Globule)
Kademlia: Peer-to-peer информационна система, базирана на XOR метрика (Whitepaper)
Разпределителни хеш таблици (MaidSafe Whitepaper)
DHT-базирана NAT Traversal (MaidSafe Whitepaper)
Структура на данни, разделени на групи (Wikipedia)
Разпределяне на раздели (MaidSafe RFC)
Маршрутизиране – специализирано съхраняване на DHT (MaidSafe repository)
Архитектура на SAFE мрежата (Ian Coleman)
Верига от данни: Какво? Защо? Как? (David Irvine, Metaquestions блог)

5. Възраст на възела и доказателство на ресурс

Трезор, който се присъединява към мрежата, изисква IP адресите на другите Трезори, за да се свърже към тях. За тази цел MaidSafe предоставя малък брой свързващи /bootstrap/ сървъри. Това са свързани с интернет машини, които движат софутера на Трезора. Публичните ключове на свързващите сървърите са кодирани в бинарния код на Трезора, което означава, че всички комуникации се кодират от самото начало.

KEEP IT SIMPLE!

Точно както на децата не им се позволява да гласуват на избори, така и един възел (Трезор) не може да гласува за мрежови събития – като например присъединяването на нов член или съхраняването на къс информация, или разделяне на Секция и сливания – докато не се докаже, че е надежден (Доказателство на ресурса/ Proof of Resource). Един възел печели доверие чрез преместване от Секция в Секция и когато действа надеждно, всеки път се повишава неговата възраст с 1. След като вече е сред най-старите в неговата група (по отношение на възраст), може да му се дадат права за гласуване. Подтикването възлите да се докажат по този начин е важна мярка за сигурност.

Един Трезор се свързва с другите Трезори чрез така наречения „кръст"/Crust/ слой, изпращайки съобщение, че иска да се присъедини към мрежата. Една група от Трезори, които имат отворено място могат да достигнат до консенсус и да позволят на новия Трезор да се присъедини към групата. В този случай Трезорите ще изпратят запитване за Доказателство на ресурса, при което новия Трезор трябва да докаже, че може да предостави определено количество трафик и капацитет на процесора.

Ако новия Трезор успешно премине теста за Доказване на ресурса, групата ще му даде

WHAT DOES THAT MEAN?

Crust – съкратено от Connected Rust, Crust е софтуерна библиотека, писана на програмен език Rust, за установяване и поддържане на надеждни партньорски / peer-to-peer/ мрежови връзки сред широк обсег от мрежови условия и протоколи.

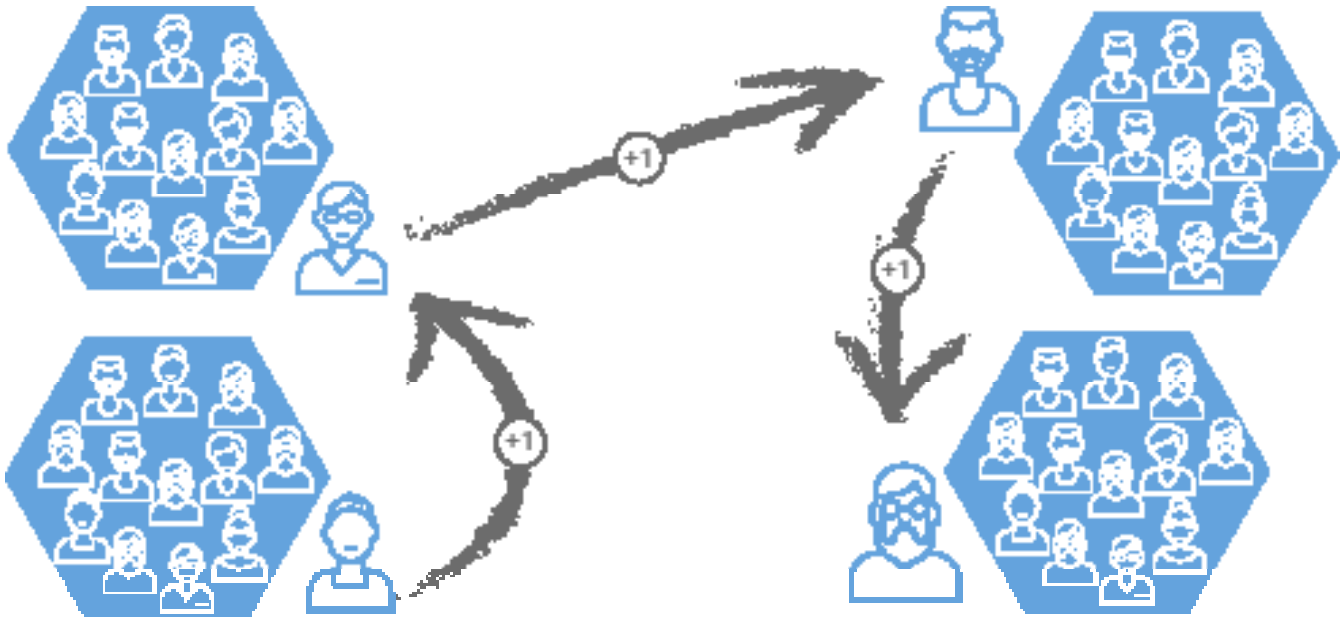
Доказателство за ресурса - 1. тест, дали Трезора, който иска да се присъедини към мрежата има достатъчно трафик и мощност на процесора. Ако се провали на теста, няма да му бъде позволено да се присъедини. 2. Понякога се правят случайни проверки от управляващите възли, за да се уверят, че Трезора действително поддържа късовете информация, които се предполага, че съхранява. Ако в този случай се провали (като не предостави исканото доказателство) неговата възраст се намалява.

Възраст на възела – мярка за наежеността на един възел (Трезор). След първоначалната връзка, Трезора се мести на случаен принцип от Секция в Секция и изгражда своята репутация или Възраст на възела. След като неговата възраст достигне определена стойност, то може да стане активен участник в решенията на групата.

Churn/разбъркване – действие на Трезори напускащи групата или нови Трезори, които се присъединяват, изисквайки реорганизация на взаимоотношенията и отговорностите. Разбъркването означава, че групите не са статични за дълго.

Старейшина – възел с права за гласуване в неговата секция. Старейшините са просто възлите с най-голяма възраст

Пътят на един Трезор към развитие. Трезорът трябва да се докаже в редица секции преди да има шанс да получи права за гласуване като Старейшина на Секция.



адрес от мрежата в рамките на тяхната Секция и ще стане член с ниска „възраст на възела", което означава, че все още няма права за гласуване и подлежи на преместване към друга Секция във всеки един момент (разбъркване/ churn). Когато един възел напусне групата, той се изпраща на случаен принцип в друга Секция на мрежата, т.е. дава му се нов случаен XOR адрес. Ако групата, която управлява тази нова Секция достигне пълен консенсус за това действие, Трезорът ще се присъедини и неговата възраст ще нарасне с 1.

> Възрастта на възела и разбъркването правят набелязването за атака на определена Секция върху SAFE мрежата близко до невъзможното.

Възрастта на възела е експоненциална функция. Новите Трезори е по-вероятно да бъдат преместени в нова Секция (и това да увеличи тяхната възраст) отколкото по-старите и по-надеждните възли. Трезорите трябва да докажат своята стойност (CPU, трафик, надеждност) пред другите, за да могат да спечелят доверие. Ако това доверие се изгуби, то трябва да бъде спечелено отново. След като веднъж един Трезор достигне до определена Възраст на възела, той може да гласува за събитията в мрежата. Тъй като новите Трезори трябва да доказват своята стойност в различни Секции преди да могат да гласуват, набелязването на определена Секция на SAFE мрежата от атакуващ е почти невъзможно. Затова Възрастта на възела и разбъркването са жизненоважни защитни характеристики.

Само най-надеждните Трезори в Секция, тези Трезори с най-голяма Възраст на възела, имат право на глас. Тези Трезори се наричат Старейшини. Другите Трезори в Секцията просто получават информация за техните решения.

Кажи ми повече (линкове за кликване)

Обяснение на SAFE мрежата
Въведение и технически преглед на SAFE консенсуса
Верига от данни – По-дълбок преглед
Crust- Надеждни p2p мрежови връзки в Rust с NAT traversal
Разбиране на разбъркването в партньорските мрежи (Sigcomm, Research paper)

6. Всичко е криптирано

Всички данни върху SAFE мрежата са защитени от няколко слоя криптиране. Дори публичните данни (като напрмиер блог safe://website/blog) са защитени от криптиране, но в този случай ключовете за премахване на криптирането се споделят с посетителите, за да може данните да са достъпни за тях.

KEEP IT SIMPLE!

Всички данни върху SAFE мрежата са криптирани или се държат в криптирани контейнери. За да съхраните файл върху мрежата, първо трябва да бъде разбит на късове информация, да хешира и след това да се криптира. Тези късове се криптират като се използва хеш от друг къс от същия файл. Това е т.н. само-криптиране, метод патентован от MaidSafe.

На мрежово ниво, SAFE мрежата използва TCP и µTP протоколи и всички данни предвижвани от този протоколи са в кодирана форма от първия бит на данните, изпратен към мрежата. Първата връзка със SAFE мрежата, която Трезора или Клиента прави е към свързващия сървър на MaidSafe, единият от множеството сървъри, управлявани от MaidSafe, който позволяват на нови машини да се присъединят. Публичните ключове за тези свързващи сървъри са кодирани в софтуера на Клиента, така че комуникацията между мрежата и потребителя винаги да е криптирана, и никога да не е обикновен текст.

Клиентите и Трезорите в мрежата получават списък с адреси и публични ключове на други потребители с които да се свържат. Тези връзки също са криптирани от първия бит. По този начин най-ниското ниво на свързване (Crust) принуждава всички комуникации да бъдат криптирани.

Прокси възел за Клиенти
За да се запази анонимността, идентичността на Клиента, който се свързва към мрежата трябва да бъде скрита от възлите (Трезорите) които го обхващат. Поради тази причина връзките между Клиенти и Трезори в SAFE мрежата винаги се осъществяват чрез Прокси възел. Прокси възелът, знае IP адреса на Клиента ще му позволи да се свърже към групата от Трезори като докаже своята интернет скорост (bandwidth). Трезорите не могат да видят IP адреса на Клиента, но те знаят неговият публичен ключ и XOR адрес. Разбира се, връзките между Клиента и групата(ите) са изцяло криптирани.

Прокси възелът е в състояние да предостави услуга на потребителя, свързвайки него или нея към мрежата, без да знае каква ще е активността му/ѝ след това. Групата Трезори към които потребителят е свързан, може до известна степен да знае какво прави потребителят на мрежата, но те могат да идентифицират потребителя само по неговия XOR адрес, но не и по неговия IP адрес. По този начин е гарантирана пълната анонимност.

Само-криптиране на данни

Когато Клиентът качва някакви данни в мрежата (например mp4 видео) те първо биват разбити на парчета с максимален размер 1 Mb и тези парчета, или късове информация, се „само-криптират", процес, който е патентован от MaidSafe, чрез който всеки къс се криптира, използвайки хеша на друг къс от същия файл. Тези криптирани късове след това се разпращат из мрежата, за да бъдат съхранени с хеша на криптирания къс, равняващ се на неговия мрежов адрес. Съхраняват се няколко копия от всеки един къс, най-вероятно върху машини разпръснати из целия свят. Ако едно копие се загуби, друго незабавно се генерира, осигурявайки високо ниво на сигурност. Клиентът запазва ключовете, за да декодира данните локално. По този начин не е нужно никакви ключове или пароли да напускат компютъра или мобилния телефон на човек. Междувременно късовете информация, които се съхраняват в SAFE мрежата са напълно криптирани. Потребителите могат да избират да споделят тези файлове с други като споделят с тях своите ключове. Те могат също така да изберат да направят файловете публични, като в този случай ключовете, които се изискват за декодиране на файловете се правят публично достъпни, като при примера с блога.

"SAFE мрежата предоставя платформа за приложения, която е не само изключително сигурна, но и проектирана да е"

Многослойно криптиране

Както е показано по-горе, SAFE мрежата използва няколко слоя на криптиране, за да защити анонимността и поверителността на потребителя. Няколко допълнителни слоя се активират, когато хората използват директни съобщения или създават публичен профил. Мрежата е проектирана да бъде с „нулево знание" дори до такава степен, че Фермерите не мога да разберат кои късове от кой файл съхраняват те – дори това да е техен собствен файл. Като се използват множество нива на криптиране и като скриват идентичността на своите потребители след първата връзка, SAFE мрежата предоставя платформа за приложения, която е не само изключително сигурна, но и проектирана да е анонимна.

Кажи ми повече (линкове за кликване)

Свързване към крипто библиотека Sodium
Crypto 101
Само-криптиране – данни, които сами се криптират, от само себе си (MaidSafe)
Само-криптиращи се данни(MaidSafe Whitepaper)
UDP Hole Punching (MaidSafe RFC)

7. Фермерство за Safecoin

Основният стимул за операторите на Трезор да се присъединят към мрежата и да си сътрудничат за постигането на основната цел за сигурно място за съхранение, е възможността да спечелят Safecoin. Идеята зад Safecoin е подобна на тази на Bitcoin: да се гарантира, че кооперативното участие е по-рационален курс на действие, отколкото некооперативното участие. Safecoin може да се харчи в мрежата или да се обменя за други валути. Количеството данни, които потребителят може да съхрани на SAFE мрежата зависи от количеството пари (Safecoin) в акаунта на потребителя.

KEEP IT SIMPLE!

Фермерството
е процес при
който потребителят дава под наем
пространство за съхранение на своя компютър и
може да спечели Safecoin, валутата на SAFE мрежата.
Safecoin може да се харчи в мрежата, например като
се качват файлове.

Когато потребителят на мрежата изисква някакви данни, например да сърфира в уебсайт, се случват няколко неща. Първо, софтуерът на Клиента подава заявка за изискваните късове данни. Това съобщение (заявка GET/получаване/) след това се разпространява по мрежата и когато се намерят тези късове, има конкуренция между Трезорите в тази Секция, кой да го достави на мрежата, където то ще бъде насочено към заявителя.

WHAT DOES THAT MEAN?

Фермерство – Трезора изпраща
късове данни, които съхранява към мрежата и в
замяна печели Safecoin.

Опит за фермерство – чрез доставяне на късове данни, когато има заявка за това, Трезора има възможност да спечели Опит за фермерство. Това се осъществява чрез изпращане на валидирана заявка до произволно избран адрес на Safecoin. Ако на този адрес вече съществува Safecoin, която се притежава от някой, Опитът се проваля. Ако там няма Safecoin, се създава такъв и се дава като награда на съответния Трезор, т.е. направен е успешен Опит за фермерство.

Фермерски добив (farming_rate) – променлива, която се използва за привличане или възпиране на фермерството, с цел да се поддържа определено ниво на свободно пространство (около 30 процента от общия капацитет).

MaidSafeCoin – токен на криптовалутата, който ще може да се размеря за Safecoin след като мрежата е активна.

Първия Трезор, който го достави има възможността да бъде възнаграден с един Safecoin. Този процес се описва като Farming Attempt /опит за фермерство/.

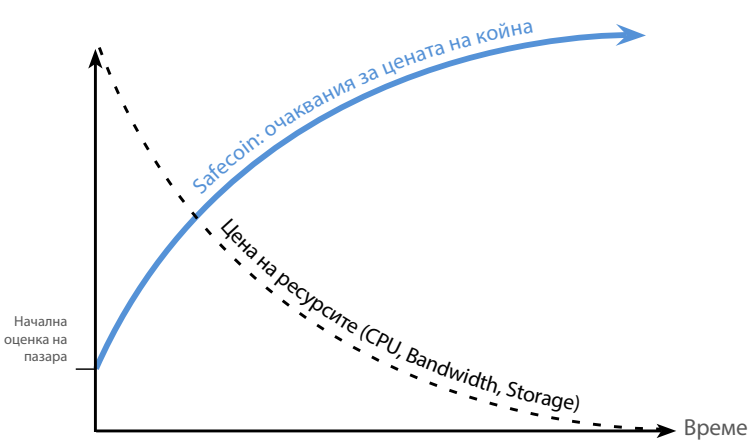
Мрежата винаги ще се стреми да поддържа свободно пространство от поне 30 процента от общия капацитет, за да покрива разединяване или прекъсване в определени части на мрежата. Затова, когато свободното пространство падне под 30 процента от общия капацитет, Фермерския добив ще се повиши и повече Опити за фермерство ще бъдат позволявани, което води до спечелване на повече Safecoins. По този начин Фермерите правят повече пари, изпращайки късове данни към мрежата. Това работи и в обратната посока. Когато има прекалено много Фермери, които предоставят място за съхранение, Опитите за фермерство ще намалеят. Това става автоматично и ефектът е, че създава по-голям стимул за фермерите да предоставят място за съхранение, когато общият свободен капацитет е нисък, и по-малко стимул, когато количеството свободното пространство е голямо.

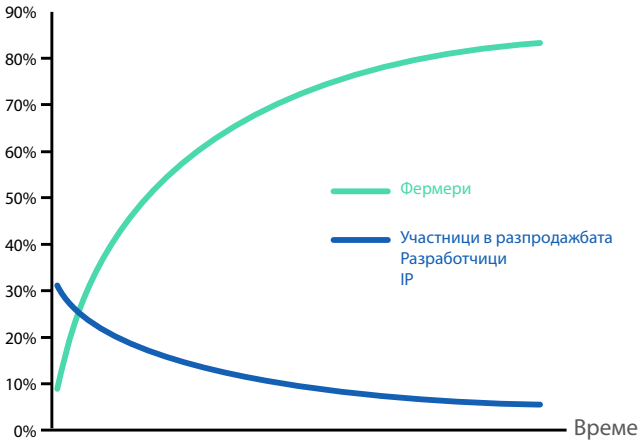
Има по-голям стимул за фермерите да предоставят място за съхранение, когато общият свободен капацитет е нисък, и по-малко стимул, когато количеството свободното пространство е голямо.

Самата мрежа ще се балансира по такъв начин, който е напълно независим от цената на Safecoin. Чрез коригиране на Опита за фермерство според количеството налично свободно пространство на мрежата, данните за съхраняване на потребителите се таксуват на оптимална степен. Докато степента на съхранение е висока (наличното пространство е ниско) потребителите се обезкуражават да съхраняват, помагайки по този начин да се освободи повече пространство. Това динамично ценообразуване ще позволи много конкурентни цени за съхранение на данни.

Всеки, разполагащ с подходящо устройство и достатъчно интернет скорост, е добре дошъл да фермерства и с това да допринася за мрежата – включително и собственици на центрове за данни. За да се минимизира риска от централизация, обаче, използването на огромни фермерски платформи ще бъде икономически неблагоприятно в сравнение с действащите многобройни по-малки възли.

Ресурси и валутата





Safecoin

За разлика от Bitcoins, които са числа в блокчейна, Safecoins са реални файлове, наречени MutableData (MD) единици (виж глава 9). Когато Safecoin си размени собствениците след транзакция, се записва като информация в MD. Пълната история на монетите не се записва, за разлика от блокчейн базираните валути, само предишния и настоящия собственик, което прави Safecoin по близък до фиатните пари (кеш парите). Количеството на Safecoin ще бъде ограничено до 4.3 милиарда монети, и всеки Safecoin ще има своя собствена дигитална идентичност. Safecoins ще се рециклира когато потребителите ги обменят за мрежови услуги, гарантирайки по този начин, че винаги ще има наличност за други потребители, които да печелят.

Забележка: По време на писането на настоящия документ SAFE мрежата е все още преди пускане (Alpha) и Safecoin все още не е вграден. Въпреки това, може да се закупи прокси токен, наречен MaidSafeCoin (MAID) от няколко борси за криптовалути. Когато мрежата стане активна MAID ще се разменят за Safecoin на база 1 към 1.

Кажи ми повече (линкове за кликване)

Фермерство (SAFE Network Wiki)
Вграждане на Safecoin (MaidSafe RFC)
Опит за фермерство (MaidSafe RFC)
Въведение в MaidSafe: какво е това, как работи и как се сравнява с Bitcoin (Blanshey)

8. Ролите на Трезорите

Трезорите, които формират SAFE мрежата имат различни функции за изпълнение. Те насочват и съхраняват късове данни. Те криптографски проверяват съобщенията и се разделят на нови групи или се сливат отново, ако тяхната група стане прекалено малка. Те също така поемат и по дефиниращи роли, които се наричат персонажи.

Клиентски мениджър

Персонажът Клиентски мениджър държи акаунта на всеки Клиент, който е близо до него в пространството на мрежовите адреси - т.е. в неговия Сектор. Всеки клиентски акаунт се управлява от около осем Трезора.

Акаунта на Клиента съдържа детайли за броя късове от данни, които са съхранени върху мрежата от този Клиент и колко нови късове могат още да се качат. Ако акаунта на Клиента показва, че не могат да се качват повече късове върху мрежата (заради недостатъчно Safecoin), Клиентският мениджър на този Клиент отказва всякакви допълнителни запитвания за качване /PUT/, отговаряйки с изписване на грешка LowBalance /нисък баланс/.

Клиентите могат да получат информация за баланса на сметката си като изпратят специфично запитване към техните Клиентски мениджъри (запитване GetAccountInfo /получаване на информация за акаунта/).

Клиентският акаунт в SAFE мрежата е напълно различен от Gmail или Facebook акаунта, тъй като не е свързан към никаква идентичност. Клиентските мениджъри знаят какъв е баланса на Клиента, но за тях той е просто адрес в мрежата. Те не знаят IP адреса на Клиента, нито имат информация за потребителското име, публичната идентичност или нещо друго, което може да свърже Клиента с определен човек.

Мениджър на данни

Персонажът Мениджър на данни, управлява хранилище за късове, в който се съхраняват късове данни и той е отговорен само за тези късове, които се намират в неговия Сектор. Не всеки Мениджър на данни в даден Сектор задължително държи едно такова парче, но всеки е наясно кой партньор го държи.

Кажи ми повече (линкове за кликване)

Мениджър на данни – консенсус без блокчейн (MaidSafe блог)
Въведение и технически преглед на SAFE консенсуса (MaidSafe блог)
Safe_Трезор (Github repository)

9. Видове данни

SAFE мрежата предоставя два вида възможности за съхранение и извличане на данни: Променими данни (MutableData (MD)) и Непроменими данни (ImmutableData). Както подсказват имената, Променимите данни могат да бъдат променяни, докато Непроменимите данни не могат.

Променими данни (MutableData)
Структурата Променими данни се състои от вписвания. Вписването е двойка ключ-стойност (т.е. MD с ключ 1: стойност „банани", ключ 2: стойността „ябълки" има две вписвания). Вписванията могат да бъдат вмъквани, актуализирани или премахвани. Едно MutableData вписване може да съдържа до 1 000 записа и да е с максимум размер 1 Mb данни. Променими данни могат да се използват по различни начини: обществен (напр. уебсайтове), частен (частни файлове) и споделен (групи за лични съобщения) в зависимост от това дали и как са били криптирани.

Непроменими данни (ImmutableData)

Структурата Непроменими данни може да съхранява само единична стойност. Мрежовия адрес на ImmutableData се извлича от хеша на файловото съдържание. Това означава, че файлът не може да се редактира по никакъв начин след като вече е качен – всяка промяна ще доведе до изменение на хеша. Една ImmutableData единица също е ограничена до 1 Mb, но като се използва картата за данни, може да се следи местоположението на файлове по-големи от 1 Mb, които могат да се разделят на късове и тези късове да се съхраняват като отделни ImmutableData единици.

> Дедупликация на данните (Data deduplication) е уникална характеристика на SAFE мрежата, която се постига чрез процеса на само-криптиране.

Дедупликация на данните /Data deduplication/ е уникална характеристика на SAFE мрежата, която се постига чрез процеса на само-криптиране (виж глава 6). Два идентични къса ще имат същата хеш стойност и затова само една от тях е нужно да се съхранява върху мрежата. Бинарните данни и други видове файлове са добри кандидати за съхраняване в мрежата като Непроменими данни. Видовете Непроменими данни се кешират от клиентите и намирането на един и същи файл може да стане по-бързо.

SAFE също така има и характеристика, наречена Opportunistic Caching /опортюнистично кеширане/, при която повече копия на популярните данни се създават по-близо до мястото, където е направена заявката, така че популярните уебсайтове и други информационни канали всъщност ще се ускорят когато имат повече посетители, вместо да се забавят, както това се случва днес в уеб пространството.

Данните се запазват като се използва комбинацията Промени данни и Непромени данни, за да се създаде емулирана файлова система на върха на мрежата, наречена NFS (Network File Storage /мрежово файлово съхранение). NFS съхранява съдържанието на файла като Непромени данни. След това създава запис в MutableData единицата, с името на файла като ключ за вписването и ImmutableData адрес като стойност на вписването. Файлът може да бъде актуализиран като се качи нов ImmutableData файл и след това се актуализира адреса на файла в MutableData структурата, като се насочи към новия файл.

Уебсайтовете върху SAFE мрежата могат да бъдат идентифицирани използвайки URLs адреси, като например safe://service_name.public_id (напр. safe://mysite.alice). Работейки по подобен начин на позната система с интернет имена на домейни (DNS), тези адреси, които се четат от хора, се превеждат в мрежови адреси върху SAFE, използвайки Decentralized Naming System / децентрализирана система за наименуване/ - също с абревиатура DNS.

WHAT DOES THAT MEAN?

Файлово съхранение върху мрежата /Network File Storage (NFS)/ - интерфейс за приложения, който позволява на Клиента достъп до колекция от файлове, съхранявани на SAFE мрежата.

Децентрализирана система за наименуване /Decentralized Naming System (DNS)/ - аналог на системата с имена на домейни при стария интернет (също с абревиатура DNS), това е система, която превежда уеб адреса, който се чете от човек, в мрежови XOR адрес.

Публично ID – избраното име за акаунта (напр. alice или maidsafe). Един акаунт може да регистрира какъвто и да е брой публични IDs, стига те да не са били регистрирани преди това.

Име на услуга – име на услугата, като например уебсайт, имейл или приложение за чат. Така че ако уебсайтът на Alice е наименуван mysite, URL-то му ще бъде mysite.alice.

Карта за данни – запис, запазен в акаунта на Потребителя, който съдържа цялата информация, необходима за декриптиране на файла на потребителя, съхранен върху SAFE мрежата.

Вид таг – позволява на приложението да идентифицира вида данни: 15001 Public ID; 15002 Service Name; 15003 Email ID; 15004 Email Archive.

Опортюнистично кеширане /Opportunistic caching/ - автоматично създаване на повече копия на популярни данни, близо до мястото, от къде е подадена заявката, така че популярните уебсайтове и други информационни данни да се ускорят когато има повече посетители, а не да се забавят, както се случва днес в мрежата.

Върху SAFE мрежата, DNS взема хеш от публичния ID, и така 'alice' в нашия пример става низ от 256 знака. Браузърът взима този хеш и го използва като адресът, с който да намери кореспондиращата MutableData единица от която той получава адресът от сайта върху NFS, която съответства на името на услугата.

Браузърът намира контейнера на услугата за публичното ID 'alice', и извлича записа, чийто ключ съвпада с името на услугата 'mysite'.

Стойността, съхранена в този запис, съдържа препратка към NFS контейнера (MutableData единицата с изписан таг е установена на 15002), където браузъра може да извлича имената на файловете, които изграждат уебсайта заедно с адресите на ImmutableData единици, където се съхранява съдържанието на файловете. С тази информация, може да започне извличането на имената на файловете и препращането им към потребителския интерфейс.

Кажи ми повече (линкове за кликване)

Промени данни (MaidSafe RFC)
Разпределяща мрежа с опортюнистично кеширане на данни (MaidSafe)
Maidsafe NFS API документация

10. API /приложният програмен интерфейс/ на SAFE

Приложният програмен интерфейс на SAFE се използва от разработчиците, за да се взаимодейства директно със SAFE мрежата. Може да се използва в JavaScript, Node.js, Java и C#.

Приложенията свързващи се към SAFE мрежата, получават различни нива на достъп до данните чрез API в зависимост от това дали са оторизирани или не. Приложенията, които не са оторизирани имат достъп само до публичните данни, каквито са уебсайтовете. Оторизираните приложения имат достъп до пълния набор от мрежови функционалности.

Източник: Joseph Meagher

SAFE мрежата има контейнери по подразбиране, в които се съхраняват определени видове файлове. Например _documents се използва за съхранение данни свързани с документи; _downloads е контейнер за изтегляне на съдържание; _ music е мястото за съхраняване на музикални файлове, и т.н. Два специални случая са _public – за съхраняване на некриптирани данни (контейнера е криптиран дори и ако неговото съдържание не е), и _ publicNames – за съхрънение на публични IDs, които може да се търсят за публична информация.

Разработката на приложенията за SAFE мрежата не е по-различна от стандартната практика. Има safe_app библиотеки, базирани на платформата на приложението, за което са предназначени. Както е споменато, Node.js, Javascript и C# са най-добре поддържани в настоящето. Уеб приложенията могат да се изграждат като се използва приложен програмен интерфейс DOM на Peruse браузъра.

Оторизиране

Приложенията трябва да бъдат оторизирани, преди да получат достъп до данните в мрежата.

По подобен начин на познатия OAuth процес, приложението изпраща заявка, използвайки библиотеката за оторизиране. Когато оторизацията е одобрена от потребителя, приложението получава токен, който се използва за свързването му към SAFE мрежата. Оторизацията се постига чрез призив на приложението към Удостоверителя, който в момента е обединен с браузъра на SAFE мрежата - Peruse.

Оторизацията е финно филтрирана. Едно приложение може да създаде свой собствен контейнер и да изиска достъп до контейнера по подразбиране или до контейнерите на други приложенията чрез оторизирано запитване. Разрешения за READ, WRITE, UPDATE, DELETE, MANAGE /четене, писане, актуализиране, изтриване, управление/ могат да бъдат заявени за всеки контейнер.

Приложеният програмен интерфейс се отличава с множество методи позволяващи на програмните приложения да си взаимодействат с различните типове Промениими данни и Непромениими данни (виж глава 9), да пишат и да извличат данни от мрежата.

CipherOpt и Crypto APIs

Safe_app библиотеката също предоставя и API функции за криптиране. safeCipherOpt API предоставя функции за създаване на различни криптиращи опции, които да се приложат, докато се съхраняват данни в мрежата. По време на писането на това ръководство, се пишеше интерфейса за управление на ключовете.

Има три вида CipherOpts:

- Plain /опростен/ - Даните не се кодират.
- Symmetric /симетричен/ - Данните се криптират със симетричен ключ.
- Asymmetric /асиметричен/ - Данните се криптират, използвайки ключова двойка

API функциите на safeCrypto предоставят удобни криптографски функции, включително хешинг и генерирани двойки ключове.

Приложен програмен интерфейс DOM

Уеб приложение (програма) може да комуникира със SAFE мрежата и Удостоверителя чрез директно взаимодействие с програмния интерфейс DOM на браузъра на SAFE, т.е. window.safe* functions.

Този API е доста подобен на Node.js API, главната разлика е, че уеб приложението получава поддръжка за всеки от обектите, които се инстанцират когато взаимодействат с API, т.е. SAFEApp и MutableData например. Уеб приложението изисква да се освободят поддръжките, предоставени чрез извикване на специфична „освободи" функция върху всеки от получените токени.

Кажи ми повече (линкове за кликване)

SAFE Network DOM API
SAFE Network Node.js API
safeCrypto API
safeCipherOpt API
New Auth Flow (MaidSafe RFC)
Async safe_core (MaidSafe RFC)

11. Обещанието на SAFE мрежата

SAFE мрежата все още е в процес на разработка. Докато много характеристики и функционалности вече са се доказали в тестови условия, други, включително Datachains и Safecoin, тепърва трябва да го направят. Както с всяка иновативна експериментална технология, доказателството „за ястието е като се опита".

Но да предположим за момент, че мрежата е успешна и широко приета за различни случаи на употреба, включително сърфиране из Интернет, свързване, сигурност на данните, управление на личната информация, медицински досиета и други. Как би изглеждал свят с работеща SAFE мрежа?

Първо, повечето стратегии за кибер атаки, които са широко разпространени днес, ще приключат. DDoS /атака за отказ на услуга/ няма да работи тъй като мрежата просто ще маршрутизира около засегнатите възли. Вирусите и зловредните софтуери ще са изключително ограничени при дълбокото им проникване. Ransomware няма да събере и един долар. Кибер кинетичните атаки имащи за цел да деактивират националната инфраструктура или да поемат контрол върху автоматично управляван автомобил, ще бъдат изключително трудно осъществими. Медицинските картони и други лични персонални данни ще са си наши и само наши, да ги споделяме както намерим за уместно.

> Ще има ребалансиране на властта кой да разполага с данните и кой не.

За потребителите, може да има еднократно вписване към множество услуги. XOR сърфиране с опортюнистично кеширане обещава по-бърза скорост, съхранението на данните ще бъде много по-евтино и мрежата ще предложи по-високи нива на достъпност. За разработчиците, възможността за архитектура на съхранение на един адрес, има потенциала да опрости работата на системния програмист. А дедупликацията на данните ще позволи освен опростяване и спестяване на ресурси.

Сегашните интернет гиганти няма да могат повече да събират нашите данни, без да сме дали разрешение за това, нито пък правителството ще ни наблюдава. Ще има ребалансиране на властта кой да разполага с данните и кой не. Цензурата няма да е възможна и данните няма да може да се трият. За пръв път в човешката история понятието "за вечни времена" ще стане осъществимо.

Тъй като разходите за вписване ще бъдат ниски и достъпът ще бъде неограничен, текущият дебат за неутралността на мрежата ще приключи, и неутралитетът ще е спечелил. Хората на места с нисък или ограничен достъп до информацията ще премахнат тези блокади. Някои могат дори да изкарват прилични доходи, печелейки Safecoin.

Нови бизнес модели на базата на съгласие ще се появят в един свят, където съхранението на данни и работата в мрежата и евентуално изчисленията ще бъдат стока, и светът на информацията ще бъде много по-равнопоставено поле.

Не е ли всичко това малко идеалистично? Да, разбира се, но това е естеството на мечтите. Не всичко ще работи както е планирано и ние ще трябва да устоим на това. Техно-утопизмът е опасно нещо. Има ги и двете, предвидими и непредвидими последствия от приемането на статуквото и внедряването на всяка нова технология, като не всички ще бъдат положителни.

Въпреки това, там, където се намираме днес и там, накъдето сме се запътили с Интернет на нещата (IoT), нещо от типа на SAFE мрежата е съвсем определено необходимо, за да компенсира неравновесието в силите, и да подсигури бъдещето, задвижвано от данните.

За MaidSafe

MaidSafe е компания, основана от Дейвид Ървайн през 2006 година, която има мисията да предостави сигурност и поверителност за всеки чрез изграждане на по-добра интернет платформа. Тази нова платформа е SAFE мрежата, която е първата автономна и децентрализирана мрежа за данни в света. Тази мрежа е изградена от неизползвано пространство на твърдия диск, процесора и интернет скоростта на потребителите. SAFE мрежата ще включва съхранение, директни /peer-to-peer/ комуникации, транзакции, интернет функционалност и широко разнообразие от приложения (програми), ако трябва да назовем някои от нейните характеристики.

Посетете: www.maidsafe.net

Този документ е написан и изготвен от членовете на форума на SAFE мрежата, независимо от MaidSafe.

Присъединете се към дебата на safenetforum.org

Превод и редакция Димитър Димитров и Цветелина Ангелова

3 март 2018 г. - safenetwork.bg