Como a blockchain está revolucionando a segurança digital?

Sumário

Para navegar pelos capítulos deste estudo, **clique nos botões na margem superior**. A qualquer momento, **clique no logo do Distrito no canto inferior direito para voltar a esta página.**

Sua opinião é muito importante!

Sua opinião é muito importante para o Distrito. Por isso, queremos saber quais foram as suas impressões, críticas e sugestões sobre este relatório. Além disso, gostaríamos de saber quais outros estudos você gostaria que o Distrito Dataminer realizasse.

Quer falar com a gente? É só encaminhar um e-mail para: inside@distrito.me

Introdução

No Inside Cybertech #2, além de trazer atualizações sobre o ecossistema das startups que estão transformando o mercado de cibersegurança no Brasil, focamos em trazer soluções especializadas em blockchain dentro do contexto da segurança de informação, e como essa tecnologia está revolucionando o mercado, em diferentes setores, sendo base em algumas soluções nacionais e internacionais.

Com aplicações em diversos âmbitos e setores, a tecnologia blockchain superou as barreiras das criptomoedas. Sua natureza descentralizada, segura e confiável está sendo aplicada em soluções que visam melhorar os processos de segurança da informação dentro das corporações. O ecossistema brasileiro de startups está presente nesse processo, espelhando tendências internacionais.

Nas próximas edições do inside Cybertech, após contextualizar o cenário do ecossistema de cibersegurança brasileiro e internacional, serão iniciados uma série de temas específicos que rondam o universo da cibersegurança.

Agradecemos o apoio e o patrocínio da Cisco na confecção do report, que pretende alimentar cada vez mais conteúdos sobre um tema que se torna cada vez mais relevante dentro das corporações.

Boa leitura!

Metodologia

As startups delineadas no report foram selecionadas a partir de um trabalho minucioso de pesquisa e consulta ao banco de dados de startups proprietário do Distrito. Também foram realizadas consultas a bancos abertos e informações públicas do governo.

As startups foram examinadas individualmente para verificar adequação ao tema do report e aos critérios de seleção estabelecidos. São eles:

- Ter a inovação no centro do negócio, seja na base tecnológica, no modelo de negócios ou na proposta de valor;
- Estar em atividade no momento da realização do estudo, medida pelo status do site e atividade em redes sociais;
- Desempenhar atividade diretamente relacionada ao setor estudado;
- Ter nacionalidade brasileira e operar atualmente no Brasil.

O trabalho de definição das categorias foi baseado em análise da literatura relevante e das classificações utilizadas amplamente no mercado, no Brasil e no mundo.

A definição da categoria a que pertence cada startup foi feita por nossa equipe, e, quando uma startup opera em mais de uma categoria, a situamos na que interpretamos como sua atividade principal ou de maior visibilidade.

Também temos uma preocupação em incluir somente aquilo que consideramos startups—e, por mais que nosso critério para defini-las seja bastante amplo, excluímos alguns tipos de negócio que, embora muitas vezes se autodenominem startups, acabam fugindo do conceito. Isso inclui empresas que têm como característica principal serem:

- Software Houses (desenvolvimento de software sob demanda);
- Consultorias;
- Agências de marketing, publicidade e design.

Enfatizamos aqui que os números expostos podem sofrer alterações conforme a evolução da acurácia das informações e maior capacidade de interação com as próprias startups ao longo do tempo.

Entrevistados

Evandro Camilo
Lawyer
C2Law

Rodrigo Uchoa
Digitization & Business Development
Cisco

Marcos Sarres
CEO
Go Ledger

Hugo
Co-Founder
Growth Tech

Pedro Petri
Co-Founder & CEO
ZHealth

Ecossistemas Cybertechs

Highlights

205
Startups

12
Categorias

6.358
Funcionários empregados

45
Startups com investimento recebido

US$ 388M
Investimento recebido desde 2013

US$ 282M
Investimento recebido nos últimos 2 anos

2
M&A's desde 2012

O ecossistema da boas vindas ao primeiro unicórnio

A startup Unico, antiga Acesso Digital, captou no início do mês US$ 120 milhões em rodada series C. Agora, com o valor da empresa avaliado em US$ 1,02 bilhão, ela é a primeira cybertech no Brasil a ganhar o título de unicórnio.

O investimento, que foi liderado pela SoftBank e General Atlantic, já tem destino: aquisição de startups nos setores de saúde e educação. A startup não pretende apenas expandir seus serviços para atingir outros mercados, já que seus planos também contemplam ampliar suas atividades para alcançar o público internacional.

Por ser focada em autenticação de identidade, a startup vem ganhando clientes em diversas áreas que permitem o login do usuário por meio de impressão digital ou reconhecimento facial, principalmente bancos, companhias aéreas e plataformas de ingresso online. Ao que tudo indica, a clientela da Unico deve se expandir ainda mais nos próximos anos, já que a previsão é que até 2023, todas as empresas com presença digital serão obrigadas a contratar serviços que ofertem maior segurança de acesso e login.

Além de soluções para identificação com biometria facial, a Unico também desenvolveu a UnicoPeople, sistema para contratação de novos colaboradores de forma 100% digital, e mais recentemente lançou uma plataforma de assinatura digital, a UnicoSign.

RADAR: CYBERTECHS

DISTRITO

Identity Access Management

DAITAN
acert
AIKNOW
akiyama
Assine Online
autentique
AutoSeg
BeCloudx
BRyTecnologia
CH tecnologia
Chico
Computer ID
contraktor
CRED DEFENSE
D4S
GO! FIVE
Formalizar e-signature
FULLFace
FULLFace
griaule big data biometrics
GrupoCloud
GRYFO
hq
contract
ID ESSENTIALS
idwall
inloco
INOVACODE
JURIDOC
PONTO marcação móvel
Let's Work
.ai
mavie
MEERKAT
MULTIFACE BIOMETRIA
NATOSAFE BORN TO BE UNIQUE
nexti
nTokens
payface
qriar
QualiSign
SHIELDER
SimpleID IDENTIDADE CONFIRMADA!
SimpleID IDENTIDADE CONFIRMADA!
SVATECH
T-SHIELD
acesso digital
unike
UNISEC Segurança, tecnologia e conforto
VSOFT
w3lcome

Network _ Infrastructure Security

CONNECTA
ISH
lumiun CLOUD MANAGED NETWORK
munic SECURITY
ProFUSION
StartLink
TI Safe
Virti

Web Security

apura
AuditSafe
CromiWAF cyber defense
KRYLSEC
SITE BLINDADO
Gatefy
XLabs ON SECURITY
XLabs security
<unxpose>
UPX TECHNOLOGIES

Cloud Security

ADTsys
baxtru | cloud backup
BrasilCloud Nuvem Corporativa
DDMX
nuvic cloud solutions
RedeHost
skalena

Application Security

Berghem
BugHunt
CONVISO
OGASEC

RADAR: CYBERTECHS

DISTRITO

Data protection

a2f · ADDERE SOLUTIONS · beAnalytic · CIAware · CLAVIS segurança da informação · CleanCloud · DADOS LEGAIS · dogma · ethquo ETHICAL QUOTIENT · GLOBAL DATA BANK · guardSI Cybersecurity · ID ESSENTIALS · Intelivix · leadcomm trusted digital security · LOGS360 · MODULO · NETTIME SISTEMAS · Privacy Tools · PRIVALLY · riskex · [SAFE WAY] · senhasegura · SENSR. · Simply. · ST3TAILOR SISTEMAS E SERVIÇOS

Fraud Transaction Security

akaer · B2e Group · bankSe · bigdatacorp. · BLOCO1 · BrScan · COMBATE A FRAUDE · CQuantt · datarisk.io · EXATO DIGITAL BETA · deepen · HUPDATA · inlocomedia · infodatos · konduto · legiti · MaChiron · MOST · Neoway · NeuralMind · NeuroBanco · NEXTCODE · REFINARIA DE DADOS · Owli · TRANSFERO SWISS AG · certo · VIVALISTO · ZAIG

Security Consulting and Services

ANDRADESOTO · BLAZE INFORMATION SECURITY · CECyber · Collision INTELLIGENCE LABS · CROMISOFT · Deep.bbl · DESEC · ESTUARIO.TI · HACK3R_RANGERS · IBLISS DIGITAL SECURITY · InfoSafe · SOLVIMM · nova8 Cybersecurity · OPTRA SECURITY · PHISHX · REDBELT · RUSTCON · STRONG SECURITY · TEMPEST · Unbroken Cyber Security

IoT Security

GAVB · LATOS · Ochain · POLSEC · PREVISIOWN · ROBBIOT · TrackerThings

GRC

ECOIT SEGURANÇA DIGITAL · GAT InfoSec

Mobile Security

BluePex.

Security Operations Incident Response

AXUR · gocache next-gen CDN

Blockchain em Cybersecurity

Ransomware chega ao mercado de massa

Evandro Camilo
Lawyer
C2Law

Com base em análise dos dados de blockchain disponíveis pela Chainalysis, em 2020 os cibercriminosos extorquiram com sucesso pelo menos US$412 milhões de organizações vítimas, mais do que quadruplicando seus totais de 2019. Os cibercriminosos não mostram sinais de desaceleração este ano, tendo recebido mais de US$127 milhões em 2021 em 28 de maio. O pior pode estar por vir, já que em 3 de julho viu o início talvez o maior ataque de ransomware até agora, com o REvil infectando mais de um milhão de computadores explorando uma vulnerabilidade no software usado pelo provedor de TI Kaseya. A REvil está atualmente exigindo um resgate geral de US$70 milhões para liberar todos os sistemas afetados.

No Brasil a tendência é a mesma, o governo brasileiro divulgou nota informando que o Tesouro Nacional foi atingido por um ataque de ransomware no dia 13 de agosto de 2021. Da mesma forma, algumas empresas foram vítimas de ataques similares e que exigiam o pagamento em criptoativos.

É claro que, assim como o terrorismo, os resultados nefastos dos ataques de ransomwares vão muito além das perdas financeiras e da interrupção dos negócios.

Os cibercriminosos frequentemente têm como alvo instituições e organizações governamentais associadas à infraestrutura crítica em que todos confiamos, incluindo bancos, hospitais, instalações de energia e empresas de alimentos, o que pode levar à perda de vidas, direta e indiretamente. Assim como os terroristas, os atacantes de ransomware aproveitam o medo, o caos e a interrupção para aterrorizar e coagir suas vítimas a atingir seus objetivos.

Os paralelos entre ransomware e terrorismo se estendem além do próprio problema e para as soluções. Em sua essência, a sobreposição se resume à necessidade dos setores públicos e privados aumentarem os recursos dedicados a combater essa ameaça e encontrarem maneiras mais eficazes de colaborar. Combinados, esses esforços servirão para interromper as redes de suporte e aumentar o custo para os cibercriminosos. Isso diminuirá sua capacidade de realizar ataques futuros e desencorajar sua atividade ilícita.

No entanto, o problema é agravado pela prevalência de plataformas que fornecem serviços de ransomware (Ransomware as a Service ou “RaaS”). →

Muitos hackers que desenvolvem tecnologia de ransomware agora permitem que hackers menos sofisticados aluguem o acesso a ela, da mesma forma que uma empresa pagaria uma taxa mensal por um software como o G-Suite do Google. A principal diferença é que os criadores do ransomware também recebem uma parte do dinheiro de qualquer ataque bem-sucedido.

O que fazer se uma empresa for vítima de Ransomware?

No caso de sua empresa seja vítima de um ataque ransomware, o primeiro passo é isolar todas as máquinas afetadas, desconectando-as de quaisquer redes às quais estejam conectadas, como wi-fi ou bluetooth, e desligando-as. Em segundo lugar, feche todas as portas de protocolo de desktop remoto ("remote desktop protocol" ou RDP), pois elas são um vetor comum para ataques de ransomware. Por fim, atualize todas as credenciais administrativas e de usuário, para que os hackers percam qualquer acesso que tenham aos seus sistemas. A partir daí, você deve restaurar o máximo possível de seus dados a partir dos backups.

A C2LAW, junto com o FBI , recomenda não pagar resgates, a menos que não haja outra maneira de sua empresa recuperar dados cruciais. Caso haja o pagamento, vocês podem contar conosco para rastrear o pagamento em criptoativos até seu destino e tomar as medidas necessárias para recuperar os recursos.

No caso de você ser atacado, você deve coletar o máximo de evidências possíveis, como capturas de tela de mensagens de resgate que você recebeu e enviá-las a nossos investigadores para que eles possam saber com qual cepa de ransomware você foi atingido e começar a formular uma resposta para os criptoativos pagos em resgate. Você também pode relatar ataques à C2LAW diretamente usando nosso formulário de relatório de ransomware . Os detalhes que você fornece podem nos ajudar a coletar mais dados sobre seus invasores e trabalhar com as autoridades para detê-los.

Sobre a C2Law

Somos a primeira lawtech especializada na tecnologia blockchain e provemos serviços de consultoria em prevenção a ilícitos e ferramentas tecnológicas para rastreabilidade, combate, prevenção e compartilhamento de dados de ataques cibernéticos envolvendo criptoativos.

Ransonware chega ao mercado de massa

Evandro Camilo
Lawyer
C2Law

Blockchain 1.0

Criptomoedas

- Fundação das tecnologias blockchain.
- Redes blockchain para transação entre criptomoedas
- Transações descentralizadas
- Protocolo Proof of work (PoW)

Blockchain 2.0

Contratos inteligentes

- Mais funcionalidades além de simplesmente uma rede de transações
- Aplicações de descentralização baseados em linguagens de programação
- Execução anônima de algoritmos
- Protocolo Proof of work (PoW)

Blockchain 3.0

Novas funcionalidades

- Aplicações de larga escala que se distanciam da origem da blockchain focadas em criptomoedas. Focadas no Ledger distribuído.
- Melhora de performance com mais escalabilidade.
- Protocolo Proof of Work (PoW)

Blockchain: uma nova forma de pensar em cybersecurity

Conforme exposto no Inside Cybertechs #1, o prejuízo causado globalmente em decorrência de ataques cibernéticos chegou em US$ 945 bilhões, beirando a marca de US$ 1 trilhão, com grandes sinais que esse número se torne cada vez maior. Esses ataques cibernéticos usualmente perpassam as barreiras tradicionais impostas por políticas internas de cybersecurity dentro das corporações, como autenticação de identidade dos usuários na rede, manutenção de senhas, criptografia e privacidade de dados.

Com a pandemia e o aumento do número de casos de *cyber attacks* dentro das empresas, principalmente causados por uma nova dinâmica de trabalho e desafios de segurança impostos pelo trabalho remoto, muitas corporações estão repensando os sistemas implantados para garantir menos vulnerabilidades no âmbito da segurança da informação. Nesse contexto, a blockchain aparece como uma possibilidade de maior segurança, principalmente pelo *ledger* distribuído que oferece, e também por ser um ambiente menos familiar para criminosos cibernéticos que elimina as vulnerabilidades menos óbvias de um sistema de segurança.

A blockchain possibilita uma criptografia melhor, pois consegue verificar a integridade e o pertencimento dos dados mais rapidamente e eliminar a necessidade de senhas — usualmente um dos links mais fracos dentro de um sistema de segurança, por ser de responsabilidade do usuário. Uma outra vantagem importante que a blockchain possui, justamente pela sua natureza de ser uma rede compartilhada, é a possibilidade de sempre estar vigiando à ameaças, anomalias e "organismos" não familiares sem a necessidade de um controle central. Basicamente o *ledger* distribuído consegue utilizar uma infraestrutura de chaves públicas para garantir uma comunicação segura, validar mudanças de configuração do sistema, autenticar dispositivos móveis e garantir de fato uma segurança e transparência em todas as partes do sistema. Ainda, a blockchain pode ser uma forma de prevenção de ataques DDoS (ataques de negação de serviço), um DNS (Domain name systemn) baseado em blockchain elimina o ponto único de falha no sistema que possibilita crimes cibernéticos acontecerem com mais facilidade.

Dessa forma, é natural que diversas organizações, de multinacionais até instituições governamentais, estejam procurando soluções em segurança da informação que se utilizem da tecnologia blockchain. Entretanto, é necessário salientar que a intersecção entre blockchain e cybersecurity está em constante desenvolvimento e aprimoramento. Soluções que envolvem identidades digitais, sistemas descentralizados de armazenamento de dados, contratos inteligentes e outras, nem sempre estão alinhadas com as necessidades reais e imediatas do mercado, por isso considera-se que há um espaço para encontrar aquelas que seriam ideais para a maior parte das organizações.

Pilares da blockchain em cybersecurity

CONFIDENCIALIDADE

As chaves dos integrantes da rede blockchain são o único link entre os dados presentes na rede e o próprio usuário, mas essas chaves são fáceis de serem deixadas anônimas. Algumas redes também utilizam "non-interactive zero-knowledge proofs", basicamente uma forma de limitar a interação entre os indivíduos, com o objetivo de maximizar a confidencialidade e o anonimato dos próprios. Como consequência, enquanto soluções em blockchain tem a traceabilidade como um dos seus principais ativos, o anonimato dos usuários é mantido.

INTEGRIDADE DOS DADOS

Redes de blockchain são compostas por blocos que utilizam criptografia baseada nas funções dos *hashs*, que são guardadas no *ledger*. Dessa forma, quando uma transação é realizada na blockchain, ela não pode ser deletada nem alterada. Quaisquer novas alterações serão gravadas em cima do que já foi processado, gerando uma nova informação. Dessa forma, as soluções em blockchain garantem a integridade de todos os dados, inalteráveis e gravados no livro razão.

DISPONIBILIDADE

Ter um grande número de nós (agrupamento de participantes que tem o mesmo interesse, para exempo, no caso do bitcoin seria a transferência de dinheiro) garante que a blockchain seja resiliente mesmo quando alguns não estão disponíveis. Como cada nó na network tem uma cópia do *ledger* distribuído, a informação correta permanece disponível para os usuários em caso da falha em um nó.

Vantagens da Blockchain em Cybersecurity

PROTEÇÃO E PROCESSAMENTO DE DADOS

Dados gravados na blockchain são imutáveis e qualquer mudança feita gravada e transparente, além de não removível. Dessa forma, dados guardados na blockchain são mais íntegros e seguros se comparados à outros métodos tradicionais.

TRANSFERÊNCIAS SEGURAS DE INFORMAÇÃO

A blockchain permite transações rápidas e seguros de dados ou produtos financeiros. Adendos como contratos inteligentes registrados na própria rede garantem que o negócio seja feito da forma mais transparente e efetiva possível.

ELIMINAÇÃO DE UM PONTO VULNERÁVEL

Redes blockchain que não precisam de senha para serem acessadas são descentralizadas e portanto, como já exposto, se tornam mais resilientes. O comprometimento de um único nó não afeta todo o resto da operação de segurança, isso significa que mesmo em caso de ataques DDoS, o sistema será operável normalmente, graças às várias cópias do ledger distribuído em cada um dos nós.

TRANSPARÊNCIA E RASTREABILIDADE DOS DADOS

Todas as transações na blockchain são digitalmente assinadas e com o horário gravado, logo qualquer informação é facilmente rastreável a qualquer momento

CONFIDENCIALIDADE DO USUÁRIO

A confidencialidade dos usuários da rede é extremamente alta devido à uma chave pública criptografada que autentica os usuários. Entretanto, algumas startups conseguem ir um passo além, desenvolvendo soluções que permitem a autenticação do usuário sem a utilização dessas chaves

AUMENTO DA CONFIANÇA

A principal vantagem da blockchain é o conjunto de todas as vantagens já citadas, que garante que os usuários e consumidores do produto se sintam seguros em utilizar soluções de blockchain

Blockchain reduz o risco de fator humano

Com empresas que geram grandes quantidades de dados todos os dias, o armazenamento deles de maneira centralizada sempre é um fator de vulnerabilidade que pode ser explorado por criminosos. Ademais, o número de dispositivos conectados à internet está projetado para chegar em 13,8 bilhões em 2021, que naturalmente são alvos de ataques de segurança da informação. É imprescindível que um protocolo uniforme de cibersegurança dentro das empresas seja consolidado. Entretanto, mesmo que eles existam, erros humanos geralmente são a principal porta de entrada para vazamento dados.

Dito isso, além de um protocolo estabilizado e medidas de conscientização constantes para manter a segurança da empresa, todas as medidas necessárias para reduzir o risco do fator humano precisam ser estabelecidas.

A natureza descentralizada da tecnologia blockchain provém os melhores padrões de transparência e integridade de dados, diminuindo abruptamente as chances de vazamentos de dados causados por erro humano. Dados na blockchain, como já foi exposto anteriormente, não podem ser adulterados, porque todas as informações são cruzadas entre os nós. No combate às ameaças cibernéticas que permeiam as empresas diariamente, a blockchain pode pode se aliar aos sistemas de defesa e agregar valor, criando um protocolo de segurança padrão, verificando todas as atividades que podem trazer riscos à corporação.

95%
Dos vazamentos de dados são causados por erros humanos

90%
Dos malwares são entregues e acessados via e-mail

34%
Das empresas demoram mais de uma semana para recuperar acesso aos dados invadidos

US$ 6 Trilhões
Deve ser o custo de crimes cibernéticos no fim de 2021

Principais riscos da Blockchain em Cybersecurity

Embora existam vantagens claras na utilização da tecnologia, é essencial destacar que existem riscos associados à implantação de soluções que utilizam blockchain dentro de cibersegurança.

DESAFIOS DE ESCALA

Redes de blockchain tem limites distintos, relacionados ao volume dos blocos e transações processadas por segundo, que podem impedir a escalabilidade de algumas soluções.

NECESSIDADE DE CHAVES PRIVADAS

Apesar de representar uma grande vantagem no âmbito da segurança e da autenticidade das informações, as longas sequências de números que dão origem às chaves privadas da blockchain, caso forem perdidas, não conseguem ser recuperadas. Dessa forma, é preciso ter muito cuidado com o armazenamento dessas chaves.

PROBLEMAS DE ADAPTABILIDADE

Apesar de tecnologias em blockchain puderem ser aplicadas em quase todos os modelos de negócio, muitas empresas enfrentam dificuldade na implantação. Soluções de Blockchain podem precisar substituir completamente os sistemas existentes para funcionar da melhor forma. Assim, antes de implantar soluções que utilizem esse tipo de tecnologia, é importante considerar todos os trâmites necessários.

CUSTOS DE IMPLANTAÇÃO

Uma rede blockchain precisa de um poder computacional substancial e necessita de uma grande quantidade de espaço para ser armazenada. Todos esses fatores podem aumentar os custos marginais da operação em comparação à outros sistemas de segurança.

GOVERNANÇA E REGULAÇÃO

As operações realizadas na blockchain não são necessariamente regularizadas ao redor do mundo, e algumas nações estão mais avançadas que outras. Entretanto, as regulações ameaçam mais soluções ligadas às criptomoedas, que são vistas como risco financeiro para alguns países, por não ter o estado como produtor e detentor do monopólio.

ESPECIALISTAS

Apesar do número crescente de soluções em blockchain no mercado, ainda existe uma falta de profissionais qualificados que consigam manter a rede funcionando da melhor forma. Desenvolvimento de soluções em blockchain requerem uma grande quantidade de habilidades, conhecimento em diferentes linguagens de programação e ferramentas.

Blockchain em cybersecurity

Rodrigo Uchoa
Digitization & Business Development
Cisco

A Blockchain oferece uma série de vantagens no contexto da cibersegurança, e é fundamental no desenvolvimento de diversas soluções. Quais os principais desafios que a blockchain auxilia dentro do contexto de segurança da informação?

A tecnologia Blockchain viabiliza confiabilidade a partir da colaboração de atores não confiáveis em ambientes descentralizados não confiáveis. Uma rede pública blockchain, com um número significativo de nós, permite que transações e informações sejam validadas e armazenadas, garantindo consistência, confiabilidade, integridade, conformidade e a imutabilidade dessas transações e informações sem que haja a necessidade de um elemento gestor central e confiável. Desde o primeiro computador comercial e início do processamento de dados em 1951, o setor de tecnologia da informação lida com os desafios de gestão das informações e controle de usuários. Esta pessoa é realmente quem ela está dizendo ser? Esta máquina realmente está autorizada a realizar esta operação? Este ativo realmente pertence a esta organização? Esta operação foi realmente realizada? Esta informação foi adulterada? Estes são apenas alguns exemplos de desafios do setor de TI e que a tecnologia blockchain poderá finalmente ajudar a endereçar permitindo novos níveis de cibersegurança para as plataformas e serviços digitais.

Quais os principais setores que podem se beneficiar com a blockchain dentro das soluções de cybersecurity?
Todos os setores da economia que demandam confiabilidade, colaboração entre atores não confiáveis, integridade de informações, e principalmente setores onde a adulteração de transações ou informações representa impactos econômicos relevantes, possuem o potencial de se beneficiar do uso das tecnologias, plataformas e redes blockchain.

Como estamos falando essencialmente de gestão e proteção de transações e informações, todos os setores da economia se beneficiarão com a evolução e implementação das tecnologias blockchain. Mas talvez o setor com o maior potencial de transformação é o financeiro, não apenas porque o blockchain foi inicialmente pensado para a operacionalização de criptomoedas, mas porque é um setor extremamente centralizado e controlado, que deve ser profundamente impactado pelo conceito de descentralização. →

Além da explosão de criptomoedas, o surgimento de tokens digitais, plataformas para implementação de contratos inteligentes, NFTs (Non Fungible Tokens) e aplicações financeiras distribuídas (DeFi) irá abrir espaço para inovação e transformações do setor financeiro, inclusive viabilizando novos modelos de negócio e rupturas profundas no mercado e seus atores.

Outro setor que também será bastante impactado pelo uso das tecnologias blockchain nos próximos anos e o de saúde, no qual a integração de atores e a segurança de informações confidenciais e sensíveis é extremamente crítico e necessário. Plataformas baseadas em blockchain podem viabilizar a segurança, controle de acesso e integridade de dados de saúde, além de permitir o armazenamento histórico e imutável de transações e registros no setor.

Como a Cisco acredita que a blockchain entra dentro das soluções de cibersegurança ofertadas no Brasil?

Apesar do enorme potencial das tecnologias blockchain, ainda estamos em um estágio muito inicial da utilização destas tecnologias em soluções específicas voltadas para a área de segurança cibernética, ainda restritas a laboratórios e centros de pesquisa e desenvolvimento. Como existem questões técnicas, tais como eficiência energética e escalabilidade, além da necessidade de aceitação de modelos descentralizados para gestão de identidade e informação, ainda serão necessários alguns anos para que serviços e soluções de segurança incorporem tecnologias blockchain e estejam amplamente disponíveis no mercado.

Um exemplo de utilização da tecnologia e redes blockchain em cibersegurança, é a proposta de evolução e extensão do serviço de nomes da Internet, Domain Name System, para um serviço descentralizado, seguro e inviolável de identidade digital. Sabemos que muitos dos ataques e ameaças cibernéticas nascem da fragilidade e manipulação dos sistemas DNS e da identidade de usuários e máquinas.

Namecoin, Unstoppable Domains, Ethereum Name Service e Handshake são exemplos de iniciativas do uso de blockchain nesta área.

Segurança em IoT (Internet of Things) é outro caso de uso de blockchain, sendo considerado para a gestão de identidade, integridade de dados, registro de transações eletrônicas e implementação de contratos inteligentes entre máquinas. IoT é blockchain são tecnologias complementares e muitas plataformas IoT já consideram a integração com tecnologias blockchain, dando origem a um novo paradigma, chamado Blockchain (BIoT), onde os dados gerados por sensores e máquinas ficam registrados e disponibilizados para uso em redes blockchain seguras. Diversas startups e empresas de tecnologia estão avaliando o uso de blockchain e desenvolvendo plataformas baseadas em BIoT, tais como: Chronicled (Gestão de Cadeia de Suprimento), Helium (Conectividade IoT) e Grid+ (Smart Grid).

Acredito que temos um espaço enorme para inovação e a evolução das tecnologias e soluções para segurança cibernética, abrindo oportunidades para empresas e startups brasileiras do setor interessadas na integração das tecnologias e plataformas blockchain e cibersegurança. Estamos apenas no início desta jornada!

Blockchain em cybersecurity

RODRIGO UCHOA
Digitization & Business Development
CISCO

Em que casos a blockchain pode ser utilizada em cybersecurity?

Apesar de não ser impenetrável, a tecnologia blockchain evoluiu para ser uma das formas menos fraudulentas e mais seguras de transação dentro de uma rede. Dentro de cybersecurity, algumas utilidades se destacam:

IOT SECURITY

Observa-se um aumento da quantidade de ataques cibernéticos voltados para dispositivos de ponta, como roteadores e termostatos, que possibilitam uma porta de entrada para a rede toda. Nesse caso, a blockchain pode ser uma possibilidade de descentralizar a administração da rede, fazendo com que os dispositivos consigam ter uma segurança própria mais efetiva, sem depender de um controle central.

PROTEÇÃO CONTRA ATAQUES DDoS e DATA HACKING

Um ataque DDoS ocorre quando uma rede fica inutilizável após um ataque cibernético, geralmente criminosos pedem resgate em criptomoedas para permitir o acesso dos usuários novamente. A blockchain consegue diminuir esse tipo de ataque por descentralizar as entradas de Sistemas DNS (Domain Name System). Dessa forma, pontos únicos e vulneráveis são eliminados. Essas soluções de descentralização também são utilizadas em sistemas de armazenamento de dados, visto que grande parte desses sistemas também são explorados por hackers por terem um ponto de acesso vulnerável, e criminosos conseguem acesso à informações sensíveis que podem prejudicar de inúmeras formas uma corporação caso vazadas.

VERIFICAÇÃO DA INFRAESTRUTURA DE CIBERSEGURANÇA

As capacidades de verificação e autenticação que existem na tecnologia blockchain são capazes de auferir falhas de sistema, adulteração de dados e problemas simples de integridade da informação que potencializam sistemas de cybersecurity dentro das corporações. Todas as informações geradas em uma estrutura com o intermédio da blockchain tem uma garantia maior de assertividade.

PROTEÇÃO EM TRANSMISSÃO DE DADOS E MENSAGENS

A blockchain consegue impedir acessos não autorizados a qualquer tipo de dado em trânsito, utilizando de uma criptografia própria da tecnologia. Destaca-se que um dos pontos de ataque mais visados por hackers no roubo ou adulteração de informações é enquanto existem dados em trânsito.

CHECAR A PROVENIÊNCIA DE UM SOFTWARE

A blockchain pode ser utilizada para avaliar a integridade de um software ou de qualquer download para prevenir possíveis invasões de ameaças externas. Quaisquer atualizações, instalações e consertos podem ter suas atividades verificadas com a tecnologia blockchain . É importante destacar que podem existir falhas, pois os *hashs* providos pela plataforma podem já estar comprometidos, mas a integridade do que é inserido no sistema é mais garantido quando se usa a blockchain.

RADAR: STARTUPS QUE TRABALHAM COM BLOCKCHAIN EM CYBERSECURITY

DISTRITO

Blockchain em cybersecurity

Panorama Nacional

Highlights

26
Startups

220
Funcionários empregados

3
Startups com investimento recebido

US$ 538 Mil
Investimento recebido desde 2016

Startups de Blockchain em Cybersecurity
Blockchain as a Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes de blockchain em nome de outras organizações.

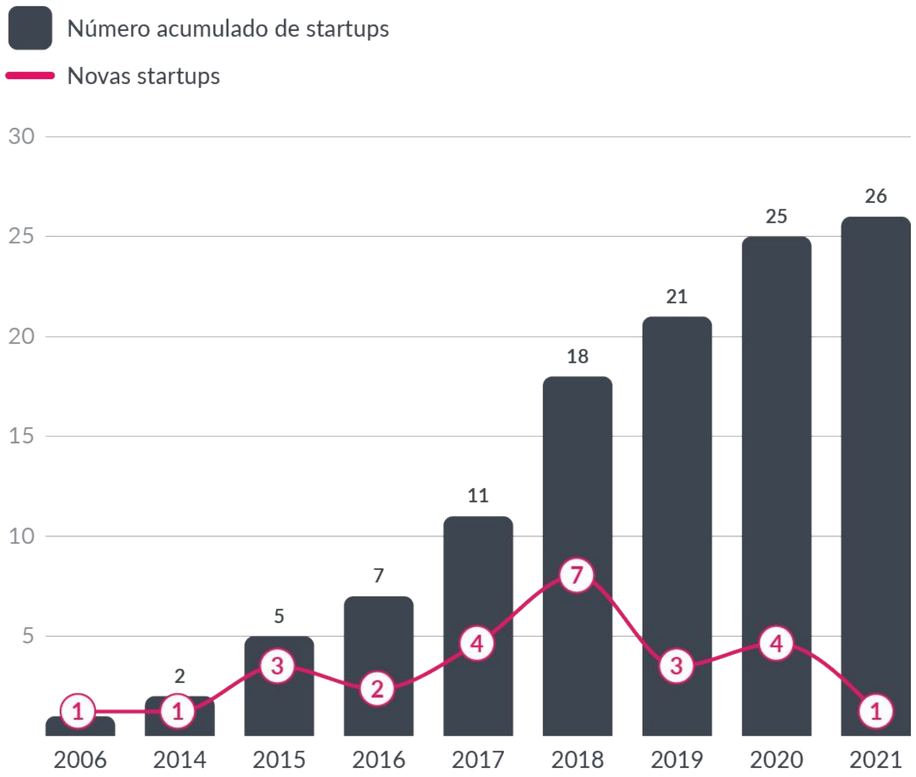
OriginalMy blockchain

Growth Tech

rhizom
IN AUTONOMY WE TRUST

Soluções de blockchain em cybersecurity

Ano de fundação startups



As soluções brasileiras de blockchain relacionadas a cybersecurity, tal como o restante do ecossistema, estão em desenvolvimento e em busca de se firmarem em um mercado que ainda não apresenta um grande número de empresas consolidadas. O segmento ainda está muito conectado com o mercado de criptoativos, oferecendo possibilidade de transações, compras e armazenagem, entretanto é esperado que mais soluções de blockchain que não estão associadas à sua origem apareçam com o passar dos anos, espelhando o mercado internacional.

Em um relatório publicado pelo Bradesco em parceria com a inovabra, dentre as startups que trabalham com blockchain no Brasil atualmente, 12,7% estão dentro do segmento de segurança digital. A categoria que mais se destaca é a de serviços financeiros, que compreende 49,7% das soluções.

GoLedger

Categoria Blockchain

Ano de Fundação 2017

Público B2B e B2G

Investimento Recebido XXX

Investidores XXX

Sobre

Com a missão de unificar e instanciar projetos compartilhados entre várias entidades ou instituições públicas, a GoLedger é pioneira no desenvolvimento de soluções em blockchains permissionados para governo. Situada na capital federal, a empresa é uma fabricante nacional de soluções focadas para atender os reguladores e tem grande vocação para atuação na administração pública e empresas privadas.

A empresa possui diversas soluções em blockchain, entre elas: Contratos inteligentes, Compartilhamento de dados e Orquestração de rede (GoFrabric), ID digital (GoBio), gestão de documentos e assinaturas digitais (GoProcess), Rastreamento de produtos (GoTrace), Portal de consentimentos LGPD (GoPrivacy) e Votação eletrônica (GoVote).

A startup tem ganhado destaque nas mídias por se posicionar como uma das empresas preparadas para implementar o voto eleitoral através de blockchain. A tecnologia foi incluída no programa de transformação digital do Governo Federal.

Já estabelecida no mercado, a GoLedger tem parceria com grandes provedores mundiais de Nuvem como AWS, IBM, Microsoft e Huawei, e já possuímos uma rede de canais e parceiros com escritórios nos estados de São Paulo, Rrio de Janeiro, Ceará, Paraná e Distrito Federal com empresas de grande porte como Capgemini e Golden Tecnologia.

Atualmente compõem o marketplace da ETICE sendo a única empresa privada capaz de realizar a venda de soluções, infraestrutura e serviços em blockchain através de Dispensa de Licitação.

Quais são os problemas que a blockchain resolve?

Marcos Sarres
CEO
Go Ledger

A GoLedger se posiciona como uma empresa de soluções em Blockchain. Como as soluções da empresa conseguem impactar diretamente as corporações e transformar processos dentro das empresas?

As soluções GoLedger têm os seguintes objetivos principais:

- Interconexão de bases e sistemas legados;
- Rastreabilidade de ativos;
- Auditabilidade de informações;

E as soluções são:

- GoFabric – orquestrador de barramentos distribuídos e plataforma DevOps;
- GoProcess – gestão de processos e documentos digitais com assinador de PDFs;
- GoBio – identificação única de pessoas e cidadãos;
- GoPrivacy – portal de consentimentos LGPD;
- GoTrace – rastreabilidade de ativos e selo de qualidade digital;
- GoVote – votação digital com privacidade e auditabilidade;

Como a blockchain pode revolucionar processos dentro da empresa relacionados a segurança da informação?

São diversos problemas que o Blockchain resolve. Quando se deseja entender quais processos podem ser melhorados/otimizados pela tecnologia, algumas perguntas são importantes:

- Quais processos precisam de etapas de conciliação, nos quais uma equipe precisa se mobilizar frequentemente para analisar dados de diferentes origens (outras organizações ou outros departamentos) para poder passar o processo adiante.
- Quais sistemas utilizam robôs para baixar informações de diversas bases para poder gerar novos resultados.
- Quais processos são questionados quanto a confiabilidade, na qual as informações armazenadas são colocadas em dúvida ou em disputa frequentemente.

Uma vez definidos os processos que podem ser otimizados, uma arquitetura em Blockchain é proposta para poder consumir e tratar os dados desses processos de forma a incluir as seguintes características: Imutabilidade; Auditabilidade; Confiabilidade; Escalabilidade.

Quais são os problemas que a blockchain resolve?

Marcos Sarres
CEO
Go Ledger

Qual a relação de inovação e blockchain dentro das corporações e a blockchain?

O Blockchain representa uma tecnologia inovadora, capaz de resolver problemas de confiabilidade na comunicação e processamento de dados entre empresas.
Diversas desenvolvedoras estão criando departamentos específicos de inovação e o Blockchain faz parte dessa jornada, juntamente com outras tecnologias tais como I.A., IoT, BigData, etc.

O Brasil precisa cada vez mais de soluções consolidadas em cibersegurança. Como vocês avaliam o futuro da GoLedger dentro do cenário de proteção de dados, principalmente em uma realidade em que as empresas precisam se adaptar à LGPD?

A Lei Geral de Proteção estabelece que o tratamento de dados de titulares deve ser feito de forma distribuída, na qual são definidos os seguintes atores:
Controlador: representando a organização-mãe que define todos os processos que precisam tratar dados de titulares
Operador: representando as empresas terceirizadas, filiais, departamentos, que operam os dados dos titulares em nome do controlador.

Nós fornecemos para os clientes a plataforma GoPrivacy, um portal de consentimentos distribuídos baseados na LGDP, que possui as seguintes funções:

- Cadastro de naturezas de dados processos LGPD

- Inventário de bases de dados de titulares

- Requisição/aceitação de consentimentos utilizando servidores de autenticação, documentos digitais ou digitalizados ou assinaturas com certificados x.509.

- Gestão do direito de ser esquecido

OriginalMy blockchain

Categoria Blockchain

Ano de Fundação 2015

Público B2B e B2G

Investimento Recebido Não divulgado

Investidores 3xBit

Sobre

Iniciada em 2015 no Brasil, mas mudando sua sede para a Estônia em 2018, a OriginalMy Blockchain nasceu com o propósito de desburocratizar o mundo. A startup utiliza a tecnologia blockchain dentro de sua plataforma para fornecer serviços como: Coleta de evidências para processo judicial (PACWeb), Consentimento do usuário em relação a LGPD (OMyPass), Proteção de direitos autorais sobre arquivos digitais (PACDigital), assinatura eletrônica e certificação de documentos digitais (OMySign) e relatório de dados sobre possíveis parceiros e fornecedores (KYC).

Eles são uma das primeiras empresas no Brasil a fornecer soluções reais baseadas em blockchain e uma das únicas com parceria com cartório para oferecer a autenticação de documentos de forma 100% digital.

Em 2018 ganhou o prêmio de empresa mais inovadora, no CriptoAwards, e em 2020 a startup ganhou o prêmio de campeã mundial na categoria Privacy, Data Protection and Compliance, em cibersegurança, realizado em um dos eventos de investimento mais importantes do mundo, organizado pelo Ministério da economia dos Emirados Árabes Unidos.

Growth Tech

Categoria Blockchain

Ano de Fundação 2015

Público B2B e B2C

Investimento Recebido XXX

Investidores XXX

Sobre

A Growth Tech é uma startup que desenvolve soluções para automação inteligente e desintermediação de processos, através de Smart Contracts e da tecnologia Blockchain. Ela usa tecnologias disruptivas como pilar fundamental em seus projetos.

A startup é uma das primeiras a trazer soluções de problemas usando blockchain no Brasil. Possui produtos para assinatura eletrônica ou digital, com certificado digital (PropLedgers), gestão condominial inteligente (Digi), rede virtual de cartórios (Notary Ledgers), além de seus projetos em consultoria em blockchain.

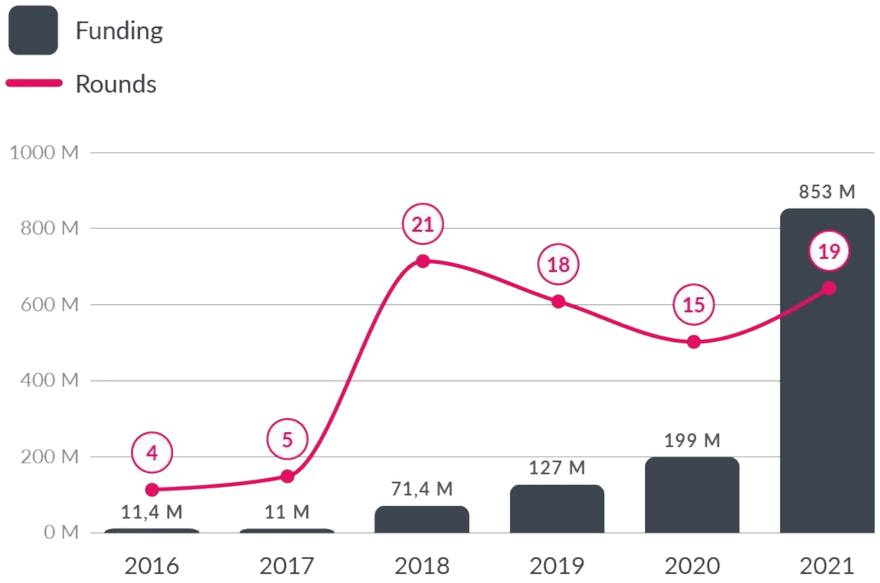
A Growth Tech foi responsável pela primeira oficialização de união estável homoafetiva através de blockchain no Brasil, assim como o primeiro registro de nascimento com a tecnologia em território nacional.

Blockchain em cybersecurity

Panorama Internacional

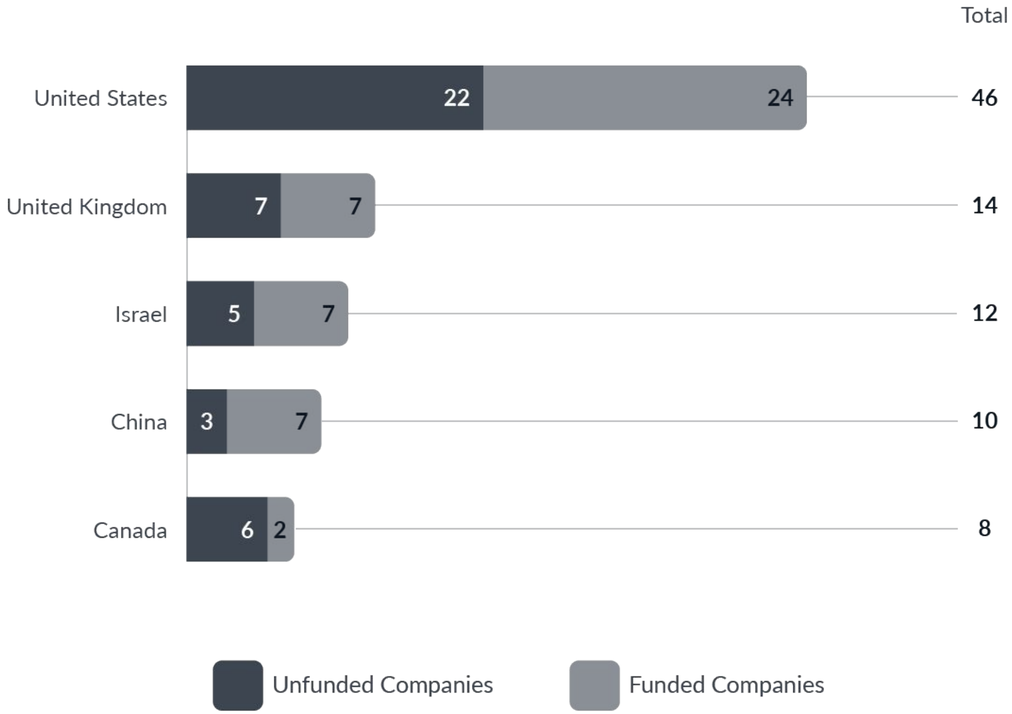
Soluções de blockchain em cybersecurity

Financiamento e número de rodadas ano a ano no mundo



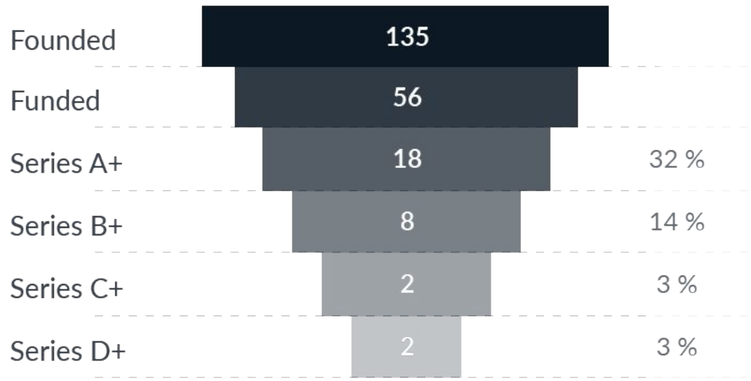
1,3 B
Total Funding

Países com mais soluções



Soluções de blockchain em cybersecurity

Empresas por estágio



Top Companies Mundo

Top Companies	Ano Fundação	País	Total Funding
Fireblocks	2018	Estados Unidos	489,0 M
Chainalysis	2014	Estados Unidos	367,0 M
StartkWare	2018	Israel	118,0 M
Elliptic	2014	Reino Unido	44,3 M
Casa	2016	Estados Unidos	10,0 M

Top 5 investidores internacionais

Como o panorama das soluções de blockchain no Brasil se compara ao internacional?

Marcos Sarres
CEO
Go Ledger

O mundo conheceu a tecnologia Blockchain através das criptomoedas, que desde 2009 tem oferecido à sociedade novas formas de guarda de valor e transferência de ativos. Mais de 10 anos depois, novas soluções foram apresentadas para o mercado baseadas nessa inovação tecnológica. Com uma união elegante de algoritmos e tecnologias já conhecidas (tais como redes peer-to-peer e criptografia avançada), a tecnologia Blockchain oferece atualmente modelos sistemáticos de confiança, transparência, unicidade e integração de dados como nunca foi visto até então.

Desde o cidadão comum até empresas e governos agora podem se beneficiar e melhorar os seus processos e os casos de sucesso estão se espalhando no mundo. Internacionalmente, empresas de renome tem colocado processos importantes com lastro digital em Blockchain em diversos setores, tais como o mercado financeiro, cadeia de suprimentos e saúde. Um dos exemplos mais emblemáticos é a Tradelens, uma joint-venture entre a IBM e a Maersk (maior transportadora do mundo) para desburocratizar o trâmite de mercadorias entre aduanas, portos e transportadoras.

Outros grandes projetos em Blockchain no mundo são capitaneados por grandes empresas como Walmart, JP Morgan, UPS, dentre outros. O Brasil também está investindo de forma expressiva na tecnologia Blockchain, porém com maior foco na regulação. Governos Federal e Estaduais têm desenvolvido projetos que visam melhorar a produtividade e transparência em diversos processos. O Blockchain se torna a ferramenta perfeita para regulação, pois permite que informações distribuídas entre regulador e regulados estejam sempre validadas com total confiabilidade e, acima de tudo, auditabilidade.

Exemplos como o Blockchain da aviação civil (Diário de Bordo Digital da ANAC), a Rede Nacional de Dados da Saúde (RNDS do Ministério da Saúde) e o bCPF (Blockchain CPF da Receita Federal) mostram a evolução de cases de sucesso em âmbito nacional. →

Porém, existe uma tendência pequena, mas crescente, de empresas privadas brasileiras que estão iniciando estudos e projetos em Blockchain para melhorar seus processos e aumentar o valor dos seus produtos, além de oferecer uma imagem positiva para os clientes com a utilização de uma tecnologia confiável.

Empresas integradoras de sistemas e desenvolvedoras também têm oferecido ao mercado serviços de qualidade com base em frameworks Blockchain, tais como o CPqD, a GoLedger e a IASIS Tech. No evento promovido pelo consórcio Hyperledger (que oferece plataformas open-source de Blockchain e DLTs), o Hyperledger Global Forum 2021, diversos casos e palestras foram apresentados, mostrando que o Brasil está se destacando na tecnologia Blockchain para o resto do mundo.

Os próximos anos devem levar o Brasil a um patamar maior que estamos hoje, com mais projetos, cases e profissionais capacitados na tecnologia Blockchain.

Como o panorama das soluções de blockchain no Brasil se compara ao internacional?

Marcos Sarres
CEO
Go Ledger

Chainalysis

A Chainalysis oferece soluções de investigação de criptomoedas e de conformidade às agências globais de aplicação da lei, reguladores e empresas que trabalham em conjunto para combater a atividades ilegais com moedas digitais.

Ela busca gerar transparência para uma economia global construída sobre blockchain, permitindo que bancos, empresas e governos tenham uma compreensão de como as pessoas usam a criptomoeda.

A empresa também fornece iformações, software, serviços e pesquisas em mais de 60 países. Sua plataforma de dados fornece ferramentas de investigação, conformidade e gerenciamento de risco que têm sido usadas para resolver alguns dos casos de ciber-criminosos mais importantes do mundo e aumentar o acesso dos consumidores à criptomoedas com segurança.

Só neste ano a startup já levantou duas rodadas de investimento, uma em março e outra em junho, alcançando assim um valuation de 4.2 bilhões de dólares.

Chainalysis

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2014	Nova Iorque, Estados Unidos	US$ 366.6 M	Coatue, Paradigm, Addition, Ribbit Capital, Sound Ventures, MUFG Innovation Partners, Sozo Ventures, Accel, Benchmark

Fireblocks

Feita para instituições que precisam armazenar e mover ativos digitais sem a dor de cabeça operacional ou de segurança, a Fireblocks é uma plataforma tudo em um para armazenar, transferir e emitir ativos digitais em todo o seu ecossistema.

A startup simplifica as operações trazendo todas as suas trocas, OTCs (Mercado de balcão), contrapartes, carteiras e custódias em uma única plataforma. Carteiras, endereços de depósito e credenciais API são assegurados usando a tecnologia de isolamento de chip com patente pendente e o mais novo avanço em criptografia (MPC). As instituições estão usando Fireblocks para movimentar fundos com segurança em segundos, ao invés de horas.

Com a API da Fireblocks, as instituições passam a ter acesso seguro a toda a gama de protocolos DeFi para estratégias como comércio de câmbio descentralizado e ativos como o token nativo da Cardano, ativos da Plygon, ou Dogecoin.

A startup entrou na lista *The 50 Fintech 2021*, feita pela Forbes e neste ano já levantou duas rodadas de investimento, uma em março e outra em julho, alcançando assim um valuation de US$ 2,2 bilhões.

Fireblocks

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2018	Nova Iorque, Estados Unidos	US$ 489 M	Coatue, DRW Venture Capital, SCB 10X, Sequoia Capital, Spark Capital, Stripes, Ribbit Capital, Paradigm, Cyberstarts, Eight Roads Ventures, MState, Tenaya Capital

StarkWare

A StarkWare resolve os problemas inerentes ao blockchain como escalabilidade e privacidade. Ela permite que o blockchain seja escalado em massa, confiando em provas criptográficas produzidas por um provérbio fora da cadeia que corre na nuvem, e depois verificadas por um contrato inteligente na cadeia. A solução em desenvolvimento pode reduzir o custo de cada transação baseada em blockchain em até 20.000 vezes.

Seus produtos são a StarkNet, uma Zero Knowledge -Rollup descentralizada sobre o Ethereum; o StarkEx, um motor de escalabilidade de segunda camada, que está em produção na Mainnet para escalonar múltiplas trocas e plataformas; e o Cairo, uma linguagem de produção para escalonar dApps usando a tecnologia STARKs.

O gasto energético por cada transição em blockchain ainda é alto, o que limita o número de aplicações. A tecnologia da StarkWare promete acelerar a adoção de blockchain para registrar e assegurar as transações não só de criptomoedas, mas de qualquer coisa que seja transferível digitalmente.

STARKWARE

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2018	Netanya, Hasharon, Israel	US$ 111 M	Paradigm, Sequoia Capital

DefenseArk

Inicialmente conhecida como OpenAVN, a norte-americana DefenseArk atua na proteção de dados e ameaças digitais por meio da coleta de um alto volume de *malwares* disponíveis na internet movida à utilização de tecnologias como Blockchain e Machine Learning. Com isso, a empresa desenvolve soluções para cada uma dessas ameaças com o objetivo de proteger os sistemas de seus usuários em uma velocidade superior à de antivírus tradicionais por meio de plataformas de escaneamento de *malwares* em tempo real (Brightscan) e extensões de cibersegurança a navegadores (Torus). Desse modo, o público-alvo de seus produtos vai desde usuários domésticos, empresas e "*home officers*" até instituições de ensino.

Posto isso, a DefenseArk recebeu seu último investimento em 2019, no qual captou um seed de US$ 1,5 M da plataforma de *equity crowdfunding* SeedInvest.

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2019	Nova Iorque **Estados Unidos**	US$ 2,2 M	MetaSquare Holdings, SeedInvest.

Blockchain no Brasil

Hugo
Co-Founder
Growth Tech

Como a blockchain revoluciona processos de segurança da informação?

Antes de qualquer ponto, destaco que a Blockchain é descentralizada e isso permite uma espécie de "governança coletiva" entre seus atores. Por si só, me parece que esta é uma característica que contribui bastante para segurança da informação.

Criptografia de ponta, rastreamento sofisticado (considerando dentre outros, a descentralização proporcionada), e a imutabilidade dos dados são outras características que podem ampliar a contribuição e sinergia para com os processos de segurança da informação.

Comparado ao mercado internacional, como o Brasil se posiciona quanto ao desenvolvimento de soluções que envolvam blockchain?

Penso que novas soluções em Blockchain tem surgido em todo ecossistema mundial, incluindo a parte brasileira. Por aqui temos avançado bem. Hoje, por exemplo, temos um "unicórnio cripto" na América Latina (Mercado Bitcoin), e este já é um fato muito considerável e de orgulho para quem 'milita' na indústria Blockchain brasileira. Porém, certamente, precisamos dar saltos maiores, fomentar mais o uso da tecnologia, educar nossa comunidade, investir em pesquisa e desenvolvimento, além de melhorar o ambiente competitivo que temos.

A Growth Tech é uma das startups pioneiras no Brasil, no segmento Blockchain. Como está sendo a trajetória de vocês?

Sim, iniciamos nossas operações em 2016. De lá pra cá vimos estudando bastante esta fabulosa tecnologia, e desenvolvendo projetos diversos. Nossa primeira solução foi uma rede de cartórios em Blockchain. Nela, realizamos alguns serviços pioneiros no Brasil, em parceria com grandes incorporadoras. Apesar de todo êxito, o ambiente cartorial brasileiro é bastante complexo e percebemos que várias questões regulatórias precisariam ser transpostas para o devido avanço desse movimento. Então, decidimos focar nossa energia em novas oportunidades, e aí desenvolvemos novas soluções. Criamos a Digi, uma plataforma para gestão de condomínios — que utiliza Blockchain para maior transparência de processos fundamentais para este mercado. Desenvolvemos também 'PropLedgers', uma plataforma para assinatura e registro de documentos em Blockchain permissionada. →

Desde o ano passado, “colocamos o pé” na Blockchain pública, e duas novas soluções foram desenvolvidas. “Registra Fácil” — plataforma para registro de documentos na Blockchain Ethereum e “PropToken” — solução para suportar novas modalidades de negócios imobiliários, através da tokenizacao. Definitivamente, percebemos que nosso mercado-alvo é o Imobiliário e estamos muito animados com as oportunidades que vimos amadurecendo nesta temática de tokenizacao. Vale destacar que essas duas últimas soluções estão em fase final de testes e devem estar disponíveis ao público final em no máximo 2 meses.

Blockchain em cybersecurity

Hugo
Co-Founder
Growth Tech

Destaques e tendências

Blockchain em cybersecurity

Blockchain acelera a adoção da internet das coisas (IoT)

Ao longo dos últimos anos temos visto um aumento constante no número de dispositivos inteligentes e capazes de se conectar com a internet para facilitar nosso dia a dia. Entretanto, trazer estes dispositivos para o nosso cotidiano, para dentro de nossas casas, pode abrir a porta para grandes ameaças e ataques cibernéticos.

Nesse sentido o Blockchain surge como ponto par essencial para viabilizar o surgimento de um ecossistema de IoT seguro. Ao longo das últimas décadas, como mostrou o report da Gartner de tecnologias emergentes, o IoT que vinha em uma crescente com o nível de maturidade projetado para um período próximo (entre 2-5 anos) regrediu para uma projeção de maturidade para a faixa dos próximos 5-10 anos.

Grande parte dessa regressão decorreu das brechas de segurança que os dispositivos conectados a rede ofereciam para invasões.

Tanto o Blockchain quanto o IoT - como tecnologias autônomas - já provaram ser altamente disruptivas. Porém, uma vez que a IoT utiliza amplamente a rede de sensores sem fio existente (WSN) ela permanece vulnerável à privacidade e ameaças à segurança. Por outro lado, o blockchain, por seu design e arquitetura é considerada como uma Trust Machine e assim possui o potencial para resolver os principais problemas de segurança encontrados na IoT.

IoT é um sistema que conecta o mundo físico a um domínio substancial do sistema de informação - o mundo cibernético. No entanto, devido a vários motivos, a segurança da IoT não costuma ser devidamente tratada na fase de design dos dispositivos e do produtos. Com o advento e aumento da popularidade do Blockchain, houve uma mudança de paradigma no desenvolvimento de IoTs, particularmente integrando essa tecnologia e Blockchain, que por seu fator de segurança se tornarão dominantes nos próximos anos.

Cooperative Storage Clouds

Dentre os diversos motivos que tornaram o armazenamento em nuvem dominante no mercado um dos principais foi o custo por terabyte por mês, que baixou uma ordem de magnitude e as empresas não precisam mais criar e manter seus próprios sistemas de servidores, pagar por backups externos e arcar com o fardo de especialistas equipes para manter tudo funcionando perfeitamente.

No entanto, apesar dos custos significativamente mais baixos e do aumento da conveniência, as empresas decidiram coletivamente confiar seus dados a terceiros. Por um lado a lógica faz sentido, é mais barato, mais confiável e bastante redundante. Contudo, toda essa economia e conveniência tem um custo e novamente tem a ver com as empresas sendo forçadas a permanecer competitivas ao escolher um serviço que tira seu poder de controlar seus dados.

O futuro parece ser ainda mais compartilhado, pois a maior parte do armazenamento de dados estará no blockchain, que é ainda mais barato por ser cooperativo. Da mesma forma que o Airbnb ou o Uber, ele usará o excesso de capacidade de todos os sistemas do mundo para reduzir o custo do armazenamento de dados em outra ordem de magnitude.

Hoje, já é possível combinar a eficiência e confiabilidade da nuvem com a segurança e controle descentralizados do modelo de armazenamento cooperativo em nuvem. Dessa forma eles se tornam a base para mais uma revolução no armazenamento de dados.

Contra os sistemas de armazenamento de dados descentralizados, o armazenamento em nuvem é bastante imperfeito. Em primeiro lugar, porque só temos os sistemas tradicionais como quadro de referência, e acreditamos que já é acessível o suficiente. Em segundo lugar, pensamos na segurança de dados como uma questão de redundância e tempo de atividade e esquecemos as questões de criptografia. Terceiro, ignoramos completamente o fato de que os dados estão nas mãos de terceiros.

Graças à contribuição flexível, várias empresas podem alugar seu armazenamento redundante e o efeito composto dessa prática reduzirá ainda mais os custos em todas as frentes. A segurança dos dados é aumentada graças aos algoritmos de distribuição geográfica. Os dados são armazenados em qualquer lugar na nuvem, o que significa que não há um único intermediário. Isso resulta em descentralização total e redundância real, privacidade total e uma redução de custos extremamente necessária.

Blockchain em diferentes setores

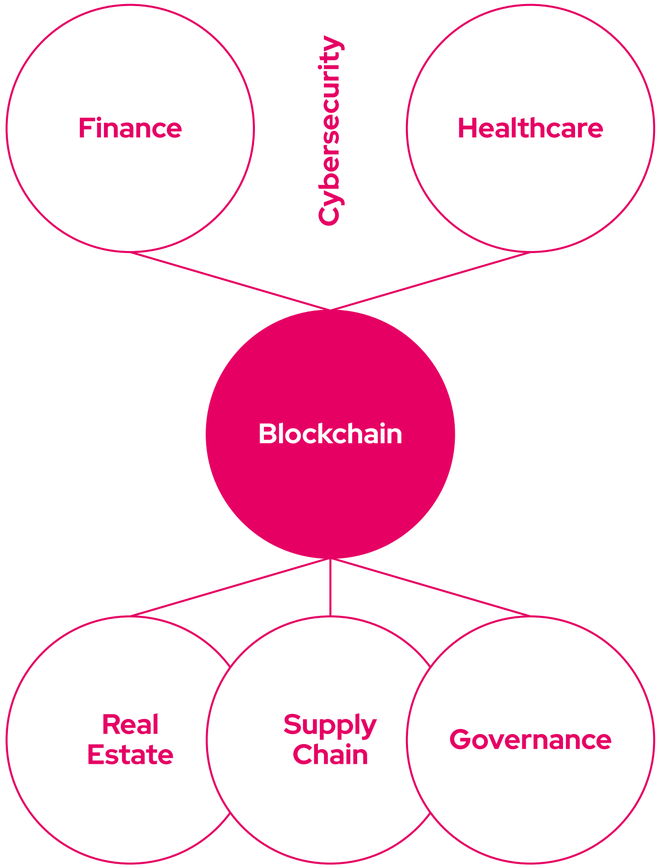
Finanças: No setor de finanças, o maior valor da tecnologia blockchain está na transparência das transações e da não adulteração dos dados transacionados. Armazenar tudo que é realizado na blockchain é mais transparente e seguro, se comparado às formas de tecnologia tradicional ou em papel. Grandes bancos já se utilizam da tecnologia para deixar seus dados mais seguros.

Saúde: O ataque a dados médicos tem sido uma preocupação crescente nos últimos anos, e organizações de saúde podem se beneficiar guardando essas informações dentro da blockchain. A BurstIQ é uma plataforma americana que auxilia empresas no setor de saúde a armazenar e proteger dados de diferentes departamentos e instituições em tempo real.

Setor imobiliário: Validação de propriedade e transferência e transferência de fundos podem ser solucionados utilizando da tecnologia blockchain, garantindo a veracidade e segurança das informações.

Supply chain: Gigantes presentes no mercado de abastecimento como Walmart e BMW se utilizam da blockchain para melhor a segurança de seus dados e a transparência da operação. A rastreabilidade dos produtos se destaca como principal solução da tecnologia.

Governança: A blockchain pode ser uma ferramenta poderosa nos processos de governança e compliance, melhorando a segurança e transparência das organizações. Confira melhor o tema no nosso Inside ESG #4, que explora as aplicações e as soluções da tecnologia voltadas para governança corporativa.



Blockchain em saúde

Pedro Petri
Co-Founder & CEO
ZHealth

A tecnologia das redes blockchain já está presente há mais de uma década em diversos setores. Se antes era restrita à soluções financeiras, cada vez mais está se provando como uma tecnologia capaz de diminuir burocracias, aumentar o compliance e a segurança de setores que necessitam de confiabilidade de dados - como o setor da saúde. Foi pensando nisso que a Zhealth nasceu, com a missão de trazer mais confiabilidade e segurança para todo o ciclo de valor do setor, com soluções que vão desde a conectividade de prontuários eletrônicos, até cadeias de logística.

Nós entendemos o quanto é difícil e custoso para empresas realizarem mudanças de CRMs ou outros sistemas, por isso desenvolvemos com o menor impacto possível na operação do cliente, desmistificando muito sobre os altos custos e baixa disponibilidade associadas a esse tipo de rede. Com as nossas soluções você não precisa de desenvolvedores de blockchain para fazer blockchain. Você só precisa de desenvolvedores que saibam ler e escrever chamadas de API. É realmente muito simples. Uma das melhores coisas sobre blockchain é que ela prova o processo por trás de suas decisões de negócios.

Ao lidar com auditorias, regulamentos de conformidade etc., você saberá que a prova vive na blockchain para sempre. Isso economizará tempo na verificação do trabalho, dinheiro em litígios e recursos para tarefas de alto nível.

Blockchain não é muito complicado. Muito pelo contrário, ela é uma ferramenta muito útil na garantia de segurança, controle de acesso e compartilhamento de dados. Nossos produtos se traduzem em uma API fácil de usar que se integra diretamente aos sistemas de processos de negócios existentes. Pense nisso como uma interface simples que esconde as complexidades da blockchain. É como qualquer outro software que você esteja usando — funciona perfeitamente com outros sistemas e fornece um back-end de blockchain para todos os dados que precisam de validação futura. Diversas grandes empresas já aderiram às nossas soluções e acreditamos que com provas de conceito ágeis e com bom custo benefício conseguimos demonstrar valor para empresas de todos os tipos e tamanhos.

Cybertechs

Glossário de categorias

Categorias

NETWORK & INFRASTRUCTURE SECURITY
Companhias que apliquem processos de proteção da infraestrutura de rede, instalando medidas preventivas para negar acesso não autorizado, modificações, exclusões e roubo de recursos e dados. Essas medidas de segurança podem incluir controle de acesso, segurança de aplicativos , firewalls, redes virtuais privadas (VPN), análise comportamental, sistemas de prevenção de intrusão e segurança sem fio. Se relaciona com a camada física de transmissão e conexão. Também englobamos soluções de endpoint e messaging security nesta categoria.

WEB SECURITY
Medidas e protocolos de proteção que empresas utilizam para proteger suas organizações de cyber criminosos e ameaças que usam a web como canal. Se relaciona com a camada não física de segurança, o que engloba internet e segurança de sites.

APPLICATION SECURITY
Medidas de segurança que impedem roubo/sequestro de dados e códigos dentro de dentro de aplicativos e plataformas.

DATA PROTECTION
Data protection engloba empresas responsáveis pela proteção de informações sensíveis à empresa (Banco de Dados, Informações de Corporações) e enquadram às corporações na LGPD.

MOBILE SECURITY
Empresas que atuam com produtos e serviços voltados a garantir a segurança do device (dispositivo móvel), IoS, Android. Via de regra, são companhias que visam a proteção contra ameaças associadas à conexões wireless.

SECURITY OPERATIONS & INCIDENT RESPONSE
Empresas que desenvolvem soluções estruturadas para responder a vazamentos de dados ou ciberataques. A solução visa minimizar os impactos de ataques cibernéticos já realizados, possibilitando um controle da situação com o menor tempo e custo.

IOT SECURITY
Empresas que atuam com segurança relacionada a internet das coisas, aparelhos e networks que estão conectados entre si.

IDENTITY & ACCESS MANAGEMENT
Empresas que desenvolvem soluções que garantem a veracidade das informações e identidades de todas as partes envolvidas em um processo. Aqui se encontram empresas de Identidade as a Service, que capturam, armazenam e asseguram a veracidade do usuário, e companhias de assinatura digital, que trazem inovação e segurança para todo o ciclo de documentos.

Categorias

BLOCKCHAIN
Blockchain as a Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes desse tipo em nome de outras organizações.

FRAUD & TRANSACTION SECURITY
Empresas que aplicam tecnologias de análise de dados para gerar avaliações e insights sobre clientes, permitindo mapear riscos, analisar a conformidade com leis e regulamentações e se prevenir contra perdas, desvio, fraude e ataques cibernéticos.

CLOUD SECURITY
Cloud Secutiry refere-se às startups que atuam com políticas, tecnologias, aplicativos e outros mecanismos de controle utilizados para proteger IP virtualizado, dados, aplicativos, serviços e a infraestrutura associada de computação em nuvem.

SECURITY CONSULTING & SERVICES
Security Consulting and Services refere-se a startups que prestam serviços para testar ou aprimorar serviços de cibersegurança. Um exemplo aqui são empresas que atuam com simulações de ataques cibernéticos como forma de identificar possíveis falhas nos sistemas.

GOVERNANCE, RISK AND COMPLIANCE
Soluções GRC (Governança, Risco e Cokmpliance) são compostas por ferramentas que abrangem a gestão de riscos, governança corporativa e práticas de auditoria e controle, com o objetivo de garantir a conformidade com leis, regulamentos, frameworks e padrões de boas práticas.

Cybertechs

Glossário de termos

Glossário – Cybersecurity

Ameaça: Causa potencial de um incidente.

Ativo: Tudo aquilo que possui valor.

Ativo de Informação: Patrimônio intangível da corporação, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a organização por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da organização ou por infraestrutura externa, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Confidencialidade: Propriedade dos ativos da informação da corporação, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Controle: Medida de segurança adotada pela corporação para o tratamento de um risco específico.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da corporação.

Integridade: Propriedade dos ativos da informação da corporação, de serem exatos e completos.

Risco de Segurança da Informação: Efeito da incerteza sobre os objetivos de segurança da informação da corporação.

Segurança da Informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da corporação.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da corporação.

Engenharia Social: Manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais.

Acha que faltou algum termo? Manda pra gente!