

Blockchain e Criptomoeedas



Rodrigo Caldas de
Carvalho Borges

Dezembro
2019

Bitcoin

O início de tudo



A História das Moedas Digitais

30 anos de trabalho até o Bitcoin

- 1982: “**e-Cash**” – **David Chaum** – moeda digital emitida pelos bancos, porém tinha o problema do “gasto-duplo”
- 1997: “**Hash Cash**” – **Adam Back** – introduziu o algoritmo para validação das transações para envio de e-mails
- 1998: “**B-Money**” – **Wei Dai** – apresentou o conceito de *proof of work* (prova de trabalho) para emissão de moedas, porém sem adequação automática do algoritmo
- 1998: “**Bit Gold**” – **Nick Szabo** – mesmo conceito de *proof of work*, com ajuste automático do algoritmo
- 2004: “**RPOW**” – **Hal Finney** – sistema semelhante ao do Hash Cash, com aprimoramentos



Problema a ser solucionado

Como evitar o “Gasto Duplo” sem intermediário?



2008

A crise financeira e da confiança

- Pior crise financeira da século XXI
- Bolsas perderam mais de 4 trilhões de dólares
- Governos injetaram recursos para salvar os bancos
- Movimento cypherpunk cresce

31 de Outubro de 2008

Surge o Bitcoin



White Paper do Bitcoin

Publicado em grupo de cypherpunks com apenas 09 páginas, a qual apresentaria conceitos que mudariam toda uma lógica de como se fazer negócios

A Peer-to-Peer Eletronic Cash System

- Sistema de dinheiro eletrônico de ponto à ponto
- Troca de valor sem intermediário
- Resolveu a questão do “gasto duplo”
- Apresentou ao mundo o que seria posteriormente conhecido como Blockchain



Moeda não estatal

Liberdade das operações físicas no mundo digital

- Sistema transparente e aberto
- Qualquer interessado pode verificar os códigos de funcionamento e sugerir melhorias
- Todas as transações estão disponíveis para consulta
- Transações podem ser realizadas livremente, independente do valor e/ou horário, a custos irrisórios
- Regras criptográficas asseguram o anonimato
- Fracionado em até 08 casas decimais
- Limitado a 21 milhões de unidades (já existem 18 milhões), devendo o último ser minerado em 2140

Satoshi Nakamoto

O mistério do criador

- Quem seria?
- Ele, Ela ou Eles?
- 2011 última “aparição”
- Candidatos mais cotados: Nick Szabo, Hal Finney e Wei Dai
- Em dezembro de 2017 alcançou patrimônio de 19 bilhões de dólares
- Anonimato: equilíbrio no sistema



Blockchain

A tecnologia da confiança

General Purpose Technology

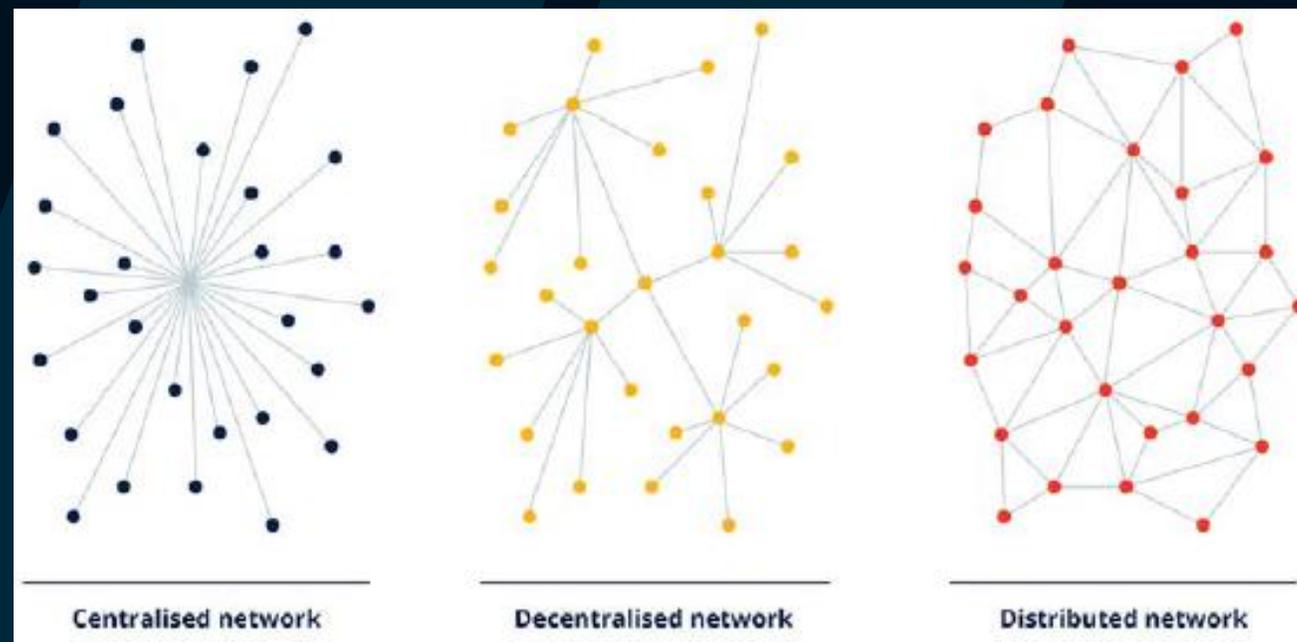
Uma tecnologia em constante desenvolvimento

- Comparada à internet (estamos em 1995)
- Potencializa outras tecnologias, tal como Inteligência Artificial e Internet das Coisas
- Tecnologia ainda em desenvolvimento
- Ainda desconhecemos o seu efetivo potencial

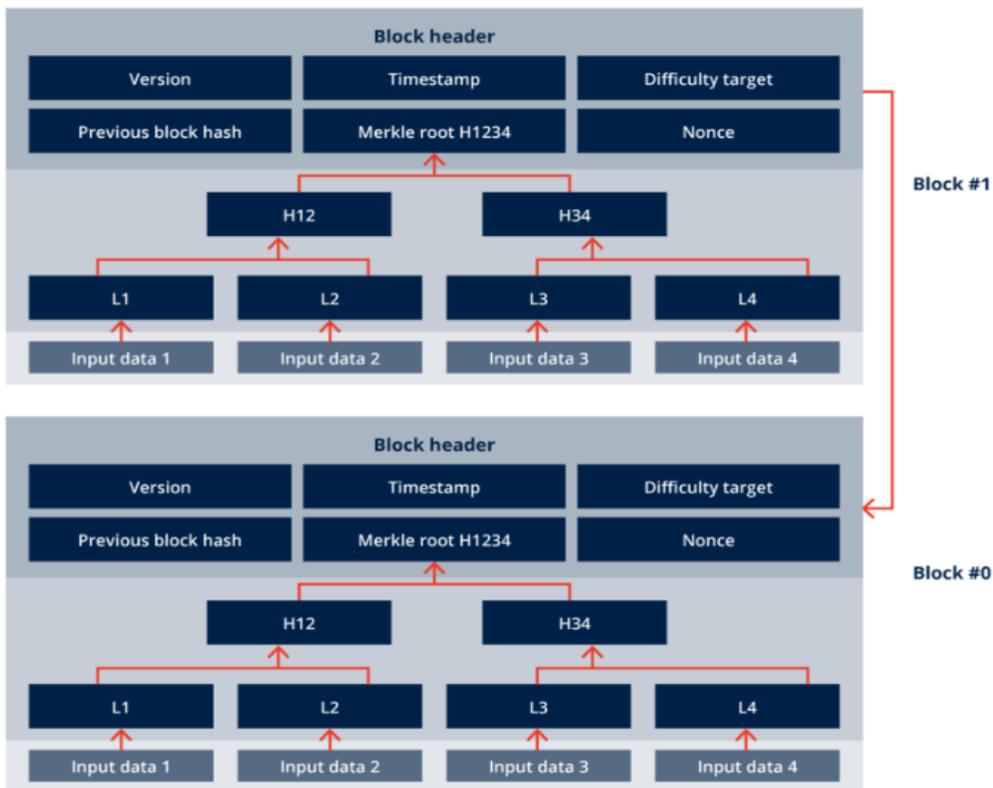
Os diferentes tipos de rede

Do controle isolado ao coletivo

- **Rede Centralizada:** todos os participantes são ligados a uma única autoridade responsável pela operação e controle do sistema. Modelo comum utilizado por serviços online tal como Amazon e eBay
- **Rede Descentralizada:** os dados são espalhados em diversos centros de controle, todos interligados diretamente à uma autoridade central. Este modelo é geralmente utilizado nos sistemas dos bancos
- **Rede Distribuída:** não há uma autoridade central. O poder é exercido de forma coletiva, por meio de um mecanismo de consenso. Essa foi a inovação trazida pelo Blockchain



Como Funciona



- As transações são “assinadas” digitalmente pelas partes, mediante criptografia
- As transações são agrupadas em blocos
- Os blocos são transmitidos pela rede
- Os mineradores (hardwares que rodam o software) tentarão resolver o cálculo matemático, sendo que o primeiro a solucionar conectará o bloco na corrente
- Algoritmo programado para solucionar em 10 minutos, ajustada a dificuldade conforme participantes da rede

Os diferentes Blockchains

A governança da rede

			Acessar	Lançar Transações	Contribuir com melhorias	Exemplo
TIPOS DE BLOCKCHAIN	Pública	Pública Não Permissionada	Todos podem acessar	Todos	Todos	Bitcoin, Ethereum
		Pública Permissionada	Todos podem acessar	Participantes autorizados	Todos ou participantes autorizados	Sovrin
	Privada	Consórcio	Restrita a participantes autorizados	Participantes autorizados	Todos ou participantes autorizados	R3 Corda
		Privada Permissionada	Restrita a participantes autorizados	Operador da rede	Apenas o operador da rede	Sistemas internos de bancos

O que faz do Blockchain uma tecnologia tão importante?

Principais características



Segurança

Os dados ficam distribuídos na rede, com todos possuindo uma cópia exata da rede



Imutabilidade

As regras de consenso impedem que um único participante altere as informações inseridas na rede



Transparência

As informações inseridas na rede podem ser disponibilizadas para consulta de qualquer pessoa





DLT x Blockchain

Diferenças

- Blockchain é um tipo de DLT – Distributed Ledger Technology
- Redes distribuídas, porém com características distintas em relação à arquitetura



Mineração

Como são gerados os Bitcoins

- Bitcoins são gerados a partir da validação das transações
- A cada resolução de cálculo matemático e inserção de novos blocos à rede, novos Bitcoins são gerados
- Mecanismo de consenso
- A cada 10 minutos Bitcoins são gerados
- Hardware específico para isso
- Custo energético
- Algoritmo ajustado conforme quantidade de hardwares plugados na rede



Smart Contracts

Não são contratos e muito menos inteligentes

Definição

- Tratam-se de protocolos de computador que executam de forma automática instruções uma vez atingidas condições previamente definidas (ex: o recebimento de bens depende do pagamento ser processado)

Finalidade

- Permite que pessoas realizem transações com desconhecidos sem um intermediário de confiança
- Transações são executadas de forma automática, desde que preenchidas as condições determinadas



coinbase



Exchanges

As bolsas de criptoativos

- Realizam a intermediação em operações de venda e compra de criptoativos
- Facilitam as operações
- Mercado balcão, diferentes preços entre Exchanges
- Enfrentam problemas com fechamento das contas bancárias
- Ação no CADE em face dos bancos
- No Brasil a Receita Federal criou regras para relativas às obrigações fiscais
- Não existem regras específicas de operação
- Problemas com hackeamento e guarda das chaves



Gestoras e Fundos

Produtos e serviços baseados em investimentos com criptoativos

- Gestoras de carteiras de criptoativos
- Fundos de Arbitragem
- Serviços de Wallet

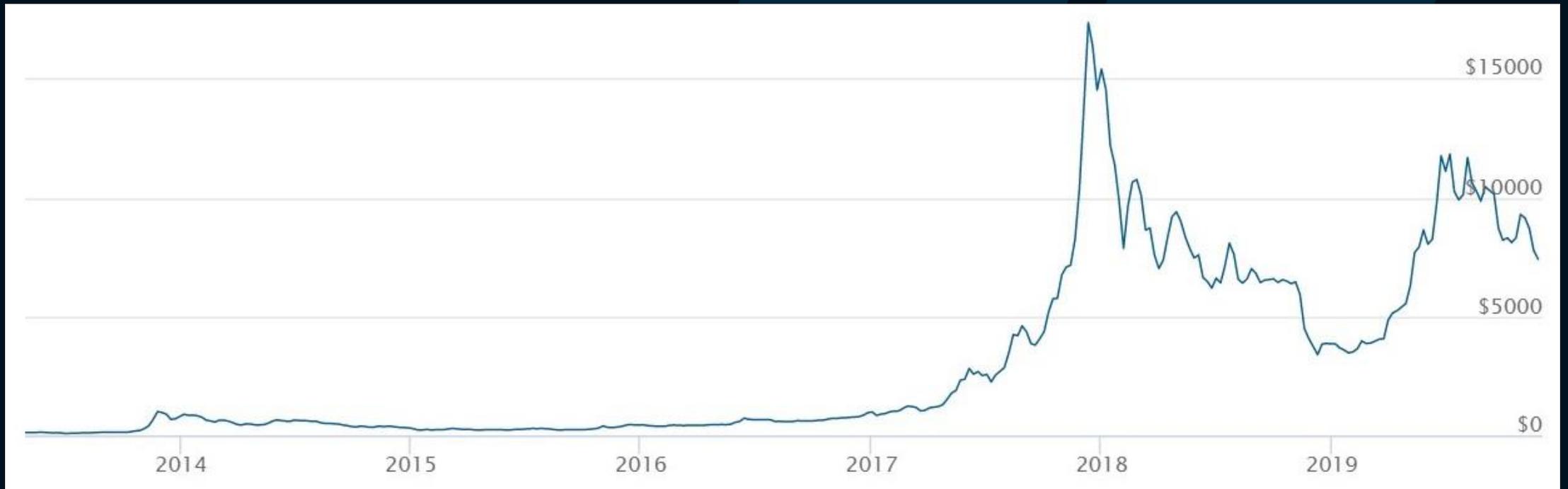
O anonimato relativo

Os benefícios e dificuldades

- Todas as transações são rastreáveis, permitindo seguir os recursos de ponta a ponta
- A identidade dos titulares das “wallets” são protegidas por criptografia
- Garante a segurança aos usuários com relação aos seus dados
- Utilizada no passado por criminosos na “Deep Web” – Silk Road – como moeda para compra de ilícitos (drogas, armas, pornografia)
- Facilita a utilização por pessoas mal intencionadas



Histórico de Valorização do Bitcoin



OBRIGADO



**Rodrigo Caldas de
Carvalho Borges**

E-mail
rborges@cbassociados.com.br

Website
www.cbassociados.com.br

Blockchain e Criptomoeedas

The background features a dark blue field filled with numerous semi-transparent, glowing blue cubes and rectangular prisms. These shapes are arranged in a way that suggests a 3D grid or a complex digital structure. Interspersed among these shapes are thin, white and light blue lines, some of which form a grid pattern. The overall effect is that of a futuristic, data-driven environment. A large, bold, black 'Z' shape is superimposed over the center of the image, partially obscuring the cubes and lines.

Rodrigo Caldas de
Carvalho Borges

Dezembro
2019

Tokenização de ativos

O mundo tokenizado



O mundo dos criptoativos

Criptomoedas ou criptoativos?

- Atualmente são 4.876 criptoativos , com as mais diversas funções e naturezas
- Volume de mercado atual de 201 bilhões de dólares – auge em janeiro de 2018 com 829 bilhões de dólares
- Bitcoin representa aproximadamente 50% do mercado total de criptoativos
- Cotação atual do Bitcoin em torno de 7,5 mil dólares – auge em dezembro de 2017 com 19,7 mil dólares



#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$134.022.464.132	\$7,413,69	\$18.515.988.816	18.077.712 BTC	-1,88%	
2	 Ethereum	\$16.474.744.961	\$151,47	\$7.104.639.528	108.763.555 ETH	-0,39%	
3	 XRP	\$9.722.868.910	\$0,224547	\$1.150.205.244	43.299.885.509 XRP *	-0,61%	
4	 Tether	\$4.123.748.551	\$1,00	\$20.723.837.128	4.108.044.456 USDT *	0,28%	
5	 Bitcoin Cash	\$3.925.498.691	\$216,36	\$1.266.284.117	18.143.400 BCH	-1,07%	
6	 Litecoin	\$3.036.872.283	\$47,64	\$2.766.236.216	63.748.544 LTC	0,23%	
7	 EOS	\$2.610.844.481	\$2,77	\$1.750.308.741	942.542.303 EOS *	0,52%	
8	 Binance Coin	\$2.403.192.872	\$15,45	\$197.982.523	155.536.713 BNB *	-1,32%	
9	 Bitcoin SV	\$1.878.722.298	\$103,98	\$373.615.973	18.068.415 BSV	-3,20%	
10	 Stellar	\$1.153.303.048	\$0,057508	\$218.856.230	20.054.779.554 XLM *	-1,94%	

ICO

Initial Coin Offer

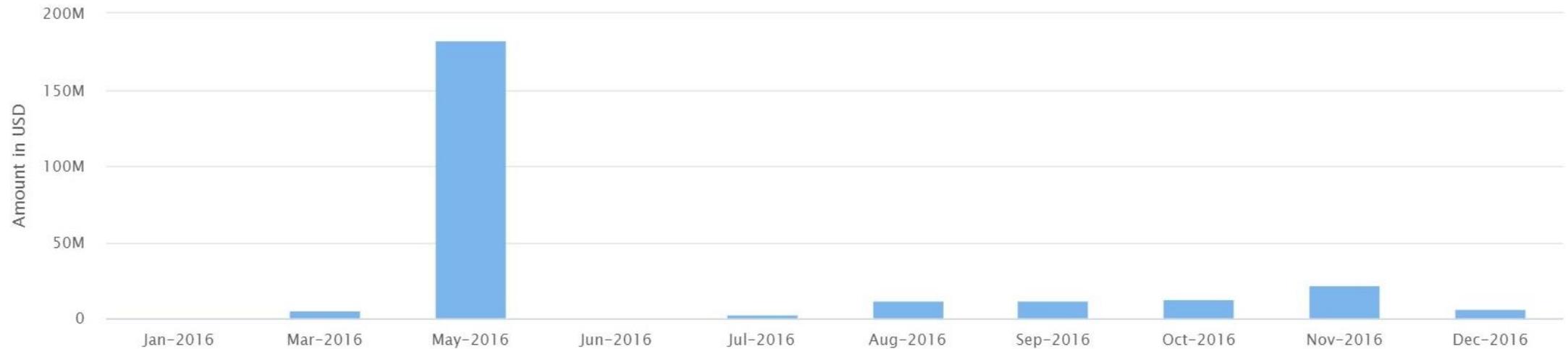
- Utility Tokens (tokens de utilidade)
- Os Tokens são o ativo em si
- Possuem finalidade específica para utilização em determinado ambiente
- Ficha para utilização
- Ganho de clientela e marketing
- Block.One – 4 bilhões de dólares para EOS, Telegram 1,7 bilhão de dólares
- Cases no Brasil, regulação menos restritiva
- EUA alterou interpretação do “Howey Test”



2016

Total Raised in the Period: USD 256,922,741.00

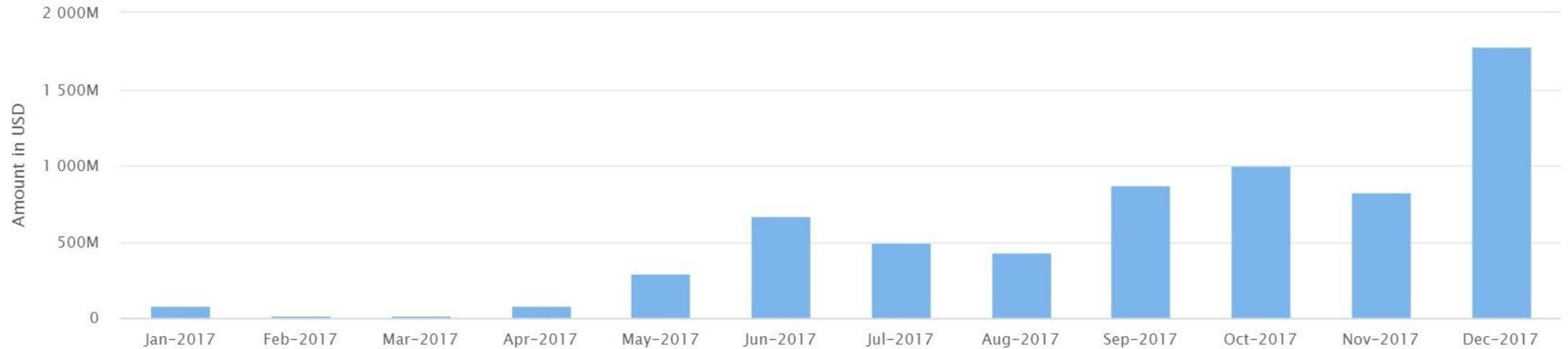
All data compiled by CoinSchedule



2017

Total Raised in the Period: USD 6,557,847,293.00

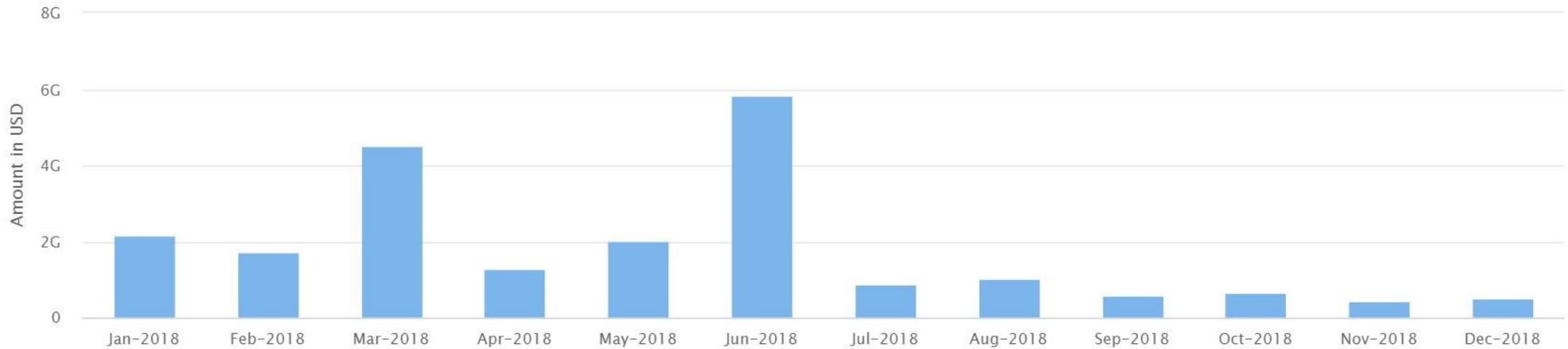
All data compiled by CoinSchedule



2018

Total Raised in the Period: USD 21,620,755,845.00

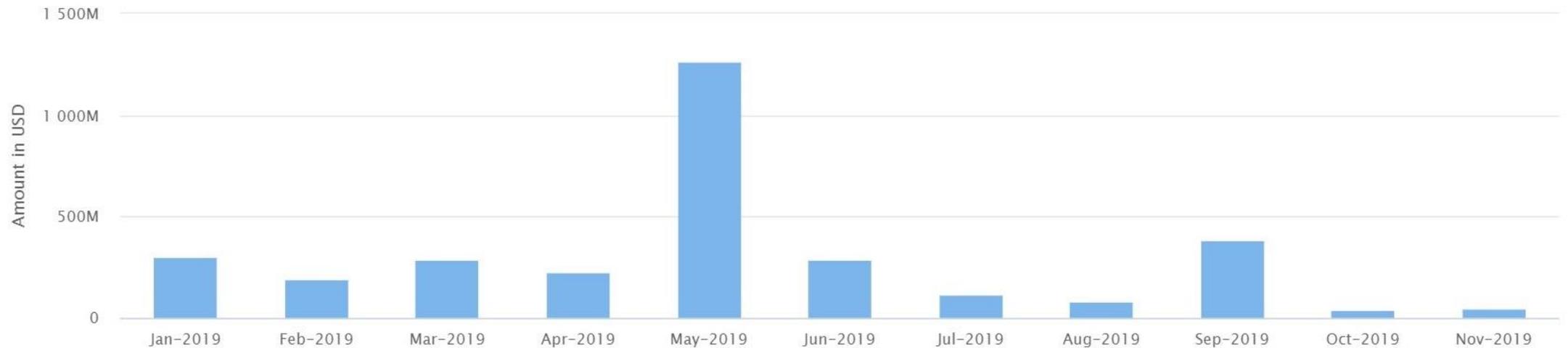
All data compiled by CoinSchedule



2019

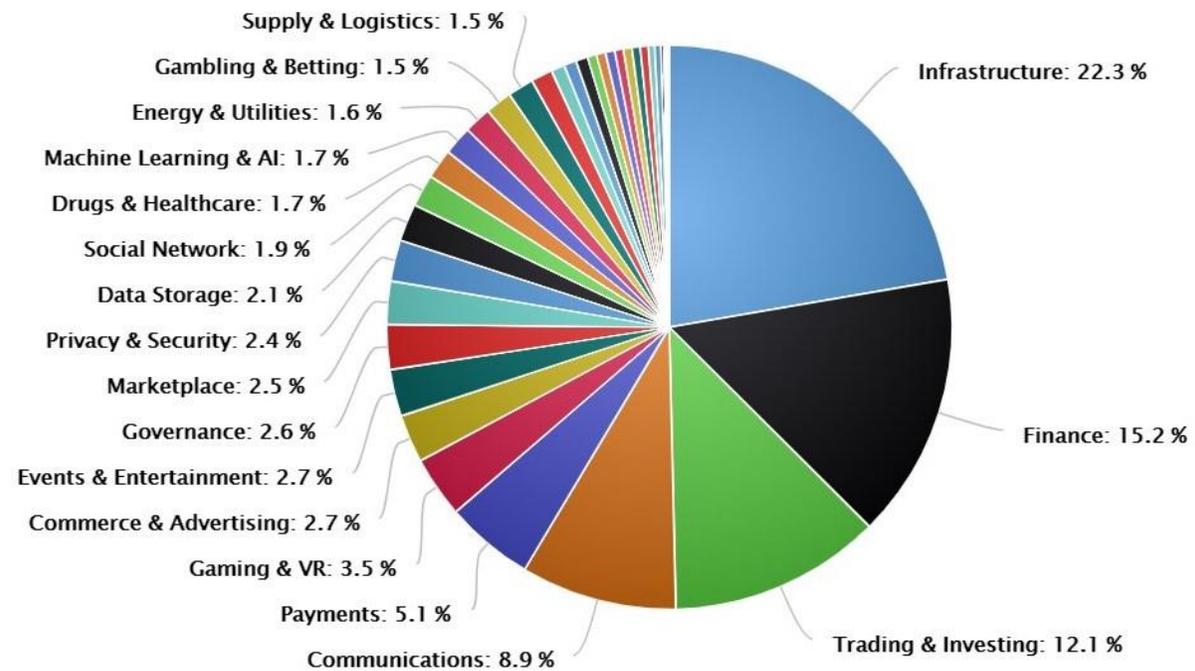
Total Raised in the Period: USD 3,250,208,609.00

All data compiled by CoinSchedule



ICO por mercados

Categories by Amount Raised



STO

Security Token Offer

- Security Token (tokens com valor mobiliário)
- Representam outro ativo
- Ações, imóveis, obras de arte, etc.
- Aumentam a liquidez
- Dificuldades regulatórias
- Banco BTG – ReitBZ – fundo imobiliário; Basement da Kria – fundo para startups; REM – Royal mint Gold



Stable Coin

A efetiva digitalização da moeda

- Tokens representativos de cesta de ativos
- Permitem todos os benefícios trazidos pela tecnologia Blockchain
- Reduzem custos de transações
- Países estudam a substituição do dinheiro papel por alternativas utilizando-se da tecnologia Blockchain
- Permite a ecossistemas criarem sua moeda própria





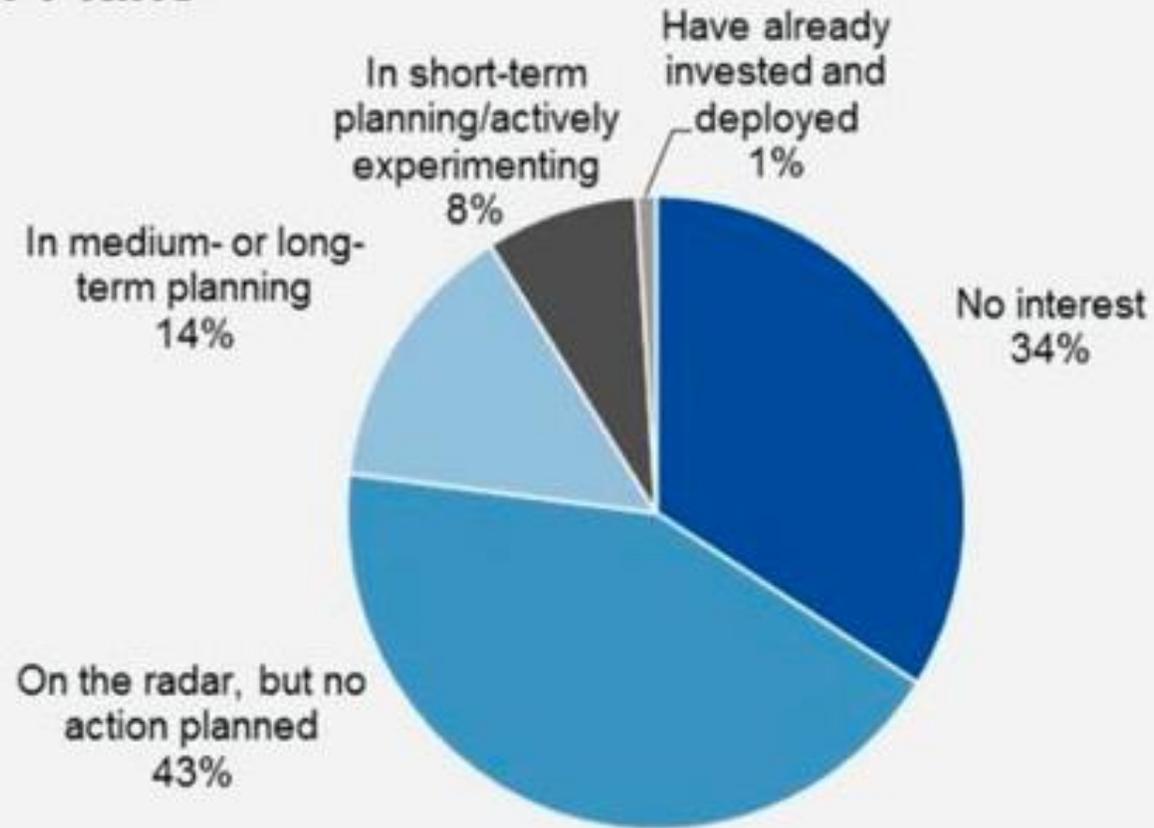
A large iceberg floats in a deep blue sea under a clear sky. The iceberg's tip is visible above the water, while the vast majority of its mass is submerged, illustrating the concept of 'the tip of the iceberg'. The image is overlaid with several thick, black diagonal lines that create a modern, geometric aesthetic.

BITCOIN É APENAS A PONTA DO ICEBERG

O potencial da tecnologia Blockchain poderá impactar todos os setores da economia



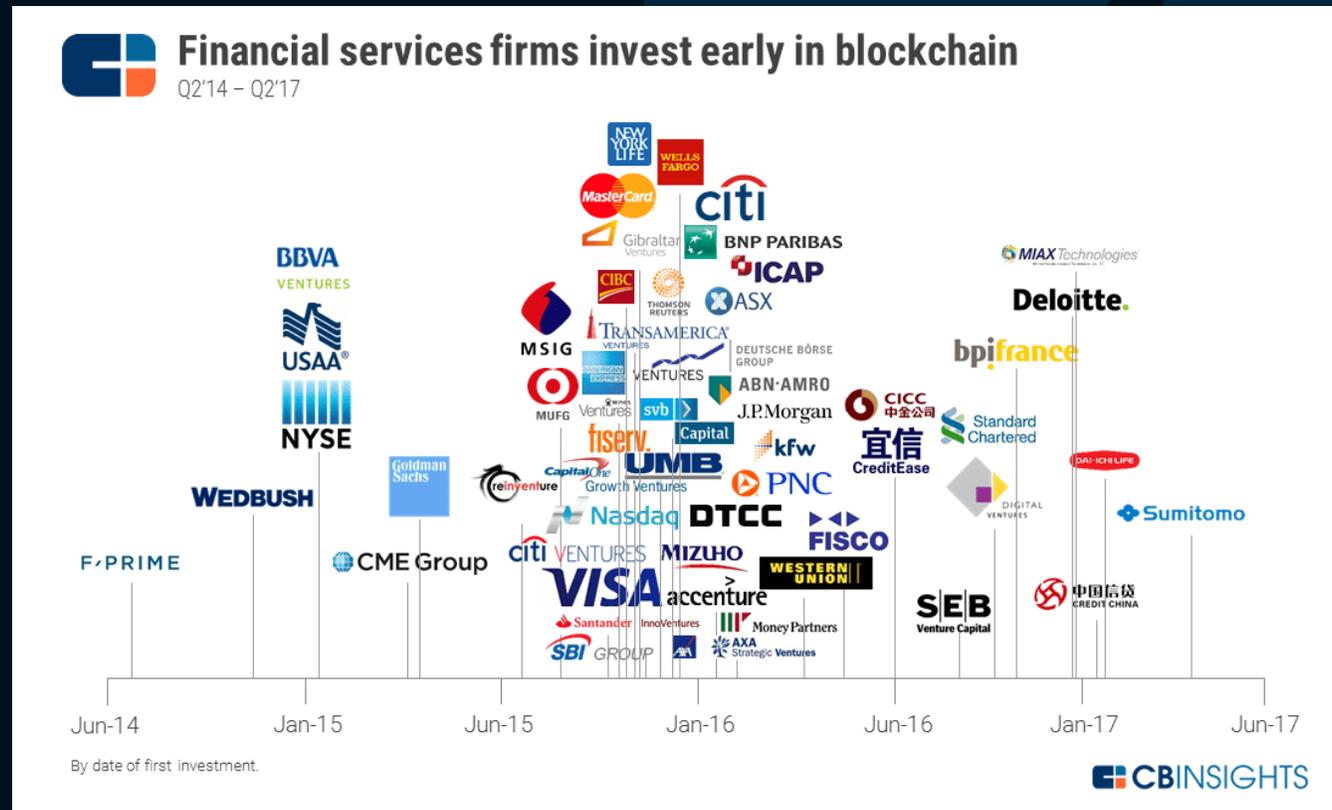
Blockchain Plans



Q: What are your organization's plans in terms of blockchain?
Base: Total answering, excludes DK, n = 3,138
ID: 355300

© 2018 Gartner, Inc.

Empresas do setor financeiro que investiram em Blockchain



Grandes empresas que investiram em Blockchain

TOP GLOBAL BRANDS INVEST IN BLOCKCHAIN



amazon



BOEING

Alibaba.com

MAERSK



BOSCH

Walmart

DE BEERS

RENAULT
Passion for life

COMCAST



AMERICAN EXPRESS

Sprint



KLM

CISCO

AIRFRANCE



WESTERN UNION
moving money for better



AVADO

Learning that works London | Hamburg | New York | Singapore | Hong Kong | Sydney

Blockchain na prática

Casos de uso nas diferentes indústrias

Casos na práticos

Meios de Pagamento

Propriedade Intelectual

Auditoria

Criptoativos

Rastreamento de Produtos

Registro Imobiliários

Micro Pagamentos

Identidade Digital

Gastos Públicos

Votação

Identidade

Uma identidade única e universal para todos



Nossa coleção de documentos

Mera identificação

- Certidão de nascimento
- Certidão de casamento
- RG
- CPF
- Passaporte

Habilitação

- CNH
- CRM
- OAB
- CREA



Problemas



- Sistema ineficaz
- Elevados custos com mecanismos de identificação
- Facilita ocorrência de fraudes
- Burocrático

Identidade única, digital e universal

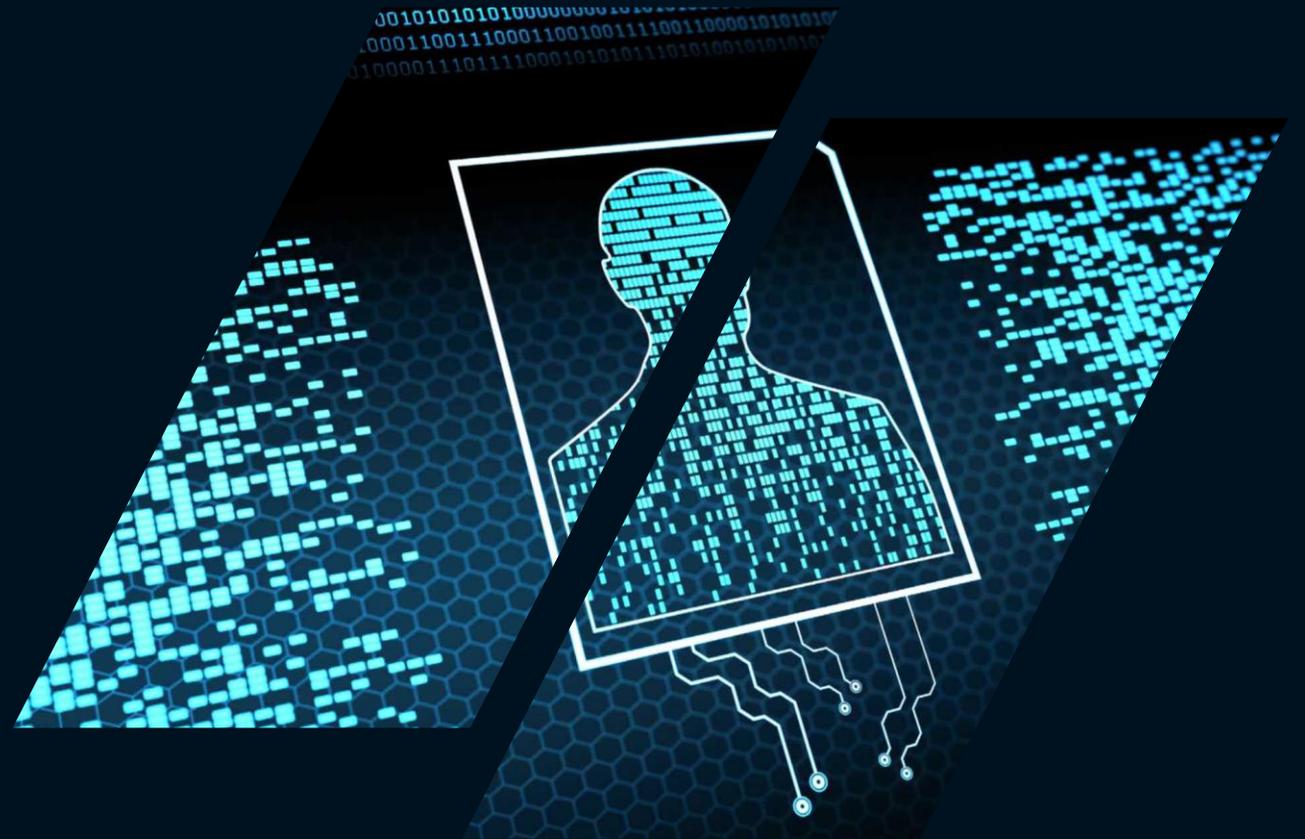
Identificação de uma mesma pessoa
perante diversos fatos jurídicos

Benefícios

- Maior liberdade aos indivíduos
- Escolha de quais informações compartilhar
- Dificulta a penetração de hackers
- Evita a retenção dos documentos

Casos Práticos

- Estônia
- Civic



Votação

Maior segurança e transparência



Atuais sistemas

Votação em papel e eletrônica

Problemas Enfrentados

- Desconfiança
- Falta de transparência
- Fraudes



Votação em Blockchain

Transparente

Auditável em tempo real

Reduz risco de fraude

Protege a identidade

DESAFIOS



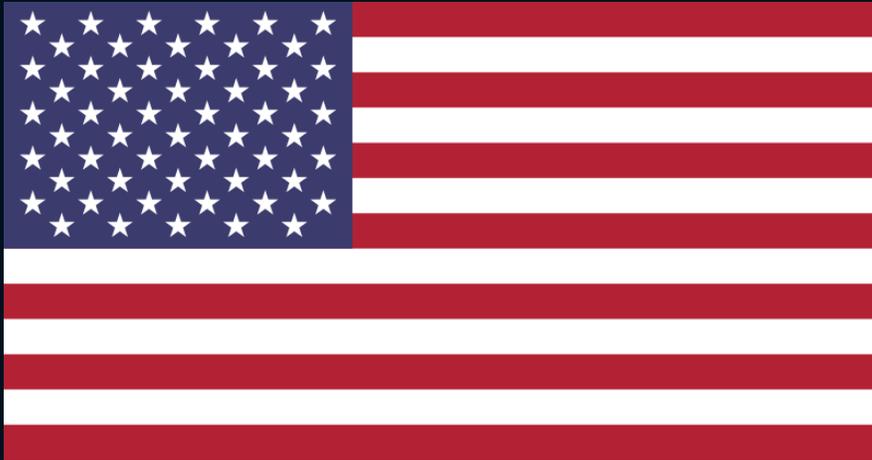
Regulação



Infraestrutura de rede

Experiências realizadas

Votação Soldados



Plebiscito Farcs



Supply Chain

Garantia da origem dos produtos



Rastreabilidade

A imutabilidade somada à transparência conferem ganhos substanciais ao setor logístico

- O uso de Blockchain reduz o número de intermediários, resultando em ganho de confiança e redução de custos
- Essas características tem permitido ganho de eficiência nos mais variados setores econômicos



Casos em implementação



Transporte Marítimo



Produtos Orgânicos



Vinhos



Moda



Jóias

Serviços Financeiros

Redução de custos e ganho de eficiência



Remessas internacionais e bolsa de valores

Operação 24/7



Substituição ao Swift



Blockchain e LGPD

Incompatíveis?



Breve contexto da LGPD

Motivações

- Diversos casos de vazamento de dados
- Necessidade de adequação às tendências e requisitos do mercado internacional
- Inspiração no GDPR

Finalidade

- Proteção dos dados pessoais
- Retomada de controle dos dados pelos seus titulares
- Transparência em relação à utilização dos dados

Como compatibilizar?

Não existe uma única rede Blockchain

Processamento de dados pessoais e sensíveis “off-chain”

- Maior privacidade (transferências não são visíveis no Blockchain público)
- Baixo custo
- Velocidade

Uso de “side chains” (redes paralelas)

Criação de regras de governança quanto ao acesso



Regulação

Brasil e mundo

Brasil

Legislativo, Banco Central, Receita
Federal e CVM



Legislativo

- 02 Projetos em trâmite na Câmara dos Deputados
- 02 Projetos em trâmite no Senado
- Grande evolução desde o primeiro projeto em 2015
- Expectativa de legislação que favoreça o ambiente de negócios e desenvolvimento



Banco Central



- Comunicado 25.306/14 e 31.379/17
- Alertas sobre os riscos com operações de guarda e negociação de moedas virtuais
- Moedas virtuais não tem garantia de conversão para moeda oficial
- Operações que impliquem transferências internacionais devem observar as normas cambiais, em especial a realização de transações exclusivamente por meio de instituições autorizadas pelo Banco Central a operar no mercado de câmbio

Receita Federal

Regras para declaração e IN 1.888/19

Regras para declaração

- Devem ser declaradas na ficha Bens e Direitos como “outros bens”, podendo ser equiparadas a um ativo financeiro

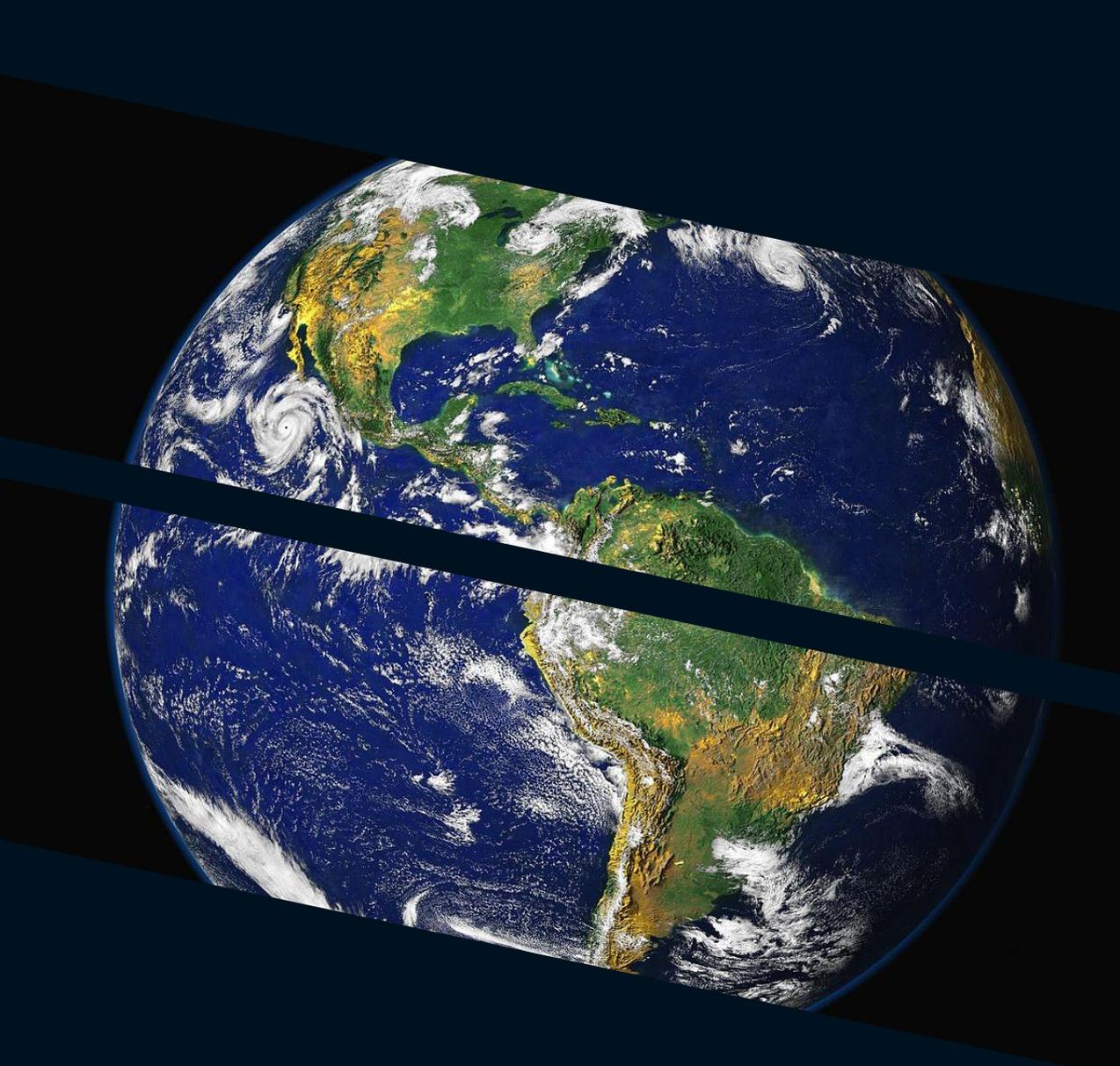
Instrução Normativa 1.888/19 e 1.889/19

- Instituiu a obrigatoriedade de prestação de informações relativas às operações com criptoativos
- Exchanges e pessoas físicas e jurídicas domiciliadas no Brasil devem prestar informações
- Sempre que valor mensal das operações superarem R\$ 30 mil
- Operações realizadas no exterior deverão ser informadas, independente do valor, exchanges nacionais farão as declarações no Brasil
- Ganho de capital incidente apenas em operações que superarem R\$35mil por mês, seguindo alíquota do IR ganho de capital



CVM

- Não se tratando de valor mobiliário não estará sob sua alçada
- Stop Order
- Sandbox regulatório



Cenário internacional

Corrida internacional

- Suíça
- Japão
- Estônia
- Malta
- Gibraltar
- Wyoming
- Delaware
- União Europeia

Pontos de atenção ao legislar sobre o tema

- Legislar sem acompanhar o cenário internacional poderá deixar o Brasil à margem dos avanços
- Proibição agravará o subdesenvolvimento
- Tecnologia é quem manda, se proibirmos, nos tornaremos exportadores de empreendedores
- Empreendedores estão buscando jurisdições mais favoráveis, pois Blockchain não tem fronteiras
- Permaneceremos exportadores de matéria prima, sujeitos aos países desenvolvidos e suas políticas econômicas



A Blockchain é uma rede de pessoas, que acreditam em um futuro melhor, em que as regras são iguais para todos, a informação é transparente, o poder é descentralizado e as boas ideias são facilmente executadas, financiadas e recompensadas



OBRIGADO



**Rodrigo Caldas de
Carvalho Borges**

E-mail
rborges@cbassociados.com.br

Website
www.cbassociados.com.br