THE DEVELOPER'S CONFERENCE

Riscos e Barreiras
Adoção de DLT/Blockchain

Suzana Maranhão Moreno
BNDES e ITU/ONU
https://www.linkedin.com/in/suzana-moreno/

Aplicações em diversos domínios

THE DEVELOPER'S CONFERENCE

Financeiro

TEL+TI

Saúde

Indústria

Horizontal

Entretenimento

Governo e Setor Público

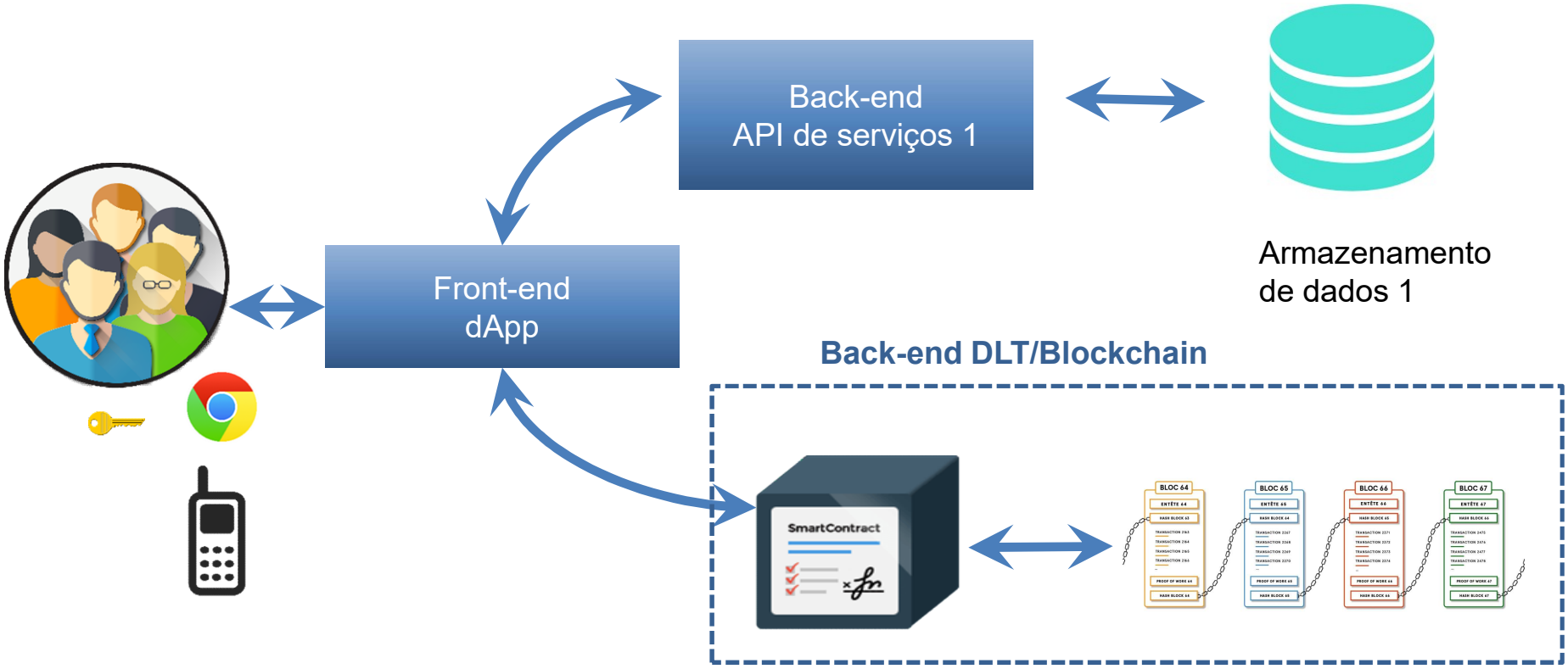
Agenda

THE DEVELOPER'S CONFERENCE

- Riscos de Execução de Projetos
- Barreiras para Adoção da Tecnologia
- Considerações Finais

Exemplo de Arquitetura com Blockchain

THE DEVELOPER'S CONFERENCE



Arquitetura para Análise de Riscos

THE DEVELOPER'S CONFERENCE

Riscos de Usuário e Conta

THE DEVELOPER'S CONFERENCE

O **Usuário**

- Interage com um dApp ou diretamente com o contrato inteligente a partir de sua conta
- Ou controla um nó da rede ou confia em um deles.

Gestão de chaves

Não conseguir enviar a uma transação

Erros de uso

Riscos de Governança/Ecossistema

THE DEVELOPER'S CONFERENCE

Governança/Ecossistema

- Estruturas e grupos decisórios sobre diversos aspectos da tecnologia, inclusive evolução
- Princípios

Falta de profissionais capacitados ou conhecimento

Falta de evolução da plataforma

Ocorrência de *forks* (decisão, bugs ou atualização de nós)

Riscos Econômicos

THE DEVELOPER'S CONFERENCE

Econômicos

- Parâmetros econômicos que influenciam no funcionamento e na segurança das plataformas

Variações imprevistas dos custos de uso da rede

Variações na remuneração dos produtores de blocos

Variação no valor dos criptoativos

Riscos Jurídicos

THE DEVELOPER'S CONFERENCE

Jurídicos

- Aspectos da legislação e da regulação que impactam nos negócios que utilizam a tecnologia ou no seu ecossistema

Inadequação da legislação ou sistema regulatório

Insegurança jurídica

Dificuldade de determinar jurisdição

Uso para fins não planejados

Arquitetura para Análise de Riscos

THE DEVELOPER'S CONFERENCE

dApps – Aplicações descentralizadas

THE DEVELOPER'S CONFERENCE

A Camada **dApps**

- A **aplicação** que faz uso do blockchain para armazenar informações e/ou de contratos inteligentes.
- Pode armazenar **informações** e **regras on-chain** e **off-chain**.
- Oferece ao usuário final da solução uma **melhor experiência de uso**.
- Simula operações de **edição e remoção** de dados na blokchain
- Análise de risco similar a de outros projetos de TI

Riscos das Regras de Negócios

THE DEVELOPER'S CONFERENCE

A Camada **Regras de Negócios On-chain (Contrato Inteligente)**

- Programa de computador que é executado para proposição/validação da mudança de estado
- Maior exposição a risco, pois pode ser implementado com ampla liberdade para lógica do negócio

Dificuldade de evolução do contrato (falha em projeto, codificação, mudanças)

Visibilidade do código para atacantes potenciais

Uso de dados externos

Contrato com desperdícios de recursos

Riscos da Plataforma (I)

THE DEVELOPER'S CONFERENCE

A Camada **Plataforma/Protocolo**

- Protocolo comum para que os estados da rede possam ser evoluídos em consenso entre os nós
- Pode suportar diferentes complexidades na sua mudança de estado

Centralização de poder do algoritmo de consenso

Baixa escalabilidade

Confirmação probabilística

Indisponibilidade ou inconsistência temporária (Teorema de CAP)

Riscos da Plataforma (II)

THE DEVELOPER'S CONFERENCE

A Camada **Plataforma/Protocolo**

- Protocolo comum para que os estados da rede possam ser evoluídos em consenso entre os nós
- Pode suportar diferentes complexidades na sua mudança de estado

Quebra de primitivas criptográficas e privacidade

Falhas do protocolo (implementação ou evolução)

Limitações variáveis (espaço, tempo exec etc)

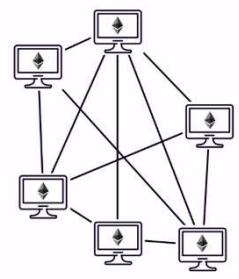
Imprevisibilidade de limitações para *Turing complete*

Riscos da Rede P2P

THE DEVELOPER'S CONFERENCE

A Camada **Peer-to-Peer**

- Cada nó pode transmitir mensagens de forma assíncrona para seus pares, descobrir seus pares, executar mecanismos de propagação de mensagens, sincronizar estado



Atrasos na retransmissão de dados

Ataques a nós especiais na rede

Segurança na comunicação com outros nós

Agenda

THE DEVELOPER'S CONFERENCE

- Riscos de Execução de Projetos
- Barreiras para Adoção da Tecnologia
- Considerações Finais

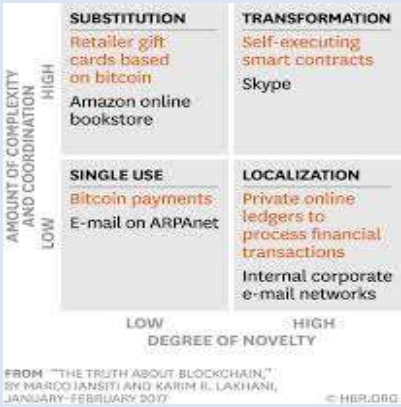
Intrínsecas

THE DEVELOPER'S CONFERENCE

- Dificuldade de construção de rede
- Imutabilidade do código
- Dificuldade de evolução de plataformas
- Novos ataques

Coordenação x Novidade

https://hbr.org/2017/01/the-truth-about-blockchain

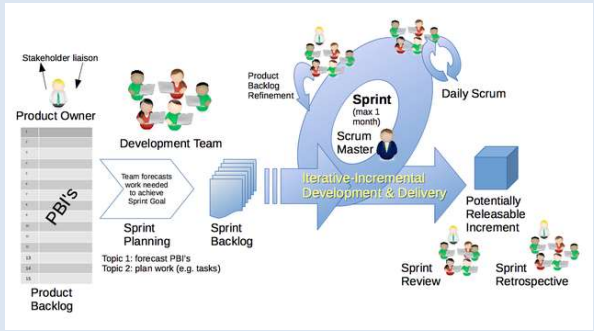


ERP x Permissionadas

Intrínsecas

THE DEVELOPER'S CONFERENCE

- Dificuldade de construção de rede
- Imutabilidade do código
- Dificuldade de evolução de plataformas
- Novos ataques



Desenvolvimento ágil x Desenvolvimento para contratos inteligentes

Intrínsecas

THE DEVELOPER'S CONFERENCE

- Dificuldade de construção de rede
- Imutabilidade do código
- Dificuldade de evolução de plataformas
- Novos ataques

→

Risco de atualização de plataformas
(> não permissionadas)

Coordenação

Trilema, Privacidade, Bugs

Intrínsecas

- Dificuldade de construção de rede
- Imutabilidade do código
- Dificuldade de evolução de plataformas
- Novos ataques

→

Nova infra de tecnologia + incentivos => Novos ataques

Ataque de maioria

Nothing-at-stake

Selfish Mining

Sybil attack

Eclipse

Conluio político

Demanda entendimento e mitigação

Cultural + Conhecimento

THE DEVELOPER'S CONFERENCE

Má Reputação
Hacks, ICOs, Crimes, Ataques

Falta de clareza de benefícios

Dificuldade de avaliar opções de plataformas

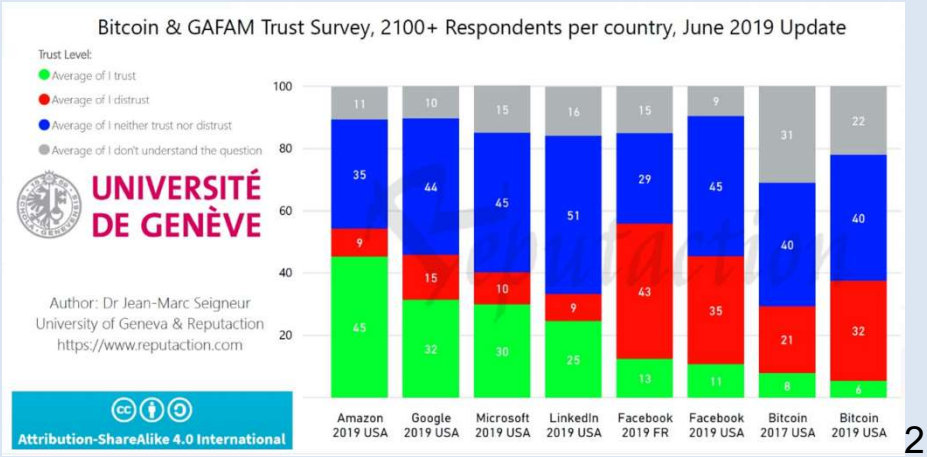
Falta de experiência para desenvolver e governar projetos

"Blockchain, by its very definition, should engender trust. But in reality, companies confront trust issues at nearly every turn. For one, users must build confidence in the technology itself"

PwC's 2018 Global Blockchain Survey

DLT x Cripto x Blockchain

Risco econômico de criptomoedas



Cultural + Conhecimento

THE DEVELOPER'S CONFERENCE

- Má Reputação
  Hacks, ICOs, Crimes, Ataques
- Falta de clareza de benefícios
- Dificuldade de avaliar opções de plataformas
- Falta de experiência para desenvolver e governar projetos

→

Poucos cases de sucesso com resultados de produção

Baixo nível de conhecimento

ROI incerto

Cultural + Conhecimento

THE DEVELOPER'S CONFERENCE

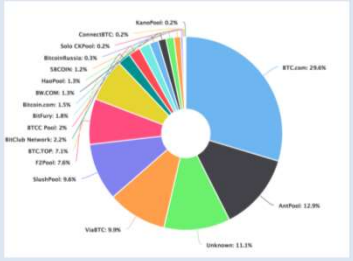
- Má Reputação
  Hacks, ICOs, Crimes, Ataques
- Falta de clareza de benefícios
- Dificuldade de avaliar opções de plataformas
- Falta de experiência para desenvolver e governar projetos

→

Aberta x Permissionada
Pública x Privada

Análise da Descentralização

Bitcoin



"Ilhas de Nomenclatura"

Cultural + Conhecimento

THE DEVELOPER'S CONFERENCE

- Má Reputação
  Hacks, ICOs, Crimes, Ataques
- Falta de clareza de benefícios
- Dificuldade de avaliar opções de plataformas
- Falta de experiência para desenvolver e governar projetos

→

Múltiplos perfis

desenvolvedores, economistas, gestores, contadores, advogados, usuários

Educar usuários

Credibilidade de Fornecedores

Governança de rede x projeto

Ecossistema

THE DEVELOPER'S CONFERENCE

Poder do Intermediário

Infraestrutura tecnológica já existente

Pouca infraestrutura e ecossistema com falhas

Ausência de plataforma dominante

Como preservar seu posicionamento?

Hostilidade política/econômica

Ecossistema

THE DEVELOPER'S CONFERENCE

Poder do Intermediário

Infraestrutura tecnológica já existente

Pouca infraestrutura e ecossistema com falhas

Ausência de plataforma dominante

→

Investimento das empresas na infra-estrutura atual

Tecnologias alternativas

Ecossistema

THE DEVELOPER'S CONFERENCE

- Poder do Intermediário
- Infraestrutura tecnológica já existente
- Pouca infraestrutura e ecossistema com falhas
- Ausência de plataforma dominante

→

Baixo suporte em aplicações / celulares

Identidade digital, link com moeda nacional, Exchange centralizadas

Geopolítica de Validadores

Testes e melhorias em plataformas

Ecossistema

THE DEVELOPER'S CONFERENCE

- Poder do Intermediário
- Infraestrutura tecnológica já existente
- Pouca infraestrutura e ecossistema com falhas
- Ausência de plataforma dominante

→

Diversidade de plataformas de mercado

Baixa interoperabilidade – Ilhas de comunidades

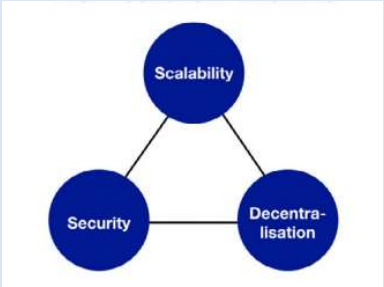
Tecnologia

THE DEVELOPER'S CONFERENCE

Dificuldades técnicas no uso de em uma plataforma

Dificuldade de interoperabilidade

Experiência do usuário



Trilema da Escalabilidade

Armazenamento de dados Descentralizado x DLT

Custo Energético POW + menor maturidade de outros protocolos

Tecnologia

THE DEVELOPER'S CONFERENCE

- Dificuldades técnicas no uso de em uma plataforma
- Dificuldade de interoperabilidade
- Experiência do usuário

→

Troca de valor ou informação

Transações distribuídas

Portabilidade de aplicações ou de infraestrutura

Tecnologia

THE DEVELOPER'S CONFERENCE

- Dificuldades técnicas no uso de em uma plataforma
- Dificuldade de interoperabilidade
- Experiência do usuário

→

Usabilidade de aplicações

Diferenças entre plataformas

Legais

Leis/Regulação →

Legislação sobre tokens, validade de registros, LGPD

Incerteza regulatória

Múltiplas jurisdições

“Crypto hubs”

Agenda

THE DEVELOPER'S CONFERENCE

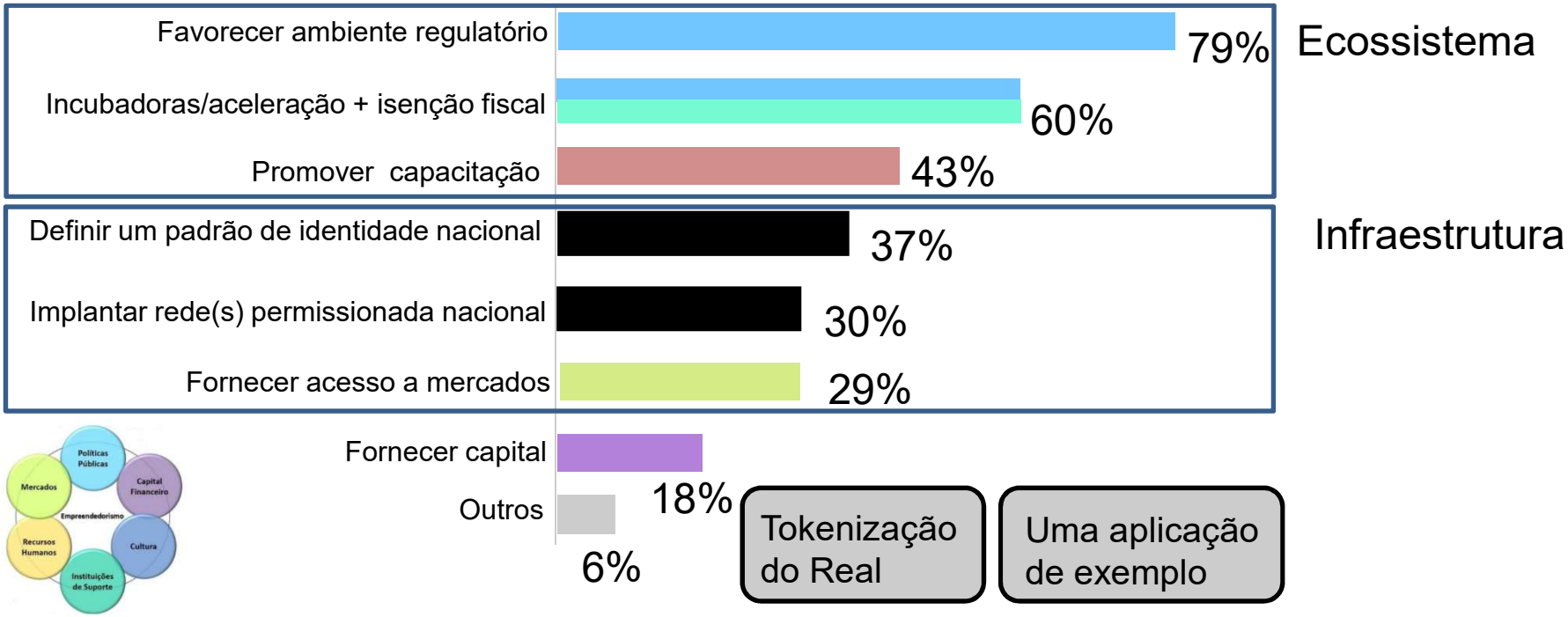
- Riscos de Execução de Projetos
- Barreiras para Adoção da Tecnologia
- Considerações Finais

Ações para Governo

https://www.bndes.gov.br/blockchaingov

THE DEVELOPER'S CONFERENCE

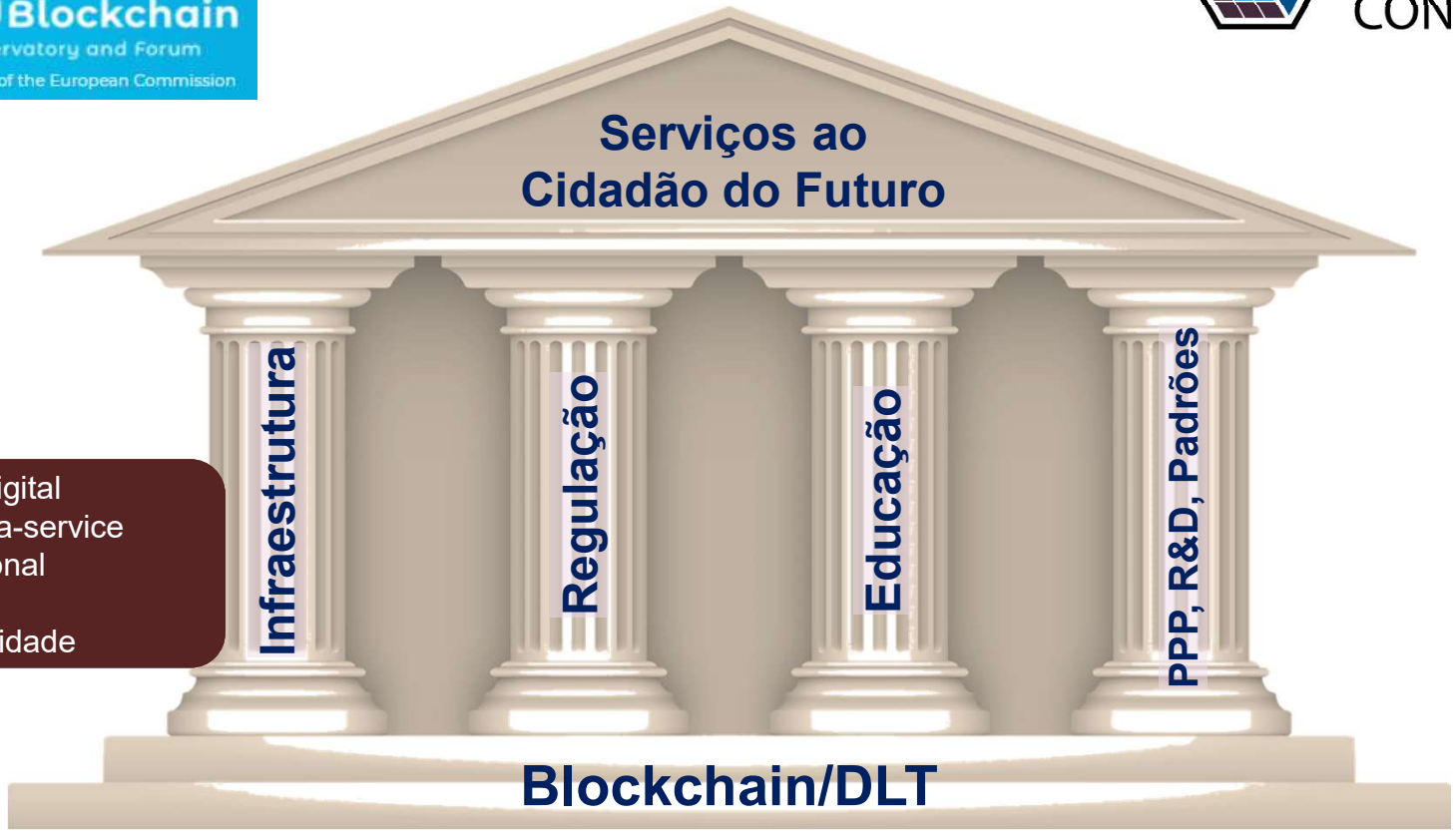
Quais as 3 melhores ações que o governo poderia fazer para ajudar o desenvolvimento do ecossistema Brasileiro?



Habilitadores de Blockchain

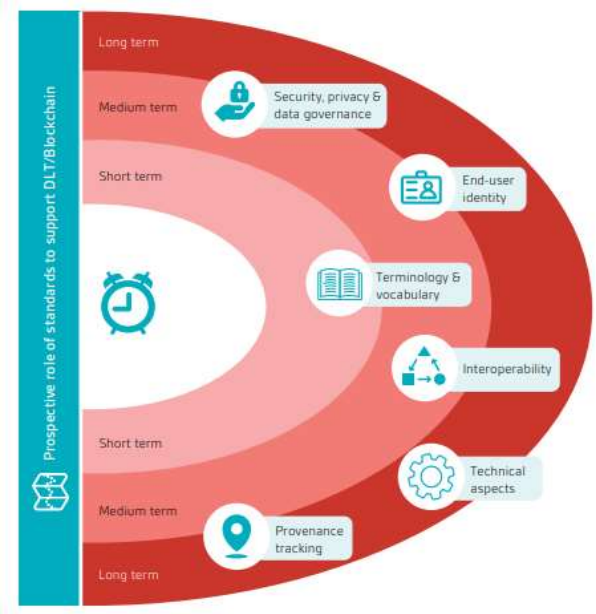
EU Blockchain Observatory and Forum
An initiative of the European Commission

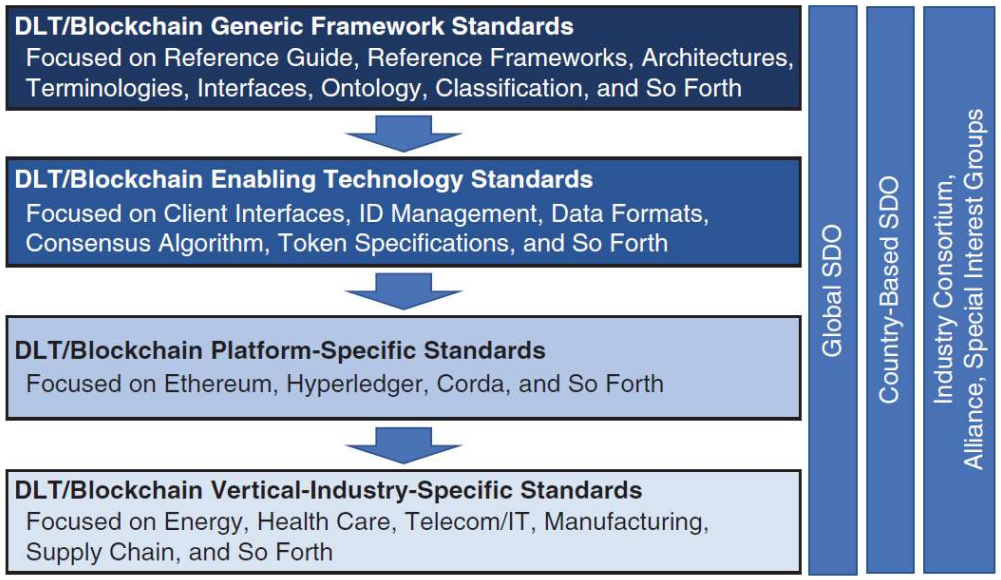
THE DEVELOPER'S CONFERENCE



- Identidade digital
- Platform-as-a-service
- Moeda nacional tokenizada
- Interoperabilidade

Padronização





https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf

https://www.researchgate.net/publication/330642079_Developing_Open_and_Interoperable_DLTBlockchain_Standards_Standards

Focus Group on Application of DLT

https://itu.int/en/ITU-T/focusgroups/dlt

THE DEVELOPER'S CONFERENCE

Objetivos

- Grupo de estudos;
- Definir propostas de padronização.

Outros grupos: Moedas digitais, Cidades inteligentes, Inclusão financeira, IOT

WG1: State of the Art: Ecosystem, Terms, Definitions, Concepts

WG2: Applications & Services

WG3: Technology Reference Framework

WG4: Policy Reference Framework

WG5: Standardization Roadmap

Geneva Oct 2017 | Bern Feb 2018 | Geneva May 2018 | Beijing Oct 2018 | Rio de Jan Jan 2019 | Madrid Apr 2019 | Geneva Jul 2019

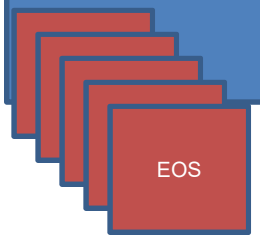
350+ inscritos de 55+ países

Comparação de Plataformas

THE DEVELOPER'S CONFERENCE

Arquitetura de referência DLT

Template de mapeamento de plataformas existentes

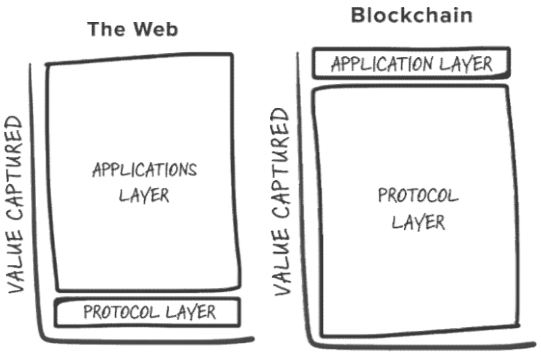


Critérios de avaliação para decisão de DLT

Sim! A tecnologia tem MUITO potencial

THE DEVELOPER'S CONFERENCE

- Blockchain (2008)
- SSL 3.0 (1996)
- HTTP/HTML (1990)
- TCP/IP (1970's)
- Ethernet (1970's)



"Far from merely tweeting, or taking and sharing photos or videos, blockchain enables an entirely new economic structure."

https://www.hbs.edu/faculty/Pages/item.aspx?num=52100

https://www.usv.com/blog/fat-protocols

https://unchronicle.un.org/article/blockchain-and-sustainable-growth

THE DEVELOPER'S CONFERENCE

Suzana Maranhão Moreno
BNDES e ITU/ONU
https://www.linkedin.com/in/suzana-moreno/