REDE BLOCKCHAIN BRASIL

ATA 024 DE REUNIÃO DO COMITÊ EXECUTIVO

Às 11 horas do dia 12 de setembro de 2024, na plataforma Teams, reuniram-se os representantes dos Partícipes da Rede *Blockchain* Brasil – RBB, conforme lista de presentes abaixo, para discussão e deliberação sobre os assuntos tratados na Ordem do Dia a seguir, com a apresentação de apoio para reunião no Anexo 1.

Ordem do dia

Observadas as cláusulas do Acordo de Cooperação n° D-121.2.0014.22, celebrado entre os Partícipes para a criação e manutenção da RBB, e sem prejuízo do que vier a dispor o Regulamento da RBB:

1. Pedidos de adesão
    - SGD
    - IBICT
2. Relato de conversa com a FGV
3. Apresentação Starlight / EY
4. Governança de aplicações

RELATO

Abertura da reunião
O Sr. Gladstone Arantes (BNDES) abriu a reunião, apresentando a Ordem do Dia e passou a palavra para o Sr. Milber Bourguignon (BNDES).

1. Pedidos de adesão

SGD
O Sr. Milber apresentou a reunião realizada com a Secretaria de Governo Digital (SGD), que foi uma conversa de alinhamento prévio para que pudessem internalizar o processo de adesão. Sr. Gladstone complementou destacando a importância da integração para a identidade digital e a possibilidade de uso do domínio Gov.BR na RBB. O Sr. Reynaldo Formigoni (CPQD) destacou a colaboração com a SGD em projetos de identidade digital, ressaltando a continuidade e o interesse em usar a RBB para aplicações futuras. As considerações dos participantes foram na linha de que é necessário que os membros associados já tenham, no planejamento junto à RBB, a intenção de subir seus nós.

IBICT
Sr. Milber e Sr. Gladstone comentaram sobre o pedido de adesão realizado pelo IBICT – Instituto Brasileiro de Informação em Ciência e Tecnologia, um órgão nacional de informação, unidade de pesquisa do Ministério da Ciência, Tecnologia e Inovação (MCTI). O pedido de adesão chegou por e-mail, sem um alinhamento prévio com os membros da RBB, salvo conversas com o Leandro Ciuffo (RNP) e rápida interação durante o evento realizado no TCU. Na reunião, foram explicados a governança e os recursos necessários para as duas formas de adesão.

Os representantes do IBICT destacaram já possuir um caso de uso em desenvolvimento, relativo a indexadores de publicações acadêmicas brasileiras. Também afirmaram que a RBB poderia ser uma plataforma para o funcionamento da aplicação.

2. Relato de conversa com a FGV

Sr. Milber e apresentou a reunião feita com o Grupo de Pesquisa sobre o Impacto da Tecnologia nas Relações Jurídicas, Sociais e Econômicas da Fundação Getulio Vargas (GITEC/ FGV). O grupo pode oferecer pesquisa e produção de conhecimento, enquanto a RBB pode oferecer objeto desses estudos. Poder-se-ia também, desenvolver um estudo em conjunto para o modelo jurídico da rede para após ACT.

Foi deliberado que, em nome do Comitê Executivo, o BNDES vai mandar um e-mail citando a reunião, a possibilidade de trabalho conjunto e sugerindo que a entrada na rede para formalizar a cooperação pode ser um bom caminho para facilitar as atividades conjuntas.

3. Apresentação Starlight / EY

Jeff Prates e Thamilla Tallarico, representantes da Ernest Young, falaram sobre a Starlight, conforme a apresentação no Anexo 2, destacando sua eficácia em prover privacidade em transações blockchain e sua compatibilidade com a RBB sem a necessidade de criar uma rede secundária.

Tecnologia ZKP: A tecnologia de prova de conhecimento zero (ZKP) utilizada pelo Starlight permite a verificação da veracidade das informações sem expor os dados, mantendo a privacidade e a confiança na rede.

Potencial de Aplicação: Jeff sugeriu um caso de uso para a tecnologia Starlight na RBB, relacionado à verificação de identidade sem expor dados pessoais, demonstrando o potencial da ferramenta para aplicações práticas e seguras.

4. Governança de aplicações

Gladstone fez a apresentação (Anexo 1) com sugestões de possíveis alterações ao regulamento. Gladstone apresentou, rapidamente, as sugestões e sugeriu que o debate ficasse para a próxima reunião. Também sugeriu que, nesta mesma data, fossem realizadas as votações de alinhamento das sugestões propostas.

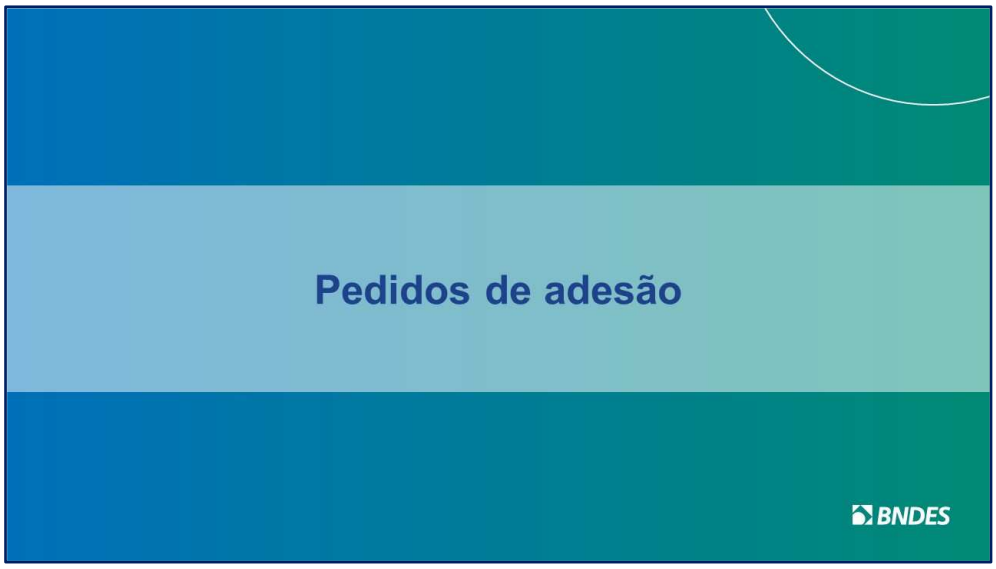
MEMBROS PRESENTES		
COM DIREITO A VOTO		
BNDES	Luciana Giuliani de Oliveira Reis	Gladstone Moisés Arantes
TCU	Rainério Rodrigues Leite	Eldon Teixeira Coutinho
CPQD	Reynaldo Formigoni	
DATAPREV	Claudemir Custódio Brum	
SERPRO	Marco Tulio da Silva Lima	Jetro Paulo Weber
SEM DIREITO A VOTO		
Pref. Araguaína	Igor Thawan	Sérgio Maia Rabelo

CONVIDADOS	
BNDES	Milber Fernandes M. Bourguignon
PUC-Rio	Paulo Henrique Alves

ANEXO 1 – Apresentação da reunião (BNDES)

Ordem do Dia

1. Pedidos de adesão
   - SGD
   - IBICT
2. Relato de conversa com a FGV
3. Apresentação Starlight / EY
4. Governança de aplicações



Pedidos de Adesão

1. SGD

- Reunião em 10/09/2024
- Mudança de equipe interna que vai conduzir a adesão
  - Diretoria de Identidade Digital
- Possibilidade de diversas integrações SGB-RBB, especialmente no que se refere à identidade
- Alinhamento para disponibilização de domínio gov.br para a RBB

Pedidos de Adesão

2. IBICT - Instituto Brasileiro de Informação em Ciência e Tecnologia

- Reunião em 11/09/2024
- Administração direta
- Entidade vinculada ao MCTI com personalidade própria
- Já possuem aplicação em blockchain em rede própria
  - Identificador para publicações brasileiras
- Preferência por entrada como associado

O Ibict

Missão

Promover a competência, o desenvolvimento de recursos e a infraestrutura de informação em ciência e tecnologia para a produção, socialização e integração do conhecimento científico-tecnológico

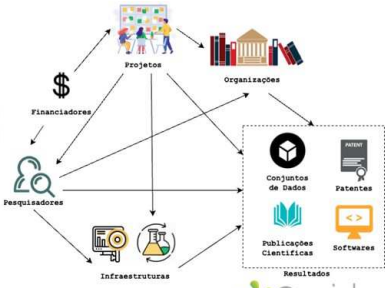
Unidade de pesquisa, vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI)

Vanguarda da Ciência da Informação no Brasil

BrCris - Ecossistema de Informação da Pesquisa Científica Brasileira

Mapeando e organizando os dados sobre a pesquisa científica brasileira: plataforma agregadora que permite recuperar, certificar e visualizar dados e informações relativas aos diversos atores que atuam na pesquisa científica do contexto brasileiro

BrCris
Ecossistema de Informação da Pesquisa Científica Brasileira
brcris.ibict.br



Oasisbr
oasisbr.ibict.br

Instituto Brasileiro de Informação em Ciência e Tecnologia
Maio/2024

ibict
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

A Importância dos Identificadores Persistentes

1. **Citação e Referência**
   Os IPs permitem que artigos e outros recursos sejam citados de forma precisa, garantindo o reconhecimento dos autores e a integridade das referências bibliográficas.

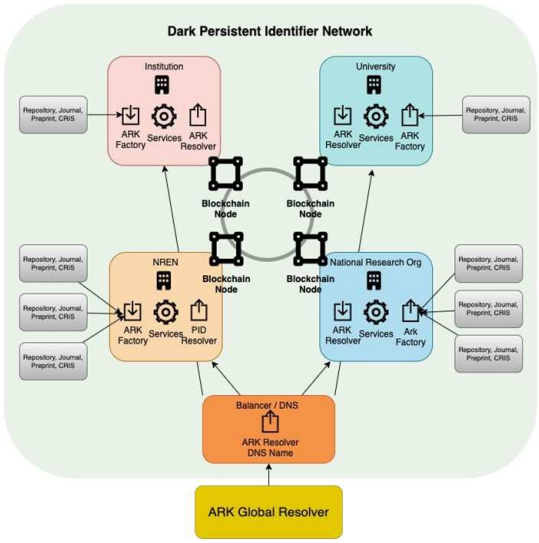
2. **Descoberta e Acesso**
   Através dos IPs, os objetos digitais podem ser localizados e acessados de forma confiável, facilitando a descoberta e o uso de informações científicas.

3. **Preservação a Longo Prazo**
   Os IPs ajudam a garantir a preservação digital de longo prazo, mesmo com a evolução de tecnologias e plataformas.

O padrão ARK: Archival Resource Key

O padrão Archival Resource Key (ARK) é um identificador persistente desenvolvido pela Biblioteca Nacional da França para atribuir IDs únicos a objetos digitais, incluindo publicações científicas, conjuntos de dados, software e outros recursos.

O ARK é uma alternativa descentralizada aos esquemas de identificação mais conhecidos, como o DOI (Digital Object Identifier), oferecendo uma abordagem mais flexível e acessível para a atribuição de IDs persistentes.



A rede de identificação persistente dARK

Conversa com a FGV

BNDES

Conversa com a FGV - GITEC

- Realizada em 03/09/2024
- Apresentação do GITEC
- GITEC/FGV: Grupo de Pesquisa sobre o Impacto da Tecnologia nas Relações Jurídicas, Sociais e Econômicas
- Rápida atualização sobre a RBB
- Avaliação de sinergias e pauta conjunta
  - Pesquisa sobre LGPD e temas correlatos
  - Capacidade de produção de pesquisa aplicada
  - Possibilidade de produção de relatórios/ registros formais de conhecimento
  - Possibilidade de estudarem modelo jurídico para além do ACT que rege a RBB
- Avaliar convite para ter uma formalização da relação do grupo com a FGV – partícipe parceiro

Apresentação Starlight / EY

BNDES

Governança de aplicações

BNDES

“Formulário” Partícipe

- Descrição breve do funcionamento da aplicação.
- Interesse público da aplicação.
  - É parte de serviço ou processo interno de alguma instituição pública?
  - É parte do processo interno de algum partícipe?
  - É parte de algum serviço ou processo interno que possa ser considerado de interesse público?
- LGPD - Garantias de não registrar dados pessoais na blockchain.
  - Se envolve informações de pessoas físicas, as técnicas de hashing são suficientes para garantir a anonimidade?

“Formulário” Partícipe

- Natureza dos usuários.
  - Que usuários enviam transações (PF, PJ, partícipes, outros SCs)?
  - Qual a natureza dessas transações (backend, frontend)?
- Criticidade da aplicação.
  - Pode rodar em regime piloto (sem SLA de disponibilidade)?
  - Quais as consequências em caso de indisponibilidade?
  - Quais as consequências em caso de reset da rede durante o piloto?
  - Há previsão de quando será necessário ir além de um piloto?
- SCs permitem reuso por outros partícipes? Como?

Regulamento

6.3. Os **CONTRATOS INTELIGENTES** deverão ser aprovados pelo **COMITÊ EXECUTIVO** antes de sua implantação.

6.3.1. Um **PARTÍCIPE** da **RBB** deverá submeter Proposta de Implantação para o Comitê descrevendo os casos de uso que serão suportados pelos **CONTRATOS INTELIGENTES**.

6.3.2. A Proposta de Implantação deve demonstrar o enquadramento dos **CONTRATOS INTELIGENTES** e seus respectivos **CASOS DE USO**, processos suportados e entidades executoras destes processos em um dos critérios definidos no item 6.2 deste Regulamento, assim como o contexto de negócio, os tipos de usuários finais que irão gerar as transações e as informações que serão armazenadas na **RBB**.

6.3.2.1. No caso de uso de natureza mais genérica, com possibilidade de aplicação em vários contextos diferentes, o **COMITÊ EXECUTIVO** pode solicitar garantias técnicas ou compromissos (inclusive por escrito) de que o uso efetivo se dará apenas dentro dos contextos permitidos.

Regulamento

6.3.3. O **PARTÍCIPE INTERESSADO** será responsabilizado, técnica e juridicamente, perante quaisquer irregularidades cometidas na execução dos **CONTRATOS INTELIGENTES** ou no envio das transações, estando sujeito às penalidades previstas na legislação vigente, incluindo as advindas da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), além das previstas no item 7.

6.3.4. No caso de descumprimento das condições estabelecidas na Proposta de Implantação, o **PARTÍCIPE** interessado pode ser solicitado a bloquear temporária ou definitivamente a DApp (aplicação descentralizada), os **CONTRATOS INTELIGENTES**, os usuários ou mesmo sua infraestrutura da rede, de tal forma a evitar o uso indevido da **RBB**.

6.3.4.1. A reincidência no descumprimento das condições estabelecidas na Proposta de Implantação pode resultar em exclusão do **PARTÍCIPE** do **ACORDO** e, por conseguinte, da **RBB**, mediante votação do **COMITÊ EXECUTIVO**, nos termos da Cláusula Segunda, Parágrafo Segundo, Inciso II do **ACORDO**, e do item 7 deste Regulamento.

Regulamento

6.3.3. O **PARTÍCIPE INTERESSADO** será responsabilizado, técnica e juridicamente, perante quaisquer irregularidades cometidas na execução dos **CONTRATOS INTELIGENTES** ou no envio das transações, estando sujeito às penalidades previstas na legislação vigente, incluindo as advindas da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), além das previstas no item 7.

- Proposta
  - 6.3.3.1. No caso de CONTRATOS INTELIGENTES disponíveis ao uso por mais de um PARTÍCIPE, a responsabilização será devida apenas ao proprietário da chave privada que assinou a transação que tenha gerado a execução irregular.

Em Desenvolvimento

- Procedimento para propostas de aplicações por entidades fora do Acordo.
  - Possibilidade de adesão.
  - Encaminhamento para Partícipe.
    - Parceria, fornecimento de serviço etc.
  - Como tratar soluções open source?
- Acolher sem sobrecarregar nenhum partícipe.
  - Filtro básico *a priori* para casos em que não há potencial de adesão.
    - Solicitação de formulário e/ou vídeo de apresentação.
  - Apresentação preliminar no Comitê Técnico.
  - Apresentação posterior no Comitê Executivo.

Obrigado

rbb@bndes.gov.br

BNDES

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Portal BNDES
www.bndes.gov.br

Atendimento Empresarial
0800 702 6337
Chamadas internacionais
+55 21 2172 6337

Ouvidoria
0800 702 6307
www.bndes.gov.br/ouvidoria

Fale Conosco
www.bndes.gov.br/faleconosco

facebook.com/bndes.imprensa

twitter.com/bndes

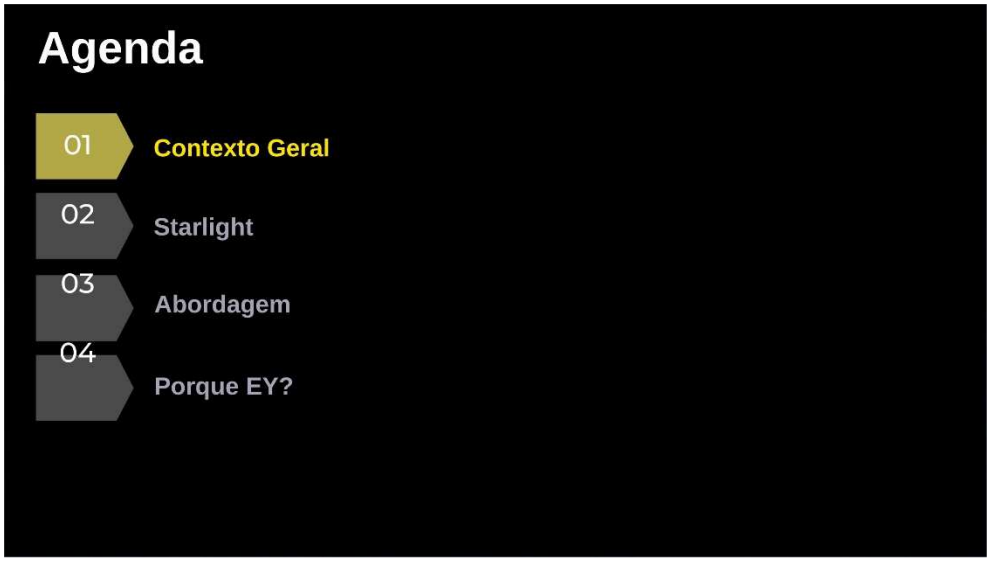
youtube.com/bndesgovbr

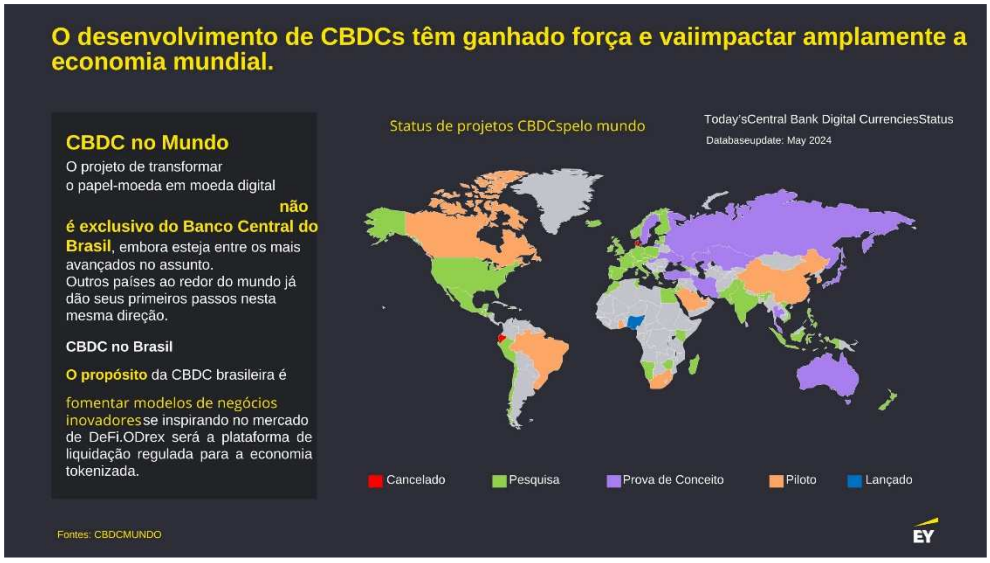
linkedin.com/company/bndes

Instagram.com/bndesgovbr

Anexo 2 – Apresentações da EY

Thamilla





Evolução e Marcos do Drexno Brasil: Panorama ao Longo dos Anos

Privacidade foi o foco da Fase 1 do Piloto Drex e continuará sendo investigada na Fase 2, que se iniciou em setembro de 2024

São 16 os consorcios participantes do Piloto Drex escolhidos pelo BACEN (totalizando quase 70 instituições):

Fontes: CBDCMUNDO

EY

Agenda

01 Contexto Geral

02 **Starlight**

03 Abordagem

04 Porque EY?

Caso de Uso

Starlight: solução open sourcede privacidade da EY

Foi selecionada pelo Banco Central para ser testada no âmbito do projeto-piloto do Drex, a moeda digital brasileira. A ferramenta utiliza o protocolo ZKP (zero-knowledgeproof)que corresponde a uma tecnologia criptográfica de comprovação da veracidade de uma informação sem que ela seja totalmente revelada para os envolvidos em uma transação

OStarlight foi selecionadopelo Banco Central do Brasil para ser testadocomo parte do projeto piloto Drex, a moeda digital brasileira.

Fonte: TIINSIDE

Fonte: BLOCKNEWS

Fonte: CBDC

Fonte: https://www.ey.com/pt_br/agencia-ey/noticias/drex-saiba-como-sera-feita-operacao-venda-titulo-publico-tokenizado

Com o Starlight, diferente de outras ferramentas testadas no Drex, a privacidade não depende da construção de redes adicionais a partir da plataforma principal (transparente).

Destaques

Construção de privacidade nos contratos inteligentes.
A Starlight constrói a privacidade diretamente nos contratos inteligentes usando técnicas criptográficas avançadas. Isso permite que a privacidade seja gerenciada de forma integrada no protocolo, **sem a necessidade de criar novas redes ou soluções externas.**

Uso de Zero KnowledgeProofs (ZKPs)
A Starlight utiliza provas de conhecimento zero (ZKPs) para **garantir a privacidade das transações**, permitindo que as partes demonstrem o conhecimento de certos dados sem revelá-los

Customização

A Starlightdemonstrou flexibilidade ao ser adaptada para atender às necessidades específicas do DREX, mostrando capacidade de evolução contínua.

Ao contrário de outras soluções de mercado o Starlight está **pronta para uso**em estágio avançado de homologação pelo Banco Central.

Fontes: Starlight

Starlight é a solução de privacidade de código aberto criada pela EY e oferece **nível de privacidade máxima** com protocolos criptográficos avançados e funções Hash Seguras

"A solução utiliza o chamado privacy pools, uma carteira digital inteligente que realiza todas as ações das operações no mercado atacadista e que está na plataforma Drex, controlada pelo Banco Central."

Uma solução que pode ser utilizada por todos e capaz de criar suas próprias estruturas. É de domínio público, segura e compatível com outros canais de distribuição

1. **Gerencia lógica complexa:**consegue entender e transformar instruções complicadas em código que funciona de maneira prática. Consegue lidar com diferentes tipos de informações e estruturas de dados (como listas e tabelas) de forma eficiente e organizada.
2. Cria sistema seguro: utiliza códigos especiais, semelhantes a uma "impressão digital"para suas informações, tornando-as inacessíveis para qualquer pessoa não autorizada. Isso garante total privacidade e segurança. Além disso, emprega métodos criptográficos amplamente utilizados e confiáveis.
3. **Facilidade de Uso:** Ao compilar uma aplicação com Starlight, você recebe um pacote completo que inclui testes, pontos de acesso para APIs e scripts prontos para uso, facilitando a implementação e operação.

Fontes: Análise EY

Desafios encontrados na implementação independente de soluções de privacidade pelas Instituições Financeiras

Desafios na implementação independente

Custo

O desenvolvimento interno de uma solução de privacidade implica um **investimento financeiro substancial**. Além disso, o custo inicial pode ser apenas o começo, já que manter e atualizar a solução ao longo do tempo também representa um gasto contínuo.

Tempo

Criar uma solução internamente envolve um **longo período de desenvolvimento e teste**. Isso pode resultar em atrasos significativos no lançamento no mercado, especialmente se houver problemas técnicos ou requisitos regulatórios que precisem ser atendidos.

Mão de obra qualificada

Desenvolver uma solução de privacidade requer **expertise técnica especializada** Contratar e manter uma equipe qualificada pode ser desafiador e custoso, especialmente porque profissionais com esse conhecimento são altamente requisitados

Fontes: Análise EY

EY

Agenda

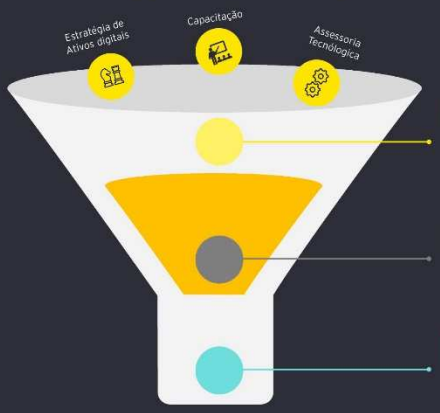
01 Contexto Geral

02 Starlight

03 **Abordagem**

04 Porque EY?

As oportunidades para atender o mercado financeiro podem ser tangibilizadas em três etapas de valor complementares



1. Assessment

Avaliação da prontidãotecnologicada Instituição Financeirae do atendimentoaosrequisitos mínimosde hardware e software

2. Piloto

Teste do Starlight em ambiente controlado dentro da Instituição financeira

3. Expansão

Implementar o Starlight, para tanto, capacitar os colaboradores que irão trabalhar com a ferramenta

EY

Agenda

01 Contexto Geral

02 Starlight

03 Abordagem

04 **Porque EY?**

A EY oferece o nível adequado de suporte por meio de diferentes capacidades para navegar adequadamente pelo ecossistema de blockchain e ativos digitais

O que torna a EY única e diferenciada?

A **EY é uma fornecedora líder** de serviços de risco de ativos digitais.Atualmente apoia as maiores exchanges e custodiantes na avaliação de suas arquiteturas de **blockchain.**

O mercado global de gestão de ativos digitais cresceu rapidamentedesde sua criação. O tamanho do mercado de criptomoedas está projetado para aumentar em USD 34,5 bilhões com um CAGR de 16,64% entre 2023 e 2028*.

Mais de cinco anos de experiência na execução de protocolos focados em tecnologia e garantia, além de revisões de ativos digitais.

20+ of the largest digital asset firms supported

1,500+ Blockchain specialists across the globe

35+ digital asset & token reviews conducted

30+ blockchain network protocols reviewed

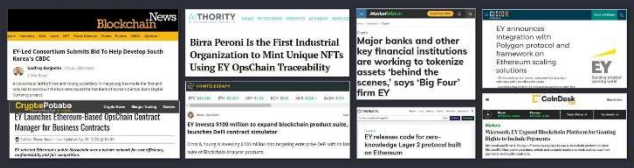
Fonte: blockchain.ey.com

O compromisso da EY com as soluções de ativos digitais e blockchain

Temos uma equipe dedicada de engenheiros, criptógrafos, matemáticos, consultores de segurança, estrategistas, além de consultores em questões de riscos, regulamentação, conformidade, impostos, auditoria, finanças, operações e tecnologia.

1.500+
Especialistas e engenheiros em ativos digitais e blockchain em todo o mundo

- Sobre 1,000 — Compromissos com clientes entregues em todo o mundo
- Estratégiade ativos digitais
- Desenvolvimentode aplicações empresariais
- Infraestruturade nós interna
- Ferramentas de contratos inteligentes e testes
- Membrosda Micr osoft /S AP
- Apresentou 17 patentes em criptografia e design de soluções



Somos líderes da indústria em blockchain, dobrando nossa escala com um investimento de 100 milhões de dólares em blockchain.

Fonte: HFS HorizonsReport PublicBlockchain Services, 2023

EY

Nossa inteligência de negócios líder examina os impactos do blockchain em diferentes setorese indústriasserviços e produtos

Starlight
How are you using blockchain to re-imagine your industry?

Smart Contract & Token Review
How can blockchain innovation gain confidence and improve quality?

EY OpsChainTraceability
How can blockchain technology transform your supply chain network?

OpsChainContract Manager
How can you revolutionize your contract management and put your business on autopilot?

OpsChainESG
How can we close the gap between ambition and action in decarbonization?

EY

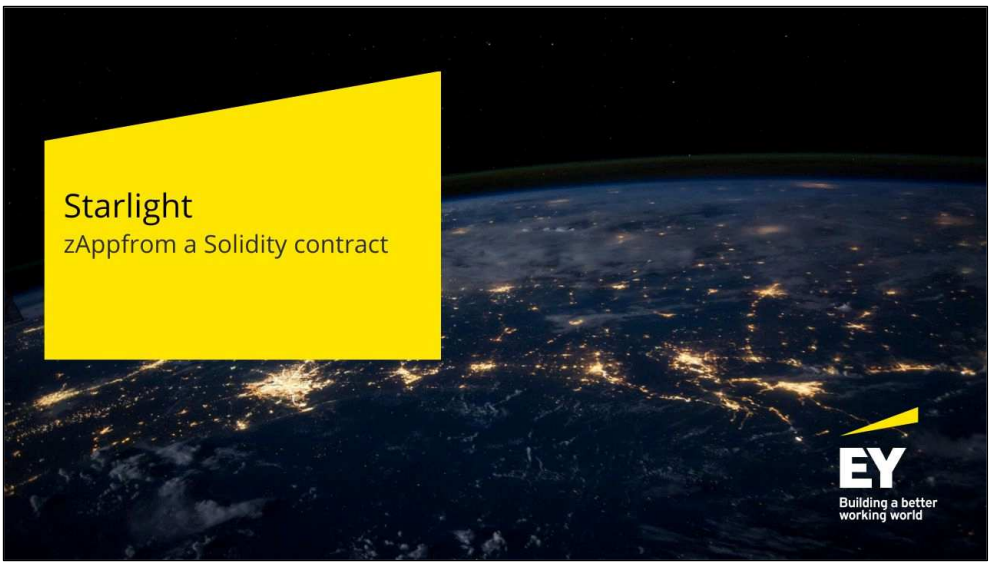
Thamilla Talarico
Sócia, Business Consulting, Líder em Ativos Digitais & Blockchain, EY
Brasil
LinkedIn

Jefferson Prestes
Especialista em Tokenizaçãoe Blockchain
LinkedIn

Muiittoo Obriigado!

EY
Building a better working world

Jeff



ZKP (Zero-Knowledge Proof)

A cryptographictechnique invented at the MITin 1985:

THE KNOWLEDGE COMPLEXITY OF INTERACTIVE PROOF SYSTEMS*

SHAFI GOLDWASSER†, SILVIO MICALI‡, AND CHARLES RACKOFF§

Abstract. Usually, a proof of a theorem contains more knowledge than the mere fact that the theorem is true. For instance, to prove that a graph is Hamiltonian it suffices to exhibit a Hamiltonian tour in it; however, this seems to contain more knowledge than the single bit Hamiltonian/non-Hamiltonian.

In this paper a computational complexity theory of the "knowledge" contained in a proof is developed. Zero-knowledge proofs are defined as those proofs that convey no additional knowledge other than the correctness of the proposition in question. Examples of zero-knowledge proof systems are given for the languages of quadratic residuosity and quadratic nonresiduosity. These are the first examples of zero-knowledge proofs for languages not known to be efficiently recognizable.

Key words. cryptography, zero knowledge, interactive proofs, quadratic residues

AMS(MOS) subject classifications. 68Q15, 94A60

https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf

ZKP (Zero-Knowledge Proof)

Cryptographic techniques that allow one party (the Prover) to prove to another party (the Verifier) that they possess certain information or knowledge without revealing what that information is.

Completeness
- If something is true, we CAN prove it and convince a Verifier it is true.

Soundness
- If something is false, we CANNOT convince a Verifier to accept it.

Zero-know ledge
- The Verifier learns nothing from the proof except that it is true.

We also want this to be in a “succinct” package (very small in size) and fast to verify and non-interactive.

Interactive Zero-Knowledge Proof

Bank A

Bank A have made a transfer

Prove it (challenge)

Send the Proof

Verifies the Proof

Update the ledger/balances

Bank B

Non-Interactive Zero-Knowledge Proof (ZK-Snark)

Bank A

Bank A have made a transfer

Create a witness and run the ZK Circuit previously agreed

Send the Proof

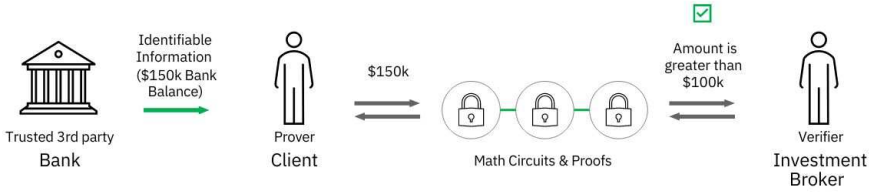
Verifies the Proof

Update the ledger/balances

Bank B

ZKP (Zero-Knowledge Proof)

Through ZKP (Zero-Knowledge Proof), Clients can prove to the investment broker that they have a certain amount of money in their bank account that is greater than $100k without revealing exactly how much they have.



ZKP (Zero-Knowledge Proof)

As you have proved, you do not need to store sensitivedata on-chain.

A common mistake is thinking of ZKP as a technology to encrypt data. If you need to share sensitive information, use offline/off-chain channelsand/or KEM/DEM encryption mechanisms,for example.

ZKP (Zero-Knowledge Proof)

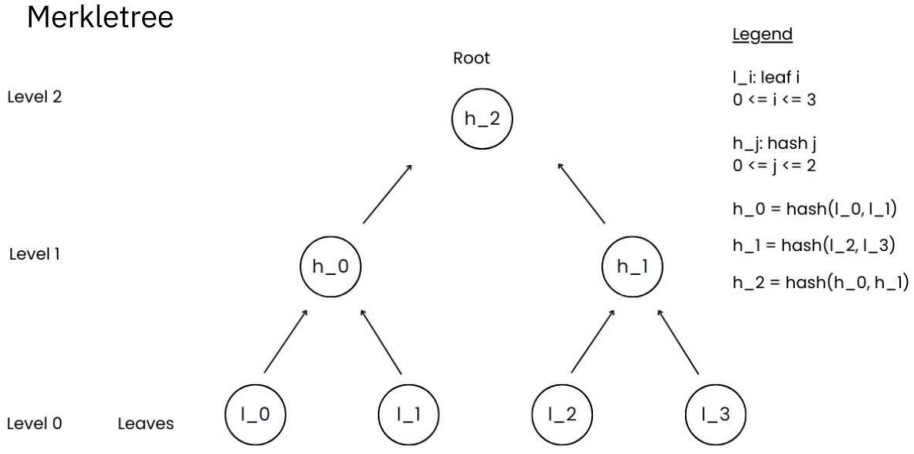
Please, for further in-depth theory, please:

Why and How zk-SNARK Works -Definitive Explanation:
https://arxiv.org/pdf/1906.07221v1.pdf

Zero Knowledge Proofs -A Technical Deep Dive:
https://www.youtube.com/watch?v=JOCUTtEeXyk&list=PLpKG2yDPRiV67eljFH0yrKl1xSx-PnHpe

What are zero-knowledge proofs?
https://ethereum.org/pt/zero-knowledge-proofs/

Merkletree



Merkletree

Please, for further in-depth theory, please:

Incremental Merkle Tree Semaphore v4
https://hackmd.io/@vplasencia/S1whLBN16

Commitment schemes

A cryptographic techniques used to commit to a value without revealing that value.

Hiding

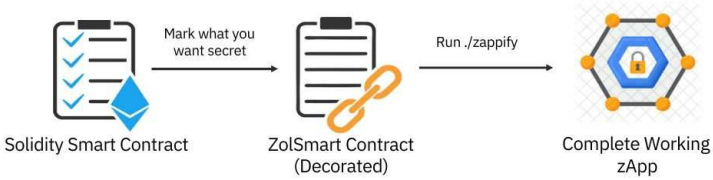
It prevents anyone from learning the committed value.

Binding

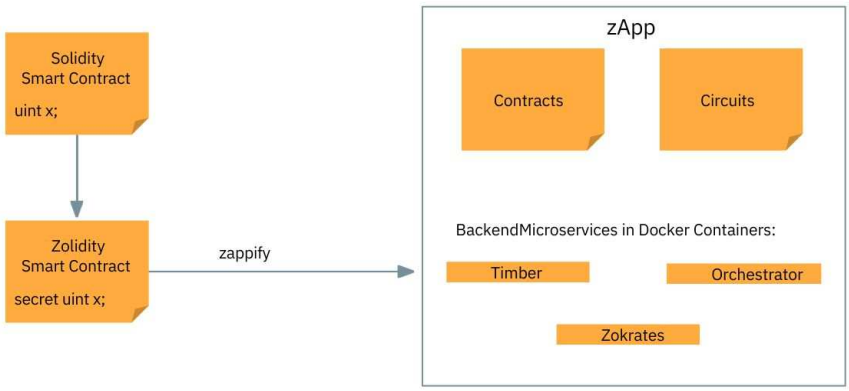
Once committed, it becomes computationally infeasible to change the value.

What is Starlight?

Starlight generates EVM-compatible ZK Applications directly from Solidity-based smart contracts. Outputs highly customized, unique application specific for an industry or even an interaction.

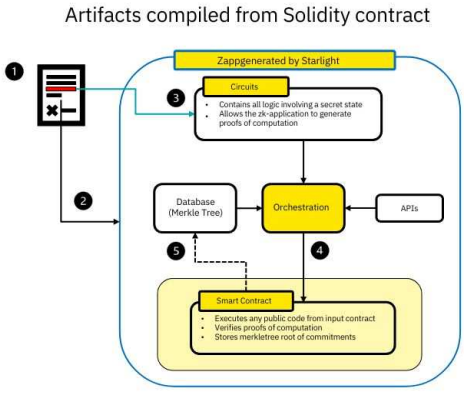


How does Starlight's transpilerwork?



The zAppArchitecture

1. The user writes a smart contract with their business logic, and marks the variables they want private
2. Starlight turns this marked smart contract into a full privacy-preserving application
3. Any logic involving a secret variable is moved to a zero-knowledge circuit
4. Instead of doing this computation in the open, a *proof*that it has been executed is verified on-chain
5. Current state is represented by values hidden inside commitments



Syntax of ZolSmart Contract

Secret

Decorator for:
- State variables
- Function parameters
- Local variable declaration

"Private" is already a reserved keyword in Solidity :(

Known

Decorator for:
Incrementation statements of secret variables

Allows a developer to enforce that "only the secret-holder may increment this secret state"

Results in:

A proof of knowledge of secret key
Nullification of an "old" commitment
Replacement with a new commitment

Unknown

Decorator for:
Incrementation statements of secret variables

Allows a developer to clarify that "anyone may increment this secret state"

Results in:

Creation of a new "part" commitment, representing the incrementation amount only
The variable being treated as "partitioned" throughout the zApp; meaning its value is a sum of many "parts"

```
contract Assign {

 secretuint256private a;
 functionadd(secretuint256value)public{

  unknown a += value;
 }
 functionremove(secretuint256value)public{

   a -= value;
    }
  }
```


Decorators -Secret

What it does?
- Contents of the variable remain confidential

For:
- State variables
- Function parameters
- Functions (future enhancement)

Not for:
- Local stack memory declarations

How it works?
- Create a commitment for this state variable that binds and hidesthe value

```
contract Example {

 secret uint x; // owned by the contract deployer

 functionadd(secretuinty)public{ knownx
   += y;
 }

}
```


Decorators -Known

What it does?
- Only the secret state variable owner can update it

For
- Incrementation statements of secret state variables

How it works?
- Proof of knowledge of existence of old commitment
- Proof of knowledge of secret key of the public key in commitment
- Nullifies old commitment
- Create new commitment

```
contract Example {

 secret uint x; // owned by the contract deployer

 functionadd(secretuinty)public{ knownx
   += y;
 }

}
```

Decorators -Unknown

What it does?

- Anyone can increment this secret state variable

For

- Incrementation statements of secret state variables

How it works?

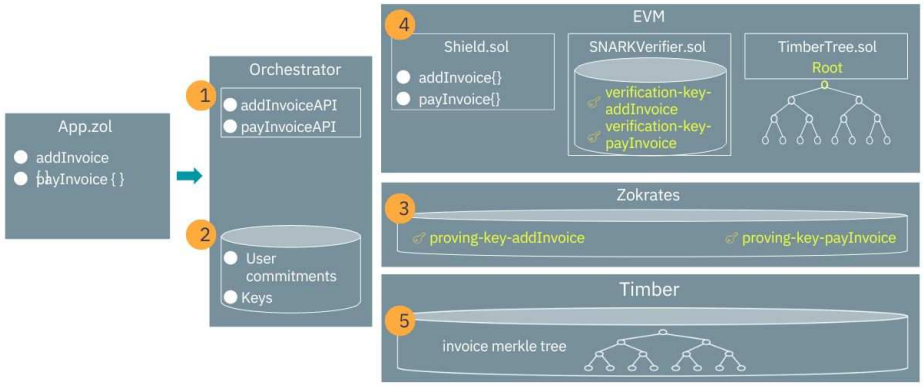
- Create a new ”part” commitment to hold only the value by which to update the amount
- Secrete state variable is a partitioned variable whose value is a summation of all it’s “part” commitments

```
contract Example {

  secret mapping(address => uint) balances;

  function deposit(uint amount) {
    balances[msg.sender] += amount;
  }

  function transfer(secret uint amount, secret
address recipient) {
    balances[msg.sender] -= amount;
    unknown balances[recipient] += amount;
  }

}
```

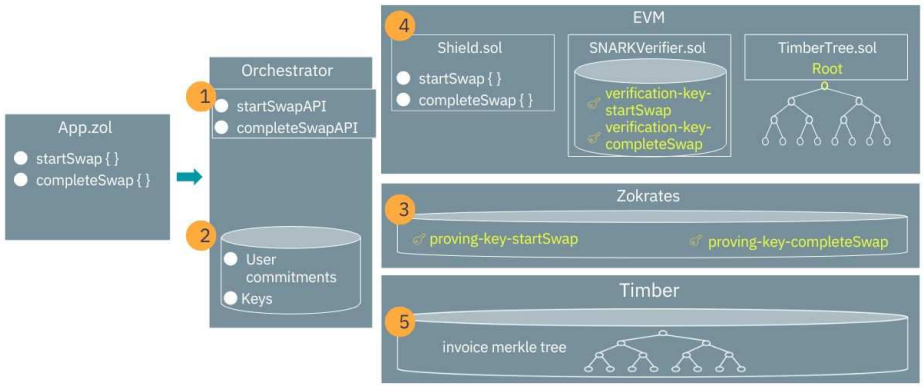

Example –Invoice.zol

```
contract Invoice {

  secret mapping(address => uint256) invoices;
  address contractOwner;

  function addinvoice(secret address owner,  secret  uint256
amount)public {
    require(invoices[owner] == 0);
    unknown invoices[owner] += amount;
  }

  function payInvoice(secret uint256 amount,  secret  address
owner)public {
    require(msg.sender==contractOwner);
    // imagine some payment here
    invoices[owner] – = amount;
  }

}
```

When user calls addInvoiceAPI

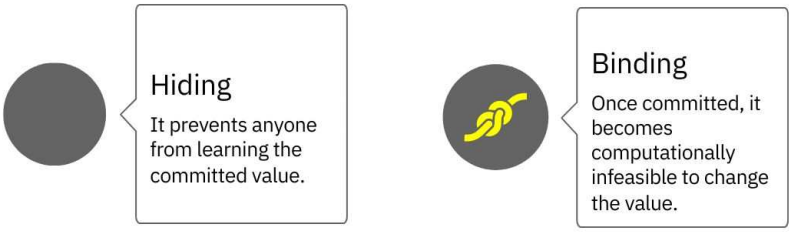


Starlight Architecture -When user perform a Swap sample



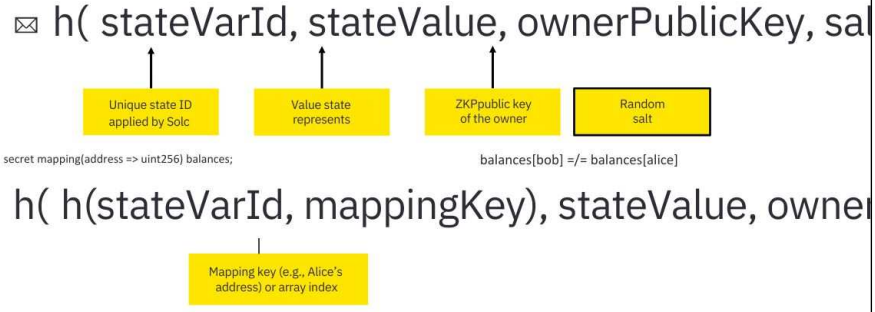
Commitment schemes

A cryptographic techniques used to commit to a value without revealing that value.



Commitment structure

What does a commitment structure that can hide any state change look like?



Nullifier to a Commitment

How does a nullifier looks like for a commitment ?

✉ h(stateVarId, ownerSecretKey, PrevCommitmentsalt)

- stateVarId: Unique state ID applied by Solc
- ownerSecretKey: ZKP Secret key of the owner
- PrevCommitmentsalt: Salt Associated with the Previous Commitment

```
secret mapping(address => uint256) balances;
```

h(h(stateVarId, mappingKey), ownerSecretKey, Commitmentsalt)

- mappingKey: Mapping key (e.g., Alice's address) or array index

Demo

https://github.com/jeffprestes/drex-starlight

For further information, please contact:

Thamilla Talarico
Thamilla.Talarico@br.ey.com
Jeff Prestes
Jefferson.Prestes.ext@br.ey.com

EY
Building a better working world

Lista de Assinaturas

Assinado por: LUCIANA GIULIANI DE OLIVEIRA REIS, 813.***.***-**, assinado em: 14/10/2024
Função: Chefe de Departamento
Papel: Representante BNDES

Assinado por: GLADSTONE MOISES ARANTES JUNIOR, 033.***.***-**, assinado em: 15/10/2024
Papel: Representante BNDES

Assinado por: ELDON TEIXEIRA COUTINHO, 471.***.***-**, assinado em: 15/10/2024
Papel: Representante TCU

Assinado por: JETRO PAULO WEBER, 904.***.***-**, assinado em: 16/10/2024
Papel: Representante SERPRO

Assinado por: RAINERIO RODRIGUES LEITE, 358.***.***-**, assinado em: 18/10/2024
Papel: Representante TCU

Assinado por: SERGIO MAIA RABELO, 815.***.***-**, assinado em: 05/11/2024
Papel: Representante Pref. Araguaina

Assinado por: IGOR THAWAN DO NASCIMENTO DA SILVA, 042.***.***-**, assinado em: 08/11/2024
Papel: Representante Pref. Araguaina

Assinado por: MARCO TULIO DA SILVA LIMA, 938.***.***-**, assinado em: 08/11/2024
Papel: Representante SERPRO

Assinado por: JOSE REYNALDO FORMIGONI FILHO, 031.***.***-**, assinado em: 09/11/2024
Papel: Representante CPQD

Assinado por: CLAUDEMIR CUSTODIO BRUM, 026.***.***-**, assinado em: 11/11/2024
Papel: Representante DATAPREV