Pauta

- Reports das iniciativas.
  - Acompanhamento.
  - Infra Básica.
  - Monitoração.
  - Responsabilização/permissionamento.
  - Comunicação.
- Controle de uso.
- Planejamento para o piloto.

Pauta

- Reports das iniciativas.
  - Acompanhamento.
  - Infra Básica.
  - Monitoração.
  - Responsabilização/permissionamento.
  - Comunicação.
- **Controle de uso.**
- Planejamento para o piloto.

Controle de Uso

- Objetivos essenciais e urgentes.
  - Garantir que a saúde da rede não seja afetada por ataques DoS.
    - Uso excessivo mal intencionado.
  - Garantir que a saúde da rede não seja afetada por *smart contracts* mal comportados.
    - Ex.: Loops infinitos.
- Objetivos gerais.
  - Evitar *smart contracts* pouco otimizados por conta do processamento gratuito.
  - Evitar que alguma instituição use mais banda da rede do que o permitido.

Controle de Uso

- Considerações.
  - Uso de ether garante tratamento *a priori* de certos ataques.
    - Não é possível atacar por não possuir ether suficiente.
    - Ether é mecanismo nativo.
      - Mesmo assim, levanta perguntas: onde a transação é bloqueada?
  - Por outro lado, é problema em alguns aspectos:
    - **A RBB não pode ter (nem parecer ter) criptomoeda.**
      - Seria preciso criar mecanismos para evitar mercado secundário.
    - Usabilidade dificultada, principalmente em casos de uso onde a transação não é de um backend e, sim, de um frontend.
      - Rastreio de gastos, por exemplo.
      - Account Abstraction pode ser uma solução no futuro.
  - Cobrança de ether controla estoque, não fluxo.
    - Ethers previamente distribuídos podem ser gastos sincronizadamente, dado que o preço não aumenta (em tese).
    - Para controlar fluxo, precisa de política ativa de distribuição de *gas,* gerando mais transações.

Controle de Uso

- Garantir que a saúde da rede não seja afetada por ataques DoS.
  - O principal é proteger os validators.
  - Testes demonstraram que um alto fluxo não atinge o núcleo da rede.
  - Permissionamento de endereços reduz muito a superfície de ataque.
    - Efeito mais ou menos similar à posse de ether.
    - Já está no escopo monitorar o permissionamento dos validators.
    - Avaliar se é possível priorizar transação para retirar o permissionamento de um endereço mal comportado.
  - Preocupação com os observadores.
    - Permissionamento local impede transações.
    - Outros tipos de ataque? Envolvimento especialistas de segurança.
- As medidas são necessárias de qualquer forma.
  - Teste de DoS, priorizar transação adm e segurança dos obs.

Controle de Uso

- Garantir que a saúde da rede não seja afetada por *smart contracts* mal comportados.
  - *Smart contracts* mal comportados podem, no máximo, tomar um bloco inteiro.
    - Não há impacto direto na estabilidade da rede.
    - Impacto indireto → Reduzir capacidade disponível para outras transações.
  - Medida de contenção.
    - Setar máx. de *gas* de uma transação → Máx de *gas* de cada instituição.
    - Garante controle *a priori* de forma simples.
    - Restritivo → Não aproveita “espaços vazios”.
      - Pode ser ajustado ao longo.

Controle de Uso

- Evitar *smart contracts* pouco otimizados por conta do processamento gratuito.
  - Após piloto, uso não será gratuito → Proporcional ao *gas*.
  - No piloto, abuso estará sendo consumido da parte do abusador.
  - Mesmo em caso de abuso, não há impactos para a rede.
- Buscar relatório de consumo por partícipe / endereço.
  - Não é tão prioritário, dado que o controle do impacto na rede já existe pelo limite do *gas* das transações.
- Medidas já atendem ao outro objetivo:
  - Evitar que alguma instituição use mais banda da rede do que o permitido.

Controle de Uso

- Resumo.
  - Decisão simplificadora.
    - Começar sem ether e com limite restritivo de tamanho de transação.
    - Monitorar situação, avaliar aplicações e ajustar ao longo.
  - Medidas já no escopo (ou que deveriam estar):
    - Monitorar permissionamento dos validators.
    - Permissionamento no Manual de Operações.
    - Teste de DoS na rede lab.
    - Segurança dos Observadores.
    - Avaliar priorização de transações de permissionamento.
  - Medidas específicas:
    - Relatório de uso de *gas*.

Controle de Uso

- Garantir que a saúde da rede não seja afetada por ataques DoS.
  - O principal é proteger os validators.
  - Testes anteriores demonstraram que um alto fluxo não atinge o núcleo da rede.
  - O permissionamento de endereços reduz muito a superfície de ataque.
    - Avaliar se é possível priorizar transações de despermissionamento de endereços atacantes.
  - Garantir que a saúde da rede não seja afetada por *smart contracts* mal comportados.
    - Ex.: Loops infinitos.
- Objetivos gerais.
  - Evitar *smart contracts* pouco otimizados por conta do processamento gratuito.
  - Evitar que alguma instituição use mais banda da rede do que o permitido.