monero (XMR)

criptomoeda verdadeiramente anônima

bruno cuconato

EMAp

monero

Figura 1: logo da monero

fatos básicos

- baseado no protocolo CryptoNote[1] (originalmente Bytecoin)

[1] https://cryptonote.org/

fatos básicos

- baseado no protocolo CryptoNote[1] (originalmente Bytecoin)
  - "correções" ao protocolo Bitcoin: PoW, emissão, constantes, scripts, anonimidade

[1] https://cryptonote.org/

fatos básicos

- baseado no protocolo CryptoNote[1] (originalmente Bytecoin)
  - "correções" ao protocolo Bitcoin: PoW, emissão, constantes, scripts, anonimidade
- monero altera o protocolo cryptonote para ser ainda mais anônimo

[1] https://cryptonote.org/

fatos básicos

- baseado no protocolo CryptoNote[1] (originalmente Bytecoin)
  - "correções" ao protocolo Bitcoin: PoW, emissão, constantes, scripts, anonimidade
- monero altera o protocolo cryptonote para ser ainda mais anônimo
- busca ser moeda totalmente anônima $\implies$ fungível

[1] https://cryptonote.org/

fatos básicos

- baseado no protocolo CryptoNote[1] (originalmente Bytecoin)
  - "correções" ao protocolo Bitcoin: PoW, emissão, constantes, scripts, anonimidade
- monero altera o protocolo cryptonote para ser ainda mais anônimo
- busca ser moeda totalmente anônima $\implies$ fungível
- top 10 em market capitalization

[1] https://cryptonote.org/

fatos básicos

- baseado no protocolo CryptoNote[1] (originalmente Bytecoin)
  - "correções" ao protocolo Bitcoin: PoW, emissão, constantes, scripts, anonimidade
- monero altera o protocolo cryptonote para ser ainda mais anônimo
- busca ser moeda totalmente anônima $\implies$ fungível
- top 10 em market capitalization
- 1 XMR $= 10^{12}$ "monoshis"

[1] https://cryptonote.org/

addresses

- o dobro do tamanho de um endereço Bitcoin, pois cada endereço corresponde à duas chaves privadas:

addresses

- o dobro do tamanho de um endereço Bitcoin, pois cada endereço corresponde à duas chaves privadas:
- a *view key* permite identificar transações enviadas para o endereço.
  essa chave pode ser entregue a terceiros para fins de verificação, transparência ou delegação de processamento (e.g., entre *thin wallets* e servidores). sem a outra chave privada, não se pode gastar fundo algum!

addresses

- o dobro do tamanho de um endereço Bitcoin, pois cada endereço corresponde à duas chaves privadas:
- a *view key* permite identificar transações enviadas para o endereço.
  essa chave pode ser entregue a terceiros para fins de verificação, transparência ou delegação de processamento (e.g., entre *thin wallets* e servidores). sem a outra chave privada, não se pode gastar fundo algum!
- a outra chave é a chave privada a que estamos acostumados.

addresses

- você pode ter um único endereço público, se quiser.

addresses

- você pode ter um único endereço público, se quiser.
- para que Alice envie XMR a Bob, ele calcula uma chave de uso único a partir do endereço público de Bob usando uma modificação do algoritmo DH.

addresses

- você pode ter um único endereço público, se quiser.

- para que Alice envie XMR a Bob, ele calcula uma chave de uso único a partir do endereço público de Bob usando uma modificação do algoritmo DH.
- essa chave não está ligada à chave pública de Bob, de modo que só Bob e Alice sabem a quem pertence essa chave.

ring signatures

- aqui entra a parte de obfuscação do destinatário.

ring signatures

- aqui entra a parte de obfuscação do destinatário.
- uma *ring signature* é uma assinatura de grupo:

ring signatures

- aqui entra a parte de obfuscação do destinatário.
- uma *ring signature* é uma assinatura de grupo:
  - ela é feita com a chave privada do destinatário e outras chaves públicas que são as *mixin*.

ring signatures

- aqui entra a parte de obfuscação do destinatário.
- uma *ring signature* é uma assinatura de grupo:
  - ela é feita com a chave privada do destinatário e outras chaves públicas que são as *mixin*.
  - só a destinatária real pode recuperar o valor da transação, usando uma imagem de sua chave privada.

ring signatures

- aqui entra a parte de obfuscação do destinatário.
- uma *ring signature* é uma assinatura de grupo:
  - ela é feita com a chave privada do destinatário e outras chaves públicas que são as *mixin*.
  - só a destinatária real pode recuperar o valor da transação, usando uma imagem de sua chave privada.
  - i.e., os destinatários fictícios não conseguem gastar o valor "recebido".

ring signatures

- aqui entra a parte de obfuscação do destinatário.
- uma *ring signature* é uma assinatura de grupo:
  - ela é feita com a chave privada do destinatário e outras chaves públicas que são as *mixin*.
  - só a destinatária real pode recuperar o valor da transação, usando uma imagem de sua chave privada.
  - i.e., os destinatários fictícios não conseguem gastar o valor "recebido".
  - mas um observador externo só sabe se a assinatura é válida, e não qual das participantes do anel a produziu[2]

[2] Traceable Ring Signature

double spending

cada nó mantém uma lista das imagens das chaves já usadas.
uma transação que tente recuperar o valor de uma UTXO já gasta repetirá essa imagem e será rejeitada.

ringCT

- um problema na privacidade proporcionada pelo protocolo cryptonote é revelação dos valores gastos

ringCT

- um problema na privacidade proporcionada pelo protocolo cryptonote é revelação dos valores gastos
- alguns desenvolvedores da monero se uniram para resolver o problema com criptografia homomórfica[3]:

[3] projeto de ringCT

ringCT

- um problema na privacidade proporcionada pelo protocolo cryptonote é revelação dos valores gastos
- alguns desenvolvedores da monero se uniram para resolver o problema com criptografia homomórfica[3]:
  - pode-se verificar se os valores das entradas e saídas de uma transação batem sem precisar revelar os valores envolvidos.

[3] projeto de ringCT

ringCT

- um problema na privacidade proporcionada pelo protocolo cryptonote é revelação dos valores gastos
- alguns desenvolvedores da monero se uniram para resolver o problema com criptografia homomórfica[3]:
  - pode-se verificar se os valores das entradas e saídas de uma transação batem sem precisar revelar os valores envolvidos.
  - precisa-se, no entanto, de uma prova criptográfica adicional para mostrar que os valores não extrapolam um intervalo.

[3] projeto de ringCT

PoW

- crítica ao algoritmo de PoW da Bitcoin: concentração de poder nas mãos de poucos mineradores.

PoW

- crítica ao algoritmo de PoW da Bitcoin: concentração de poder nas mãos de poucos mineradores.
- uma PoW igualitária só é possível com CPUs.

PoW

- crítica ao algoritmo de PoW da Bitcoin: concentração de poder nas mãos de poucos mineradores.
- uma PoW igualitária só é possível com CPUs.
- mas como implementar um algoritmo resistente à GPUs e à ASICs?

PoW

- usar instruções embutidas nas CPUs.

PoW

- usar instruções embutidas nas CPUs.
- random access to slow memory: cada novo bloco depende de todos os outros.

PoW

- usar instruções embutidas nas CPUs.
- random access to slow memory: cada novo bloco depende de todos os outros.
- 2Mb por iteração:

PoW

- usar instruções embutidas nas CPUs.
- random access to slow memory: cada novo bloco depende de todos os outros.
- 2Mb por iteração:
  - cabe no cache L3 da CPU.

PoW

- usar instruções embutidas nas CPUs.
- random access to slow memory: cada novo bloco depende de todos os outros.
- 2Mb por iteração:
  - cabe no cache L3 da CPU.
  - é grande demais para uma ASIC.

PoW

- usar instruções embutidas nas CPUs.
- random access to slow memory: cada novo bloco depende de todos os outros.
- 2Mb por iteração:
  - cabe no cache L3 da CPU.
  - é grande demais para uma ASIC.
  - cabe com folga em uma GPU, mas o acesso é mais lento do que na CPU.

no hardcoded constants

constantes inflexíveis são ponto de centralização da rede, pois a implementação de referência tem poder de escolhê-las.

além disso, perde-se em flexibilidade, e provoca-se descontinuidades.

- pensem na redução de *block reward* da Bitcoin (variações bruscas na remuneração da mineração)

no hardcoded constants – emissão de XMR

- em Bitcoin temos limite de 21 milhões BTC emitidas

no hardcoded constants – emissão de XMR

- em Bitcoin temos limite de 21 milhões BTC emitidas
  - até onde se sabe, um número arbitrário escolhido por Satoshi Nakamoto

no hardcoded constants – emissão de XMR

- em Bitcoin temos limite de 21 milhões BTC emitidas
  - até onde se sabe, um número arbitrário escolhido por Satoshi Nakamoto
- em cryptonote, temos um limite de $2^{64} - 1$:

no hardcoded constants – emissão de XMR

- em Bitcoin temos limite de 21 milhões BTC emitidas
  - até onde se sabe, um número arbitrário escolhido por Satoshi Nakamoto
- em cryptonote, temos um limite de $2^{64} - 1$:

  based only on implementation limits, not on intuition such as "N coins ought to be enough for anybody"

no hardcoded constants – emissão de XMR

$$\mathrm{BaseReward} = (\mathrm{MSupply} - A) \gg 18$$

onde A é o número de moedas já geradas e o operador $\gg$ é bit-shifting.

no hardcoded constants – dificuldade

[](aqui o ponto é a flexibilidade maior, pois ajusta-se todo dia ao invés de a cada duas semanas (mais ou menos)

- em Bitcoin é ajustada a cada 2016 blocos, usando a diferença das timestamps do primeiro e do último blocos nesse intervalo como multiplicador (usando intervalo ideal de 1 bloco a cada 10 minutos)

no hardcoded constants – dificuldade

[](aqui o ponto é a flexibilidade maior, pois ajusta-se todo dia ao invés de a cada duas semanas (mais ou menos)

- em Bitcoin é ajustada a cada 2016 blocos, usando a diferença das timestamps do primeiro e do último blocos nesse intervalo como multiplicador (usando intervalo ideal de 1 bloco a cada 10 minutos)
- em cryptonote: ajustada a cada 720 blocos usando a soma do trabalho feito dividida pelo tempo gasto para fazê-lo como multiplicador (usando intervalo ideal[4] de 1 bloco a cada 2 minutos)

[4] interessante que aqui temos algumas hardcoded constants.

no hardcoded constants – dificuldade

[](aqui o ponto é a flexibilidade maior, pois ajusta-se todo dia ao invés de a cada duas semanas (mais ou menos)

- em Bitcoin é ajustada a cada 2016 blocos, usando a diferença das timestamps do primeiro e do último blocos nesse intervalo como multiplicador (usando intervalo ideal de 1 bloco a cada 10 minutos)
- em cryptonote: ajustada a cada 720 blocos usando a soma do trabalho feito dividida pelo tempo gasto para fazê-lo como multiplicador (usando intervalo ideal[4] de 1 bloco a cada 2 minutos)
  - para reduzir o problema das timestamps não serem confiáveis, ordena-se os blocos e remove-se 60 blocos em cada extremidade antes de calcular o intervalo entre o primeiro e último bloco sem "outliers" (?)

[4] interessante que aqui temos algumas hardcoded constants.

no hardcoded constants – tamanho do bloco

- é preciso um limite duro para impedir *flooding*, mas não deve ser hardcoded

  Let M_N be the median value of the last N blocks sizes. Then the "hard-limit" for the size of accepting blocks is $2M_N$. It averts the blockchain from bloating but still allows the limit to slowly grow with time if necessary.

no hardcoded constants – tamanho do bloco

- é preciso um limite duro para impedir *flooding*, mas não deve ser hardcoded

  Let M_N be the median value of the last N blocks sizes. Then the "hard-limit" for the size of accepting blocks is $2M_N$. It averts the blockchain from bloating but still allows the limit to slowly grow with time if necessary.

- não há limite no tamanho de transação: se alguém quiser pagar o preço de uma transação gigante, *so be it*.

no hardcoded constants – tamanho do bloco

- é preciso um limite duro para impedir *flooding*, mas não deve ser hardcoded

  Let M_N be the median value of the last N blocks sizes. Then the "hard-limit" for the size of accepting blocks is $2M_N$. It averts the blockchain from bloating but still allows the limit to slowly grow with time if necessary.

- não há limite no tamanho de transação: se alguém quiser pagar o preço de uma transação gigante, *so be it*.
  - isso é útil para escolher o fator *mixin* das transações – paga-se mais por mais privacidade (pois isso gera um custo para os full nodes)

no hardcoded constants – tamanho do bloco

- para prevenir um ataque de SPAMming de um minerador que sempre preenche seus blocos até o máximo com transações inúteis, é preciso penalizar blocos grandes demais.

no hardcoded constants – tamanho do bloco

- para prevenir um ataque de SPAMming de um minerador que sempre preenche seus blocos até o máximo com transações inúteis, é preciso penalizar blocos grandes demais.
- define-se um tamanho máximo gratuito de bloco; a partir desse tamanho, diminui-se a recompensa por bloco de acordo com:

no hardcoded constants – tamanho do bloco

- para prevenir um ataque de SPAMming de um minerador que sempre preenche seus blocos até o máximo com transações inúteis, é preciso penalizar blocos grandes demais.
- define-se um tamanho máximo gratuito de bloco; a partir desse tamanho, diminui-se a recompensa por bloco de acordo com:
- $$\mathrm{NewReward} = \mathrm{BaseReward}\left(\frac{\mathrm{BlkSize}}{M_n} - 1\right)^2$$

bulky scripts

- linguagem de liberação de fundos minimalista, ainda mais do que a de Bitcoin.

bulky scripts

- linguagem de liberação de fundos minimalista, ainda mais do que a de Bitcoin.
  - só permite cinco operadores, `min`, `max`, `sum`, `mul`, `cmp`.

bulky scripts

- linguagem de liberação de fundos minimalista, ainda mais do que a de Bitcoin.
  - só permite cinco operadores, `min`, `max`, `sum`, `mul`, `cmp`.
- além disso, pode ser expressa em menos bytes, o que reduz o tamanho das transações.

bulky scripts

- segundo o criador da cryptonote, não há perda de expressividade em relação à Bitcoin.[5]

[5] não encontrei referências sobre essa linguagem.

bulky scripts

- segundo o criador da cryptonote, não há perda de expressividade em relação à Bitcoin.[5]
- monero ainda não implementou linguagem de scripting alguma, no entanto.[6]

[5] não encontrei referências sobre essa linguagem.

[6] https://monero.stackexchange.com/questions/2813/can-monero-transactions-contain-scripts

críticas

- constantes da curva elíptica

críticas

- constantes da curva elíptica
- não parece haver estratégia para conter o tamanho da blockchain: se XMR se tornasse tão popular quanto BTC haveria problemas sérios de escalabilidade

críticas

- constantes da curva elíptica
- não parece haver estratégia para conter o tamanho da blockchain: se XMR se tornasse tão popular quanto BTC haveria problemas sérios de escalabilidade
- uso inovador de criptografia no contexto de criptomoedas sempre é arriscado: podem haver brechas desconhecidas, pois o modelo não foi testado extensivamente como o da Bitcoin:

críticas

- constantes da curva elíptica
- não parece haver estratégia para conter o tamanho da blockchain: se XMR se tornasse tão popular quanto BTC haveria problemas sérios de escalabilidade
- uso inovador de criptografia no contexto de criptomoedas sempre é arriscado: podem haver brechas desconhecidas, pois o modelo não foi testado extensivamente como o da Bitcoin:
  - assinaturas, *key images*

críticas

- constantes da curva elíptica
- não parece haver estratégia para conter o tamanho da blockchain: se XMR se tornasse tão popular quanto BTC haveria problemas sérios de escalabilidade
- uso inovador de criptografia no contexto de criptomoedas sempre é arriscado: podem haver brechas desconhecidas, pois o modelo não foi testado extensivamente como o da Bitcoin:
  - assinaturas, *key images*
  - PoW algorithm

críticas

- mesmo com RingCT, a escolha das UTXO para participarem da *ring signature* é feita de forma ingênua.

críticas

- mesmo com RingCT, a escolha das UTXO para participarem da *ring signature* é feita de forma ingênua.
- na maior parte dos casos, a UTXO mais recente é a UTXO verdadeira. Miller et al.[7] propõem um algoritmo melhor para essa escolha

[7] An Empirical Analysis of Linkability in the Monero Blockchain

críticas

a principal barreira para a adoção de uma nova criptomoeda é a transparência.

referências

- cryptonote whitepaper [pdf] [annotated] [critique]

referências

- cryptonote whitepaper [pdf] [annotated] [critique]
- cryptonote coin generator

referências

- cryptonote whitepaper [pdf] [annotated] [critique]
- cryptonote coin generator
- cryptonight hash function spec

referências

- cryptonote whitepaper [pdf] [annotated] [critique]
- cryptonote coin generator
- cryptonight hash function spec
- ajuste de dificuldade

referências

- cryptonote whitepaper [pdf] [annotated] [critique]
- cryptonote coin generator
- cryptonight hash function spec
- ajuste de dificuldade
- monero research papers