ICMC USP SÃO CARLOS

THE DEVELOPER'S CONFERENCE

PRIVACIDADE EM BLOCKCHAIN:

O ESTADO DA ARTE

EDGAR TAMIO HIRAMA

IOS DEVELOPER

ARCTOUCH

THE DEVELOPER'S CONFERENCE

SUMÁRIO

ARCTOUCH

INTRODUÇÃO

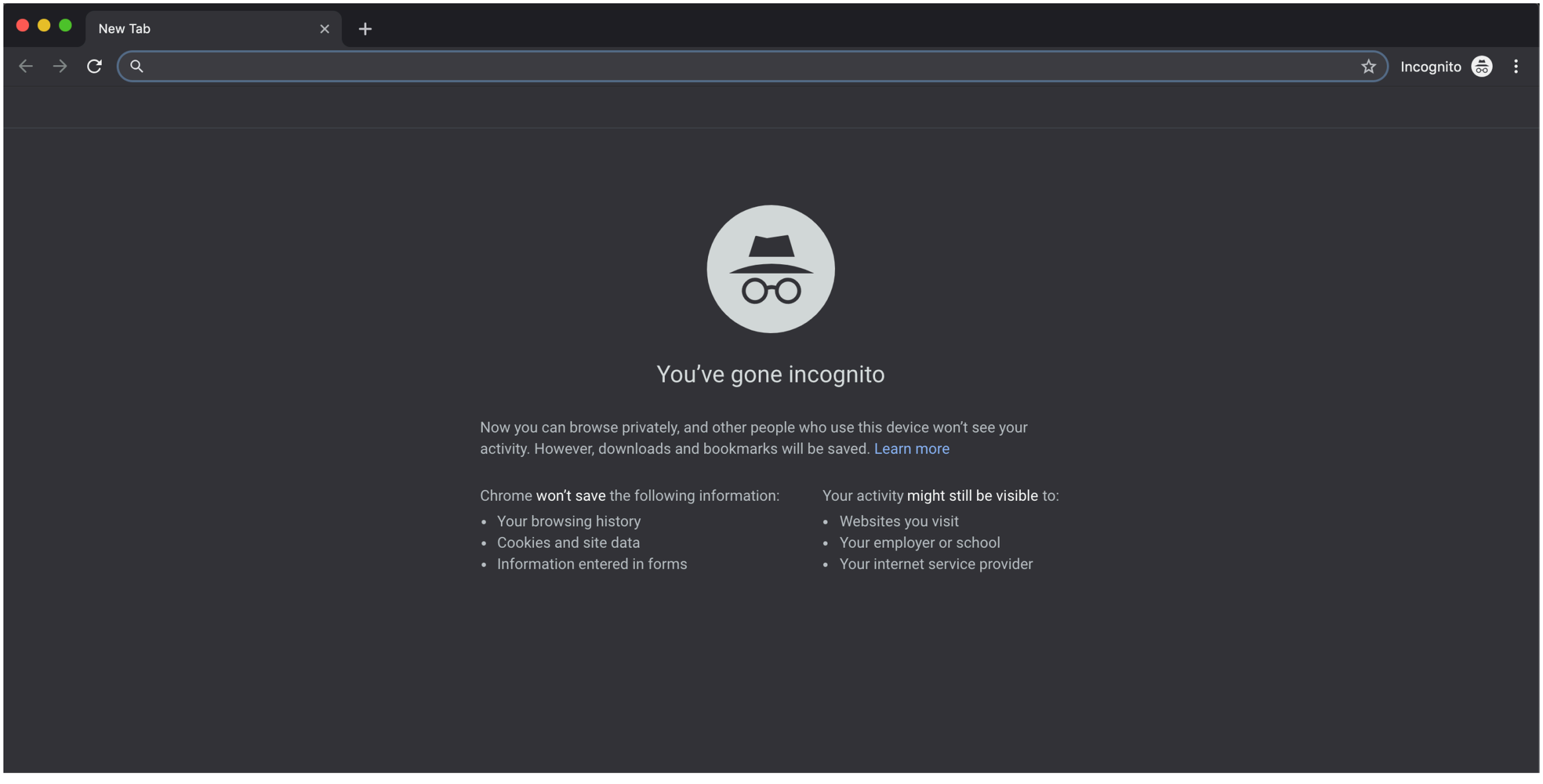
INTRODUÇÃO | APRESENTAÇÃO PESSOAL

- Desenvolvedor iOS
- Mestrando em Ciências de Dados - ICMC - USP - São Carlos
- Orientador: Prof. Dr. Jó Ueyama
- Tema: Privacidade em Blockchain

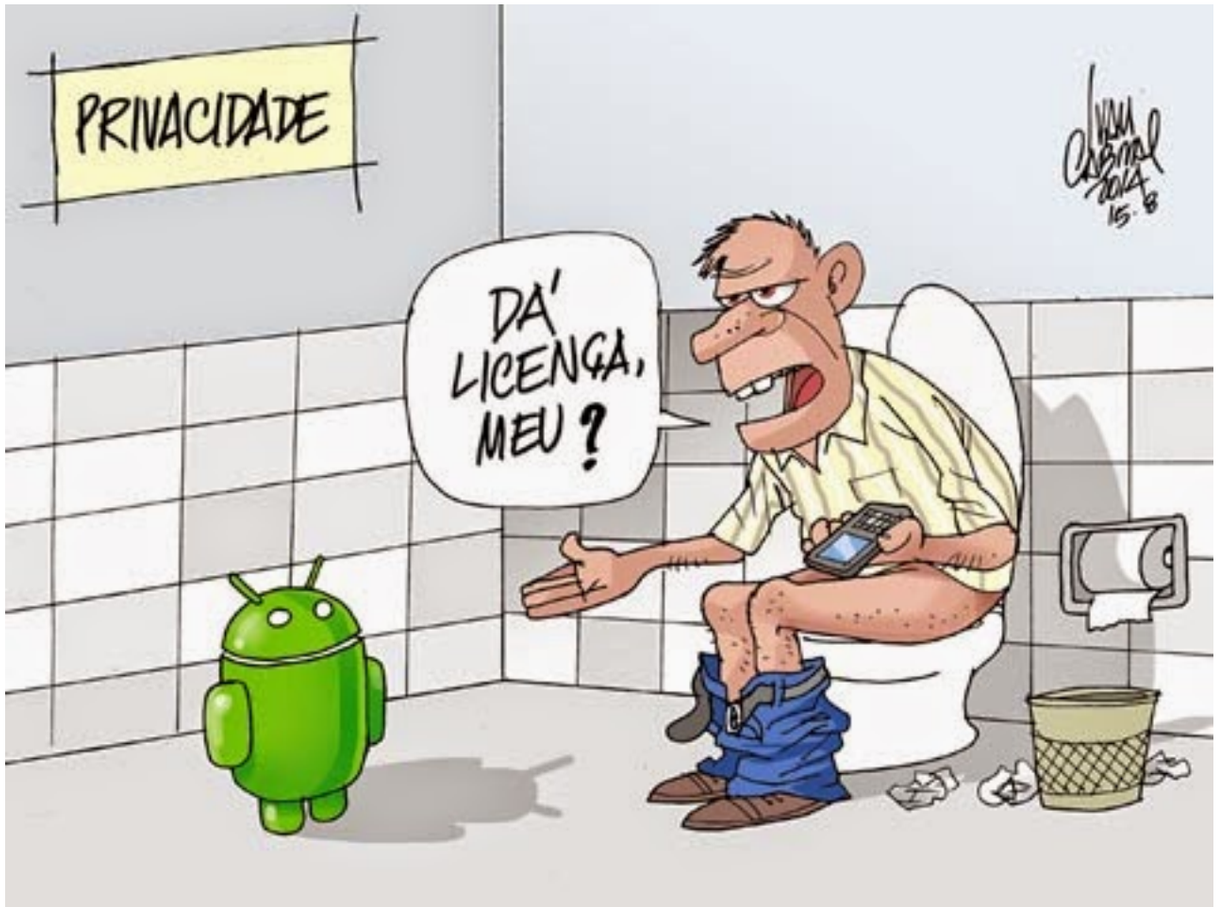
INTRODUÇÃO | CONTEXTUALIZAÇÃO

- O que é privacidade?

INTRODUÇÃO | PRIVACIDADE



INTRODUÇÃO | CONTEXTUALIZAÇÃO



http://www.ivancabral.com/2014/08/charge-do-dia-privacidade.html

INTRODUÇÃO | PRIVACIDADE

Qualidade do que é privado, do que diz respeito a alguém em particular: não se deve invadir a privacidade de ninguém.

Intimidade pessoal; vida privada, particular: cuidava dos filhos na privacidade do lar.

https://www.dicio.com.br/privacidade/

INTRODUÇÃO | PRIVACIDADE

É a habilidade de uma pessoa em controlar a exposição e a disponibilidade de informações acerca de si.

https://www.dicionarioinformal.com.br/significado/privacidade/12080/

MOTIVAÇÃO

MOTIVAÇÃO

- Necessidade para aplicações comerciais
- Falhas em servidores “centralizados” conhecidos (Facebook, Netflix)
- Valorização das informações de usuários
- GDPR (Europa)

MOTIVAÇÃO | CASO NETFLIX

Robust De-anonymization of Large Sparse Datasets

Arvind Narayanan and Vitaly Shmatikov

Who's Watching?
De-anonymization of Netflix Reviews using Amazon Reviews

Maryam Archie, Sophie Gershon, Abigail Katcoff, and Aaron Zeng
{marchie, sgershon, akatcoff, a2z}@mit.edu

TECHNOLOGY

Netflix Cancels Contest After Concerns Are Raised About Privacy

By **STEVE LOHR** MARCH 12, 2010

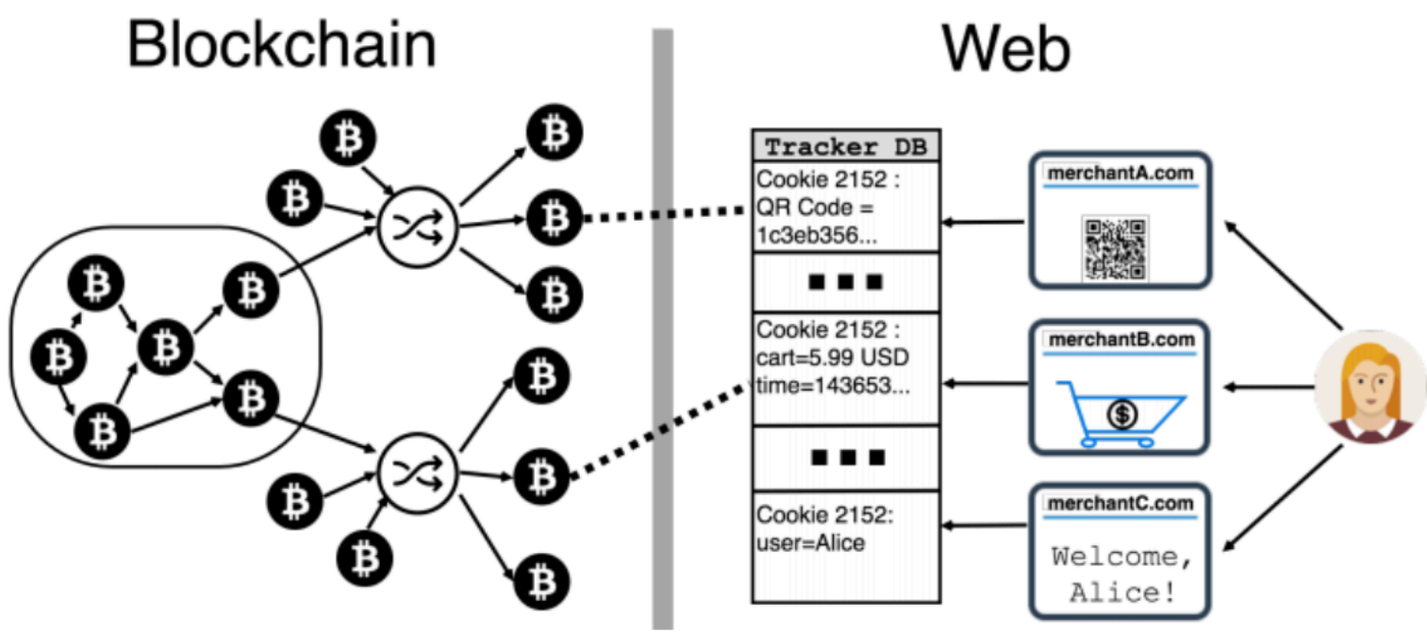
MOTIVAÇÃO | BITCOIN

Business Impact

Bitcoin Transactions Aren't as Anonymous as Everyone Hoped

Web merchants routinely leak data about purchases. And that can make it straightforward to link individuals with their Bitcoin purchases, say cybersecurity researchers.

by Emerging Technology from the arXiv August 23, 2017



ARCTOUCH

TECNICAS EXISTENTES

TÉCNICAS EXISTENTES

- Zero-knowledge proof
- zk-SNARKS
- Multi-Party Computation
- Trusted Execution Environment

TÉCNICAS EXISTENTES | ZERO-KNOWLEDGE PROOF

- Verifier (V), Prover (P)
- Possibilidade de provar que possui conhecimento de algo sem revelar maiores informações ao verificador
- Método interativo


Coca-Cola
12 FL OZ
(355 mL)
pepsi

TÉCNICAS EXISTENTES | ZK-SNARKS

- Zero-knowledge succinct non-interactive arguments of knowledge
- Não necessita de interação
- Rápido processamento (escalabilidade)

TÉCNICAS EXISTENTES | MULTI-PARTY COMPUTATION

- Compartilha uma parte da informação com outros peers da rede
- Cada um processa a parte pela qual ficou responsável
- Simula um servidor centralizado confiável

TÉCNICAS EXISTENTES | MULTI-PARTY COMPUTATION

- Exemplo: Adição
- P0 tem a = 5, P1 tem b = 8
- P0 -> a_0 = 3, a_1 = 2
- P1 -> b_0 = 9, b_1 = -1
- a + b = (a_0 + b_0) + (a_1 + b_1)

TÉCNICAS EXISTENTES | TRUSTED EXECUTION ENVIRONMENT

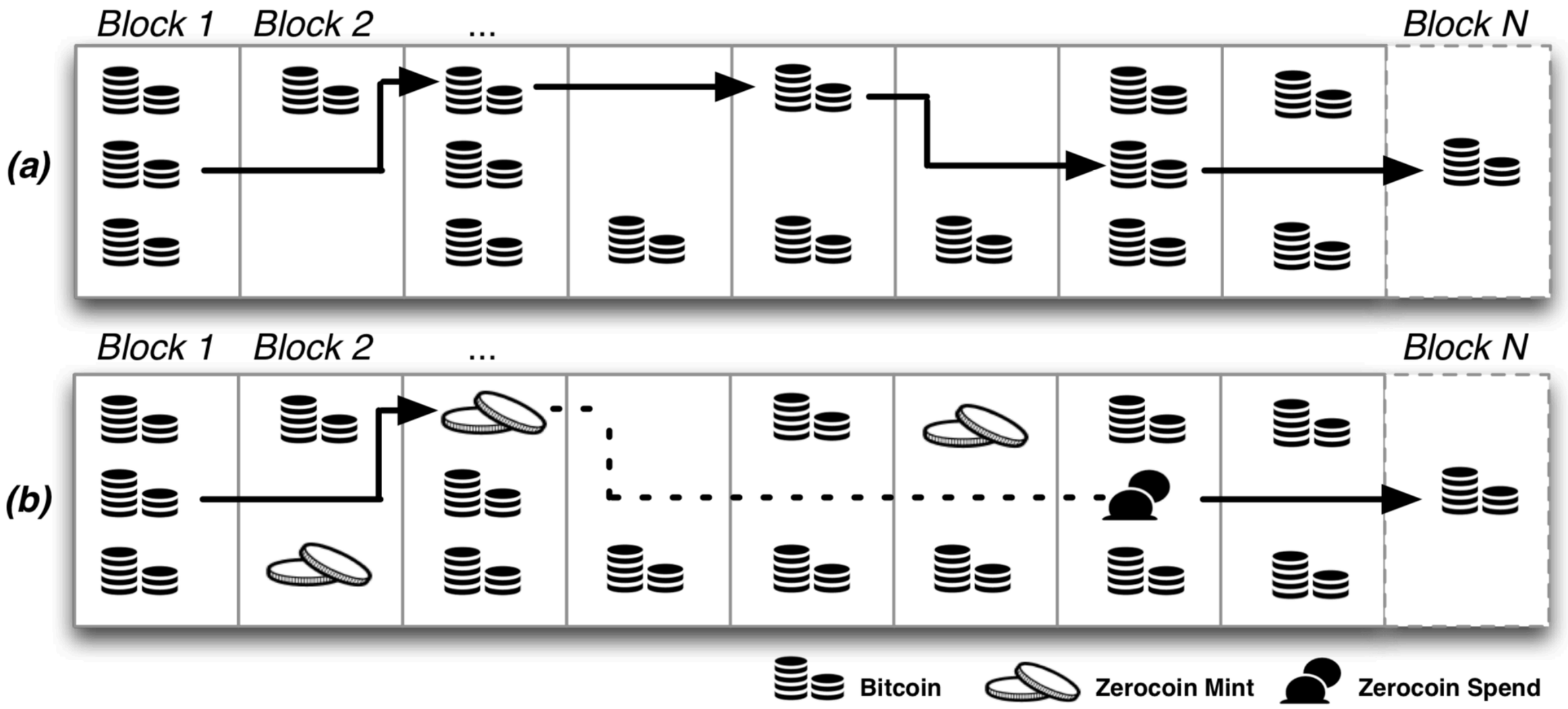
- Ambiente físico confiável para processamento de dados
- Impede que o próprio usuário / SO veja os dados sendo processados
- Funciona através de *remote attestation*
- Exemplos: Intel SGX, TrustZONE

~ APLICAÇÕES

APLICAÇÕES | ZEROCOIN

- Preocupação com a anonimidade do Bitcoin
- Baseia-se em “queimar" a moeda e transformá-la em uma nova, sem rastros
- Zero-knowledge proofs
- Valores das transações e recipiente não são encriptados

APLICAÇÕES | ZEROCOIN



APLICAÇÕES | ZEROCASH

- Encripta todos os dados da transação
- Baseia-se em zk-SNARKS
- Necessita de um setup inicial

APLICAÇÕES | MONERO

- Baseia-se no protocolo CryptoNote
- Método de *Ring Signatures*
- Método de mixing de transações

APLICAÇÕES | EKIDEN

- Sistema híbrido baseado em TEEs
- *Computation Nodes* x *Consensus Nodes*
- Maior escalabilidade e performance

APLICAÇÕES | ENIGMA

- Processamento de dados encriptados
- Trusted execution environments (SGX)
- Armazenamento de provas de execução
- Multi-party computation
- Pouca diferença para o Ekiden

CONSIDERAÇÕES FINAIS

CONSIDERAÇÕES FINAIS

- Definir que tipo de privacidade a plataforma oferece/ quer oferecer
- As grandes plataformas para processamento de dados privados ainda não estão disponíveis no mercado

LINKS

THE DEVELOPER'S CONFERENCE

ICMC USP SÃO CARLOS

LINKS | NÃO ACADÊMICOS

- https://blog.enigma.co/blockchain-privacy-transactional-or-computational-c4580d17b1f9

- https://hackernoon.com/facebook-pro-an-open-letter-c43edd70a91e

- http://zerocash-project.org/how_zerocash_works

- https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/

ARCTOUCH

LINKS | NÃO ACADÊMICOS

- https://docsend.com/view/fsdz4hv (EKIDEN)
- http://zerocoin.org
- https://gdpr.eu
- https://www.eublockchainforum.eu/reports

LINKS | WHITEPAPERS

- http://zerocoin.org/media/pdf/ZerocoinOakland.pdf
- http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf
- https://arxiv.org/pdf/1804.05141.pdf (Ekiden)
- https://enigma.co/enigma_full.pdf
- https://whitepaperdatabase.com/monero-xmr-whitepaper/

THE DEVELOPER'S CONFERENCE

DÚVIDAS?

ARCTOUCH

CONTATO

- edgar.hirama@arctouch.com
- edgar.hirama@usp.br

THE DEVELOPER'S CONFERENCE

OBRIGADO.

WE ARE HIRING !