O que é blockchain, sua origem e tecnologias

PUC Minas

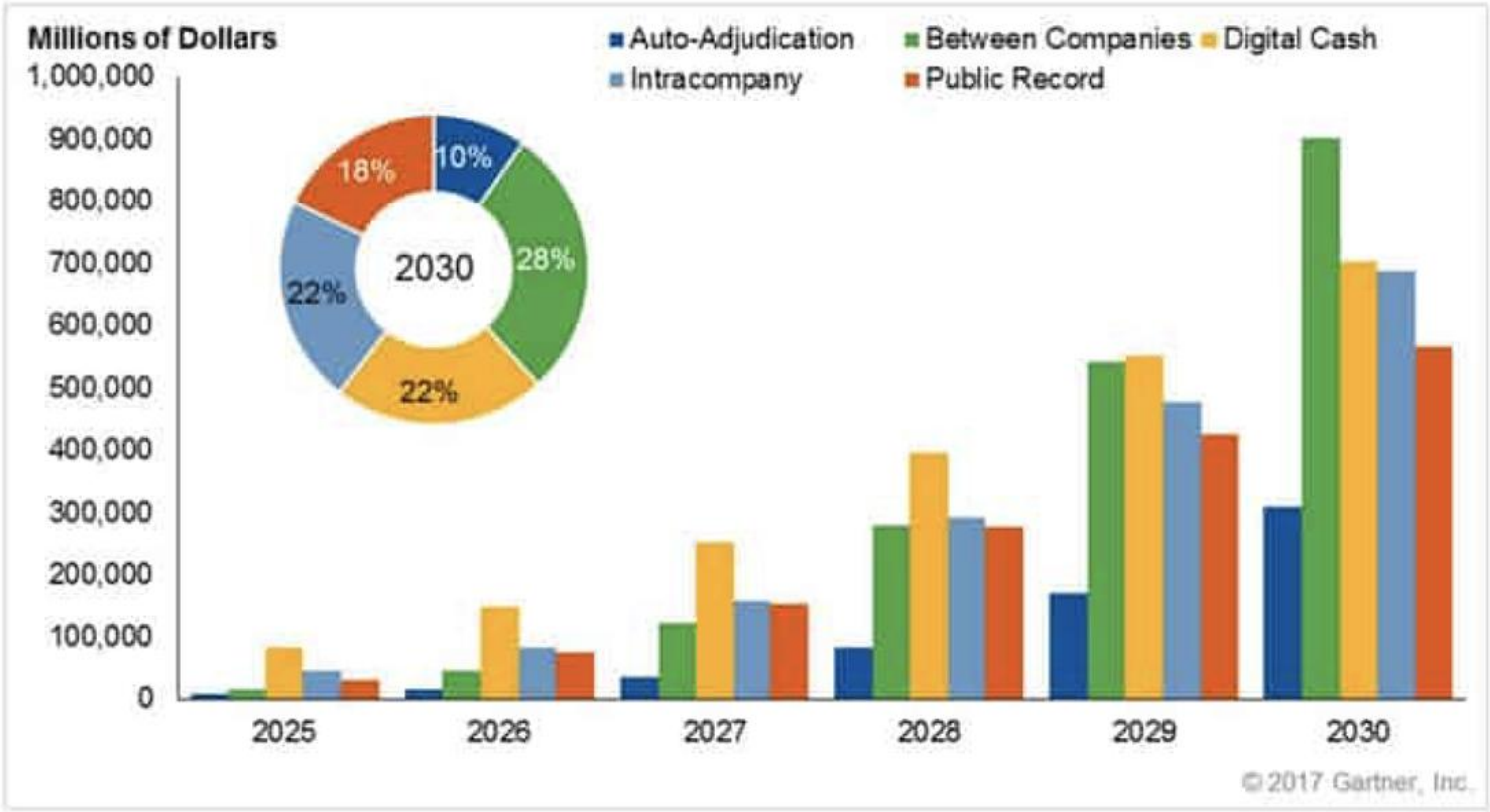
Aplicações Descentralizadas e Blockchain

Prof. Carlos Leonardo dos S. Mendes

- A confiança é fundamental para qualquer sistema de trocas.
- No sistema monetário atual, desde o abandono do lastro em ouro, o valor das moedas se baseia em um sistema de garantias oferecido pelo Estado.
- De uma forma geral, qualquer troca no sistema capitalista tem um terceiro como garantidor, geralmente um órgao de Estado.
- A ausência de confiança é a regra!

A CONFIANÇA COMO ELEMENTO FUNDAMENTAL DO CAPITALISMO

Business value-add of Blockchain - $176 billion by 2025, $3.1 trillion by 2030

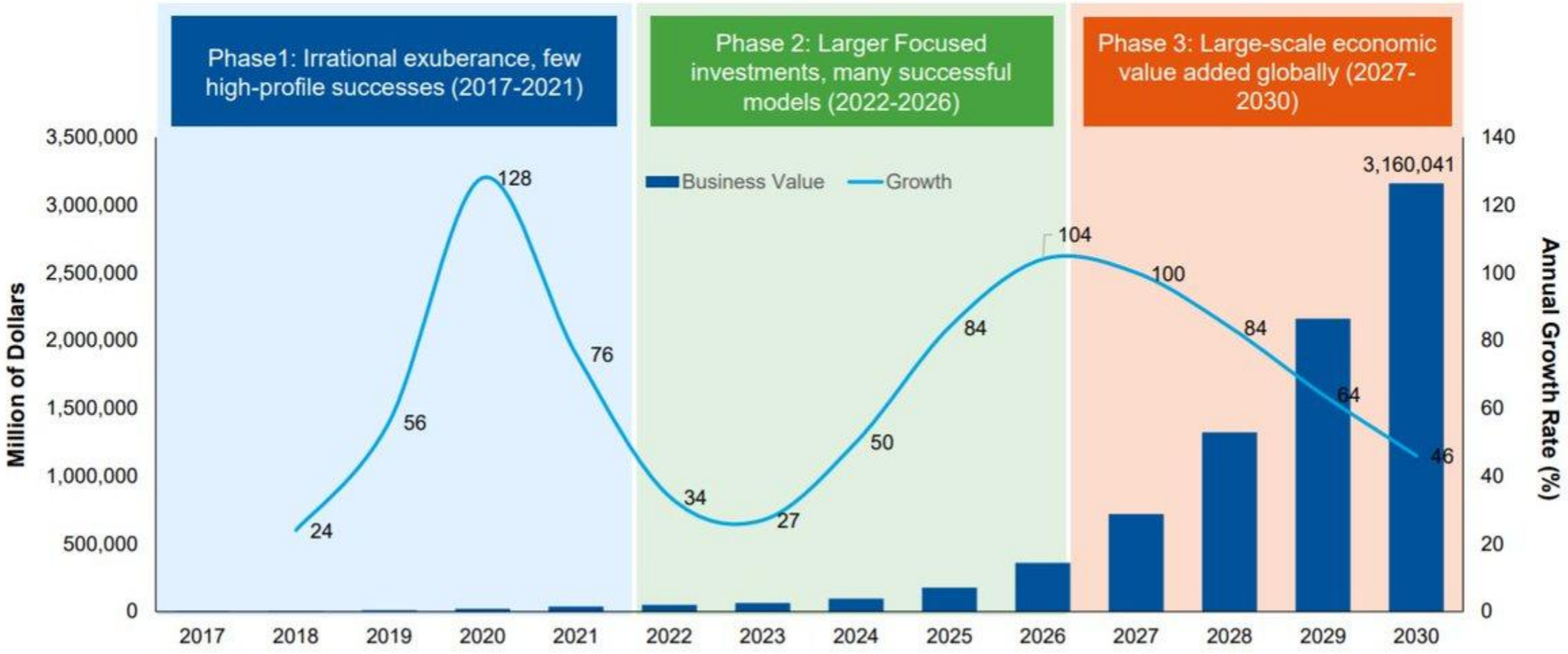


Source: Forecast: Blockchain Business Value, Worldwide, 2017-2030

Gartner

PUC Minas

Business Value-Add of Blockchain: $3.1 Trillion by 2030



PUC Minas

“Levará anos para blockchain transformar os negócios, mas a jornada já começou.”

(Marco Iansiti & Karim R. Lakhani)

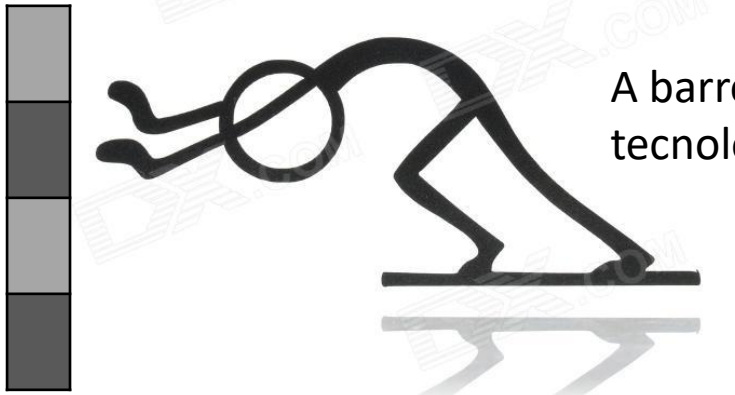
“Blockchain irá revolucionar os negócios e redefinir empresas e economias.”

Tecnológica

Governamental

Organizacional

Social



A barreira para a revolução das tecnologias inovadoras

PUC Minas

A crise de 2008 atingiu seu ápice com o colapso do Lehman Brothers em 15 de setembro.

A origem do Blockchain

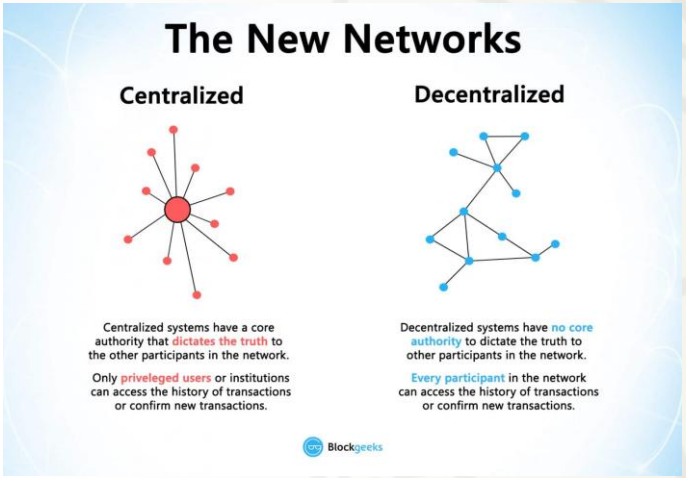
Seis semanas depois, Satoshi Nakamoto publicou um artigo onde propunha um sistema de pagamentos seguro, através de uma moeda digital, sem a intermediação de terceiros.

https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

PUC Minas

Bitcoin, a 1ª plataforma de Blockchain

- Pilares
  - Descentralização
  - Transparência
  - Imutabilidade
- Tecnologias de suporte
  - Hash criptográfico
  - Chaves públicas e privadas
  - Assinatura digital



TxHash	Block	Age	From	To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	0x2bdc9191de5c1b...	0,004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...	0xf14cb3acac7b230...	0,744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	0x2d42ee86390c59...	0,016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	0xd39681bb0586fb...	0,01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	0x8a91cac422e55e...	0,029594 Ether	0.000294

PUC Minas

Bitcoin, a 1ª plataforma de Blockchain

- Ao contrário das moedas tradicionais, Bitcoin não possui uma autoridade monetária central para monitorar, verificar e aprovar transações e gerenciar a oferta de moeda.
- Bitcoins não são impressos como dólares, mas "*minerados*" por computadores ao redor do mundo.
- *Minerar* significa usar a força computacional para resolver um problema matemático de difícil solução, mas de fácil verificação. A isso se chama prova de trabalho.
- A *mineração* garante a segurança do sistema, gerando novos bitcoins e recompensando os *mineradores*.

O que é Blockchain?

Blockchain é um registro distribuído e “imutável” que facilita o processo de gravação de transações e rastreamento de ativos.

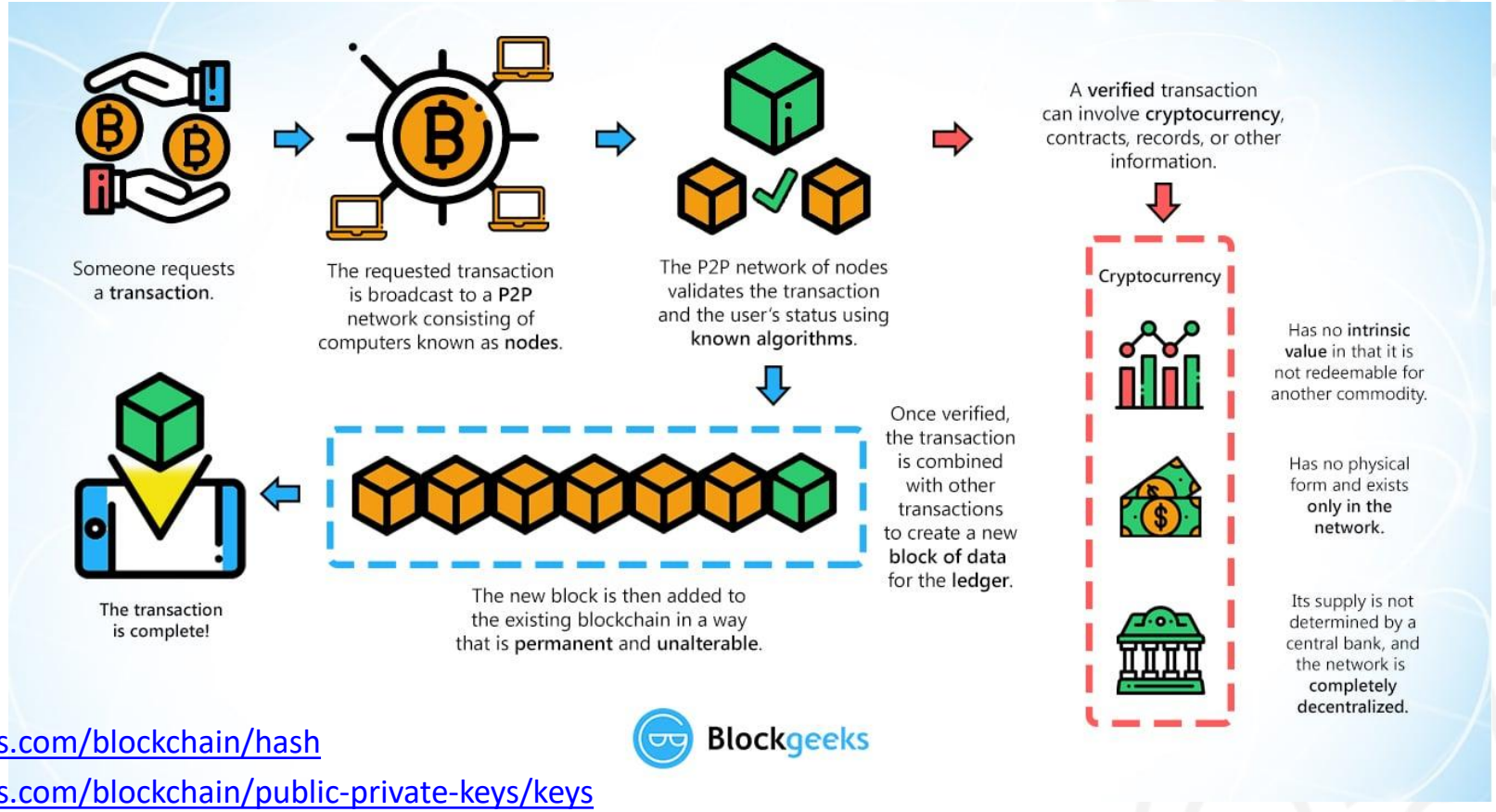
À medida que cada transação ocorre e as partes concordam com os detalhes, ela é codificada em um bloco de dados e assinada digitalmente.

Cada bloco é conectado ao seu antecessor e ao seu sucessor, criando assim uma cadeia irreversível e imutável.

O encadeamento de blocos impede que qualquer bloco seja alterado ou que um bloco seja inserido entre dois blocos existentes.

PUC Minas

Por dentro do Blockchain



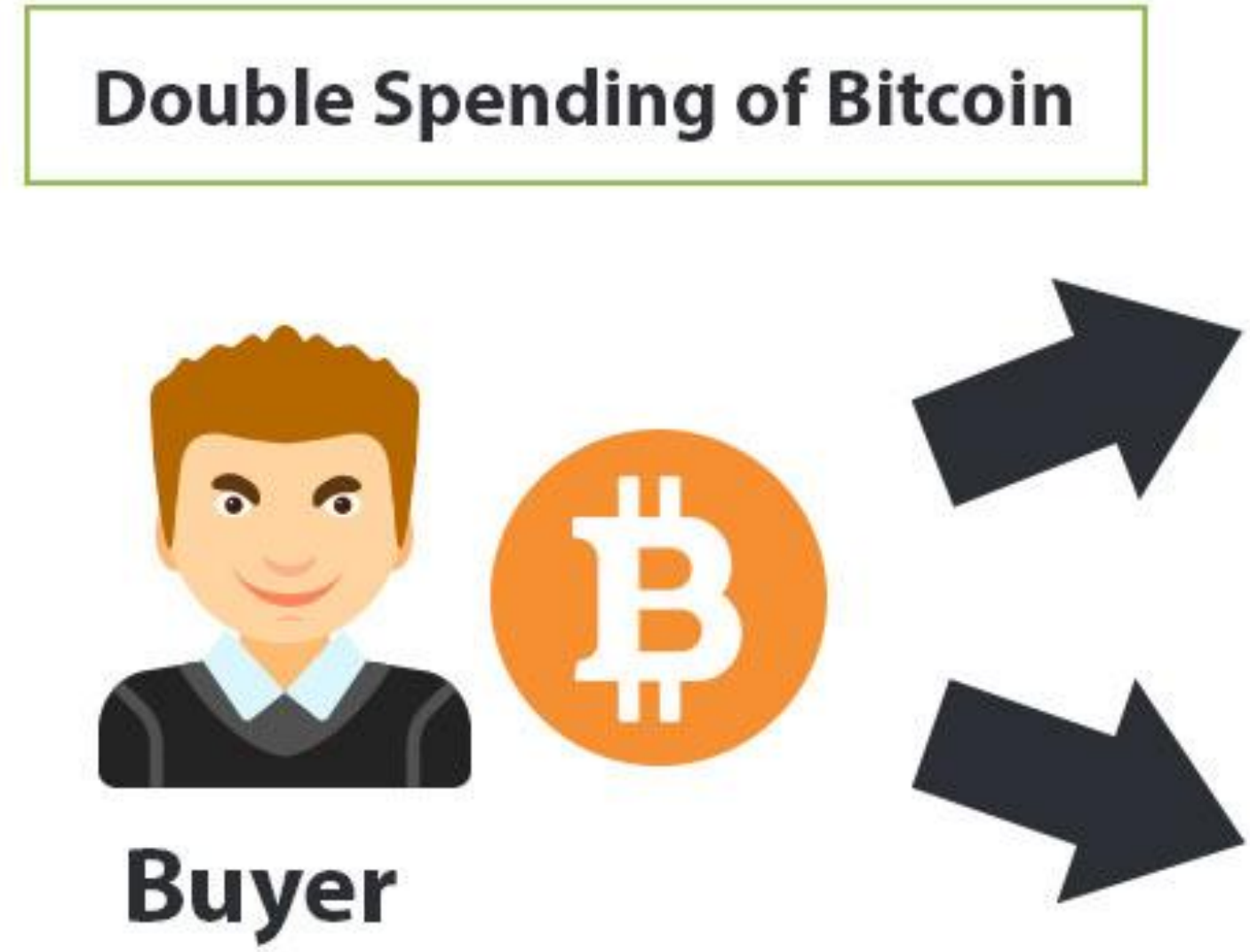
https://anders.com/blockchain/hash

https://anders.com/blockchain/public-private-keys/keys

PUC Minas

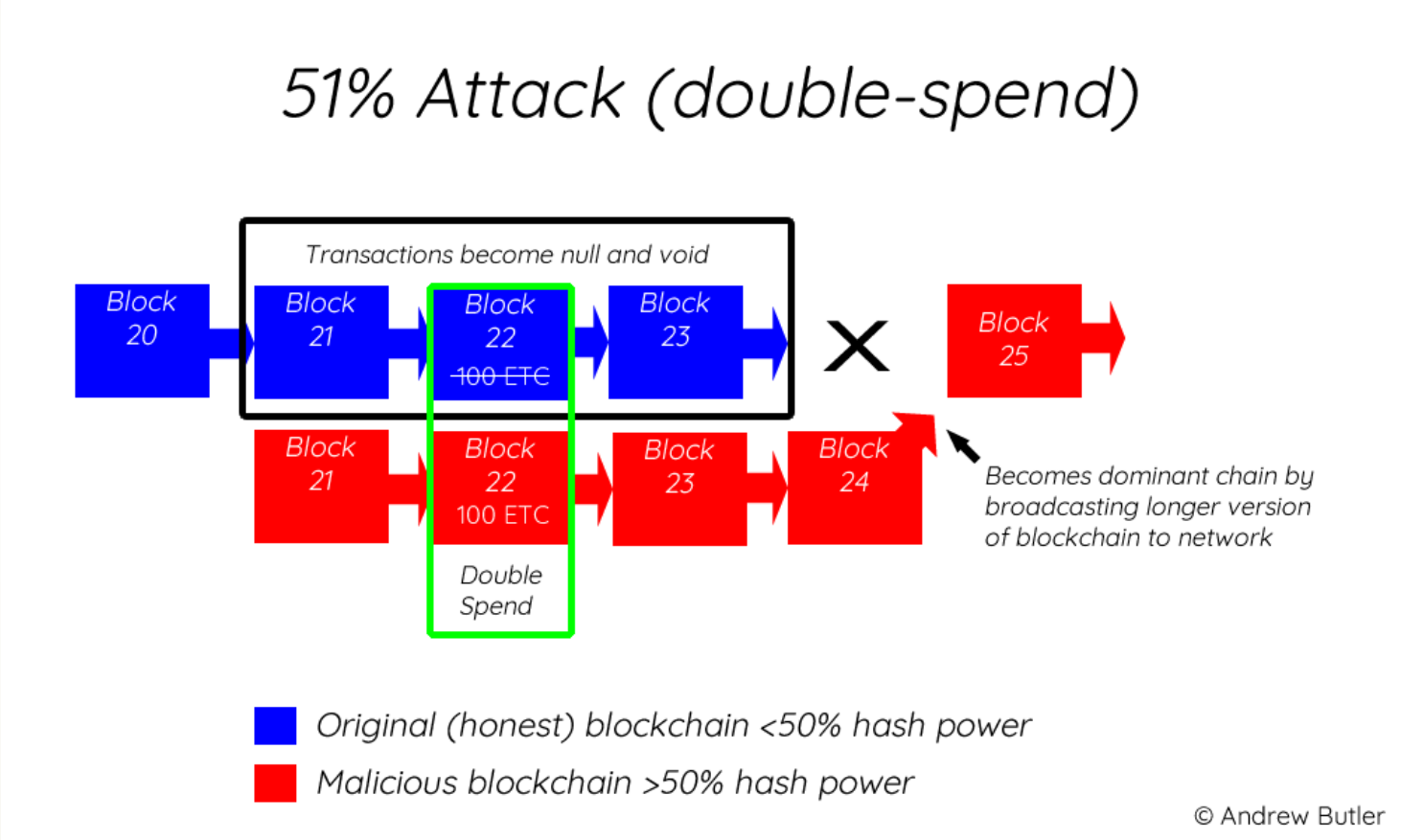
O problema do duplo gasto

- Duplo gasto é o risco de uma criptomoeda ser gasta duas vezes.
- É um problema comum a ativos digitais porque informações digitais podem ser reproduzidas com mais facilidade do que ativos físicos (ex.: moeda digital x moeda fiduciária).



É possível um duplo gasto?

- Um duplo gasto exigiria um ataque à rede modificando a cadeia de blocos.
- Seria necessário obter 50% + 1 do poder de processamento da rede para garantir o **consenso** de que a cadeia comprometida é a correta.



PUC Minas