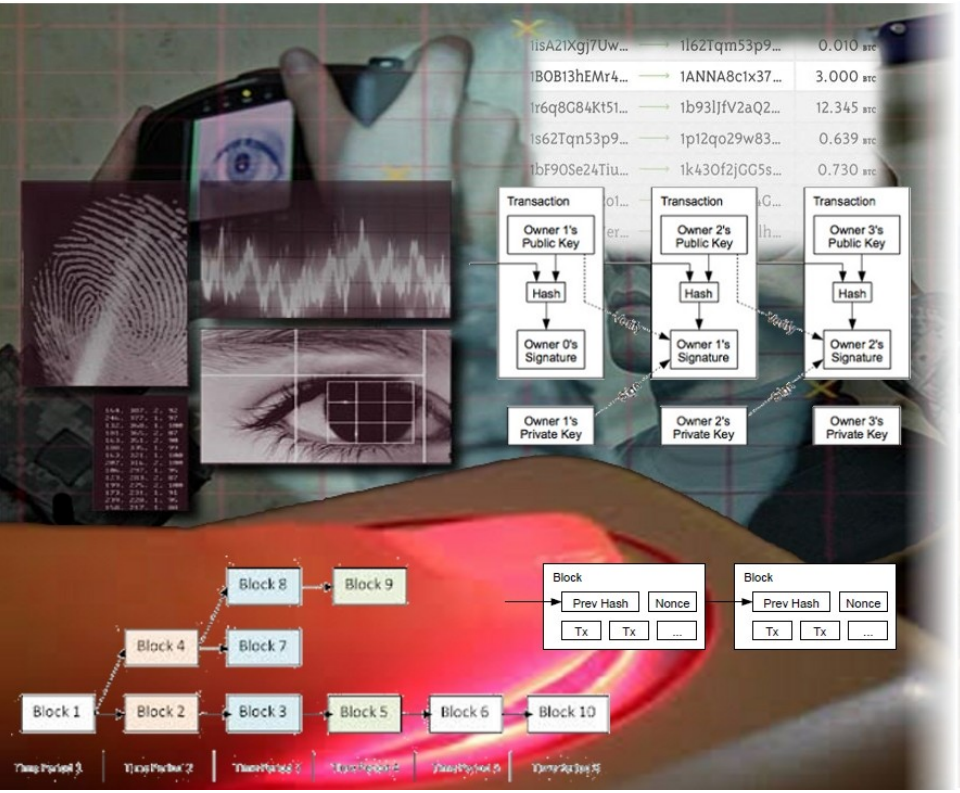


Criptomoedas: Possíveis Futuros

II BitConf, São Paulo, SP – 1/11/2014

Pedro A. D. Rezende

Ciência da Computação - Universidade de Brasília

pedro.jmrezende.com.br/sd.php

1. Criptomoedas e contabilidade pública

Conceitos, Exemplos, Relações

Moeda Corrente

- Definições:

[Wikipedia] http://www.techopedia.com/definition/27531/cryptocurrency

Meio de troca (*medium of exchange*) comum, usado para intermediar negócios e comércio sem as limitações e inconveniências do escambo.

Funções ou propriedades características ou ideais:

- *Métrica de valor para trocas*
- *Reconhecibilidade*
- *Divisibilidade*
- *Transportabilidade*
- *Utilidade constante*
- *Baixo custo de preservação*
- *Resistência à falsificação*
- *Alto valor relativo a volume e peso (escassez controlada)*

Moeda *fiat*

- Definição:

[Investopedia] www.investopedia.com/terms/f/fiatmoney.asp

Moeda corrente **oficial** (*legal tender*), i.e. tida como meio de pagamento para obrigações legais e financeiras (impostos, etc), emitida sem lastro em bens (p. ex., metal nobre), de valor baseado em demanda e oferta.

- Lastro de valor em moeda *fiat*: [*fiat* = latim para "deve ser"]

Crença na capacidade da autoridade emissora coletar impostos na moeda que intermedeia negócios e comércio em sua jurisdição;

ou

na capacidade da autoridade emissora impor demanda por sua moeda em negócios e comércio fora de sua jurisdição. [i.e., poderio militar]

Segurança criptográfica

- Para moedas virtuais, como pode ser?

http://blog.cryptographyengineering.com/2012/05/future-of-electronic-currency.html

Para uma **moeda virtual** (*digital currency*) servir como meio de pagamento, tendo sido emitida sem suporte (papel) ou lastro (ouro, prata, etc) físico, seu valor de troca (baseado em demanda e oferta) precisa ter lastro em propriedades intrínsecas. As oferecíveis por **criptografia** são >

> ***Métrica de valor para trocas*** [1]

> ***Reconhecibilidade*** [1]

- *Divisibilidade*

- *Transportabilidade*

versatilidade

- *Utilidade constante*

- *Baixo custo de preservação*

> ***Resistência à falsificação*** [2]

> ***Escassez controlada*** [2]

1- via autenticação

2- via protocolo para *public ledger + proof of work*

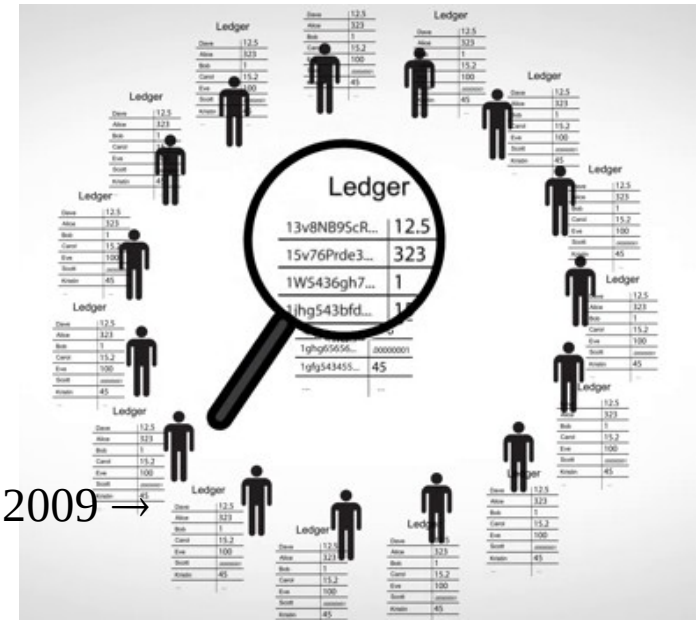
1. Contabilidade pública

- Como pode ser, no virtual?

Também de forma distribuída: https://bitcoin.org/bitcoin.pdf

Um livro-caixa digital, compartilhado entre usuários da moeda (*public ledger*), registra as transações. Pagador e recebedor são pseudonimizados por suas chaves públicas (***addresses***); as transações registradas num bloco encadeado ao *ledger* (***blockchain***) são consideradas simultâneas.

Livro-caixa em papel, 1823 ↑



Blockchain: ledger da rede Bitcoin, desde 2009 →

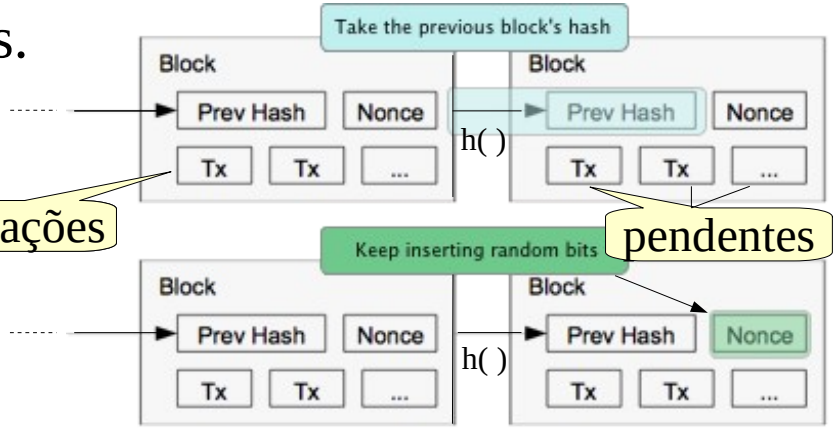
Atualização contábil

- Como pode ser, em um *public ledger* virtual?

Block chaining: https://bitcoin.org/bitcoin.pdf

Um novo bloco é encadeável ao *blockchain* quando um novo "número precioso" **N** é encontrado (minerado), capaz de "fechar" uma lista de transações pendentes com a correta "costura" no *ledger* (*proof of work*). Cada **N** vale hoje 25 novos bitcoins.

Páginas pré-costuradas e numeradas, preenchidas pela ordem. ↑



Blocos encadeáveis em tempo real →
(critério da maior cadeia subsequente)

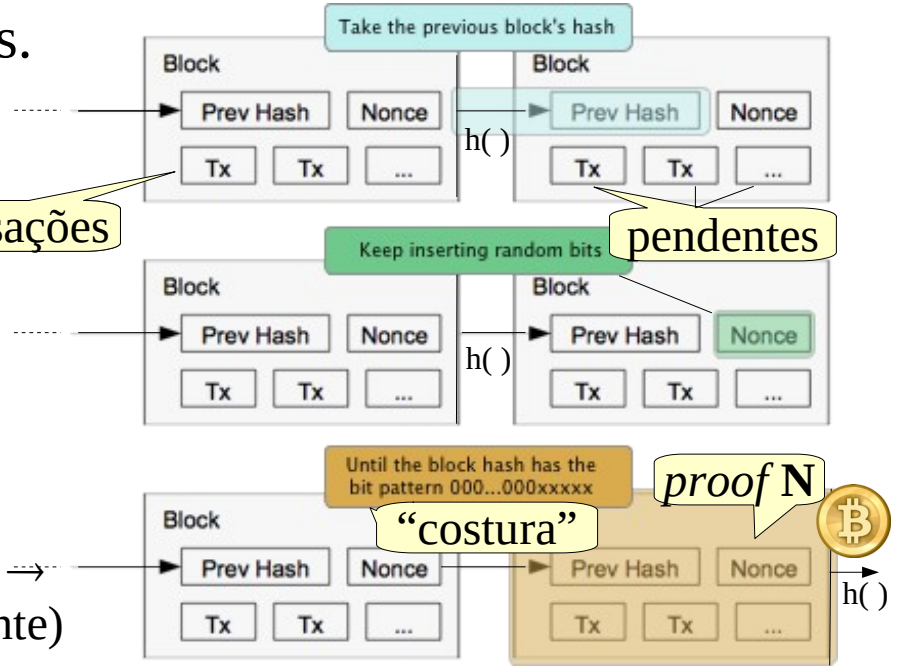
Atualização contábil

- Como pode ser, em um *public ledger* virtual?

Block chaining: https://bitcoin.org/bitcoin.pdf

Um novo bloco é encadeável ao *blockchain* quando um novo "número precioso" **N** é encontrado (minerado), capaz de "fechar" uma lista de transações pendentes com a correta "costura" no *ledger* (***proof of work***). Cada **N** vale hoje 25 novos bitcoins.

Páginas pré-costuradas e numeradas, preenchidas pela ordem. ↑



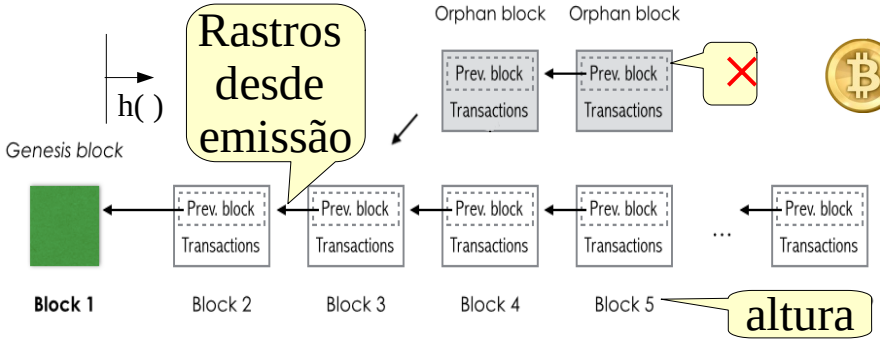
Blocos encadeáveis em tempo real →
(critério da maior cadeia subsequente)

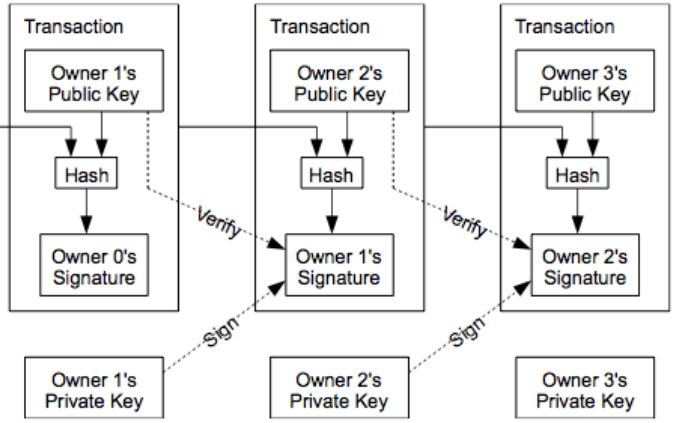
Validação contábil

- Como se valida transações na Blockchain? https://freedom-to-tinker.com/blog/felten/understanding-bitcoins-transaction-malleability-problem/

De forma distribuída: *"Votação" pela maior cadeia subsequente.*

Com moeda virtual, o risco equivalente ao de cheque sem fundo é o de se pagar várias vezes com a mesma quantia (*double spending*). Na rede Bitcoin, a estrutura Tx (*Transaction*) e a "votação" da cadeia o limitam.





Restam problemas de maleabilidade (ex: Mt Gox)

Moeda corrente vs. Dinheiro

[Von Mises] **Moeda corrente** é uma coisa,
Dinheiro é outra coisa:

} *ambas necessárias numa economia*

- **Moeda corrente** (*currency*) é métrica de valor **através do espaço**: aquilo que opera como meio de troca para bens intercambiáveis;

- **Dinheiro** (*money*) é reserva de valor **através do <u>tempo</u>**: aquilo que se retém para poupança ou negócio futuro.

Moeda corrente vs. Dinheiro

[Von Mises] **Moeda corrente** é uma coisa,
Dinheiro é outra coisa:

} *ambas necessárias numa economia*

- **Moeda corrente** (*currency*) é métrica de valor **através do espaço**: aquilo que opera como meio de troca para bens intercambiáveis;

- **Dinheiro** (*money*) é reserva de valor **através do <u>tempo</u>**: aquilo que se retém para poupança ou negócio <u>futuro</u>.

?

Moeda corrente vs. Dinheiro

[Von Mises] **Moeda corrente** é uma coisa,
Dinheiro é outra coisa:

} *ambas necessárias numa economia*

- **Moeda corrente** (*currency*) é métrica de valor **através do espaço**: aquilo que opera como meio de troca para bens intercambiáveis;

- **Dinheiro** (*money*) é reserva de valor **através do <u>tempo</u>**: aquilo que se retém para poupança ou negócio futuro.

características

> *Métrica de valor para trocas* [1]
> *Reconhecibilidade* [1, *]
- *Divisibilidade* [2]
- *Transportabilidade*

} versatilidade

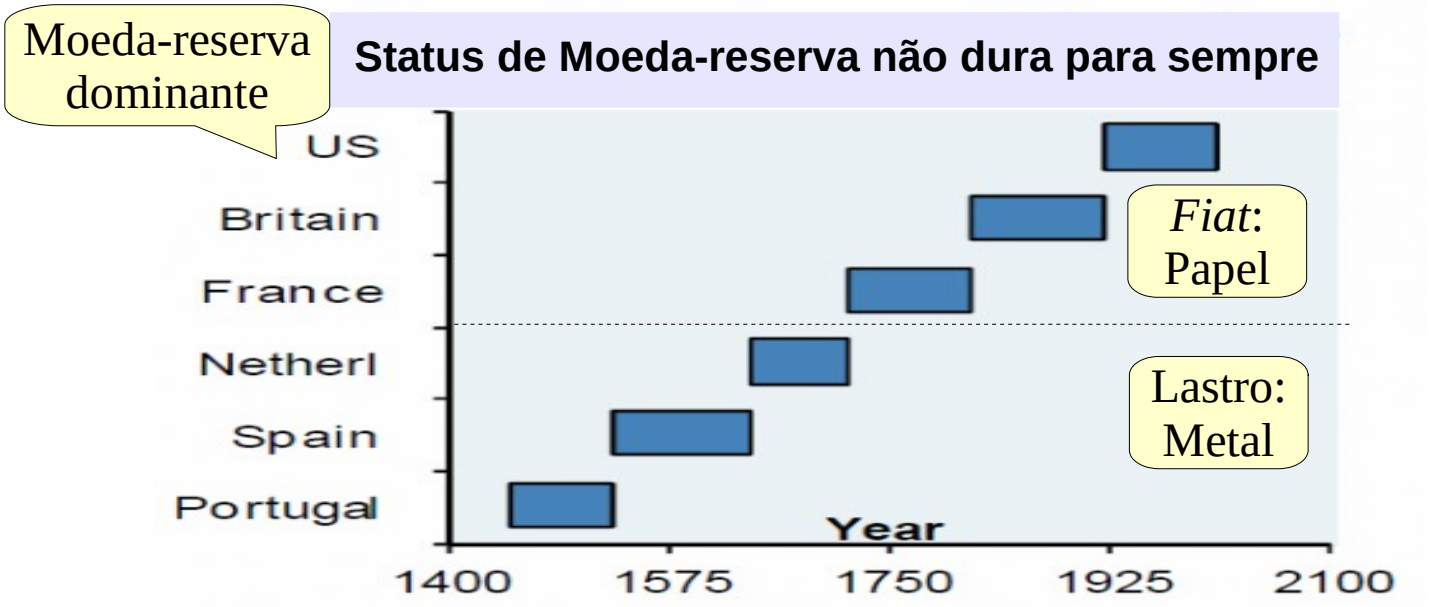
- *Utilidade** *<u>constante</u>*
- *Baixo custo de preservação*
> *Resistência à falsificação* [1, 2]
> *Escassez <u>controlada</u>* [2]

1- via autenticação 2- via protocolo *- via norma legal ou cultural >- tb via cripto

Moedas Globais Proprietárias

Moedas controladas por banco central de potência dominante tendem a assumir a função de reserva de valor, i.e. "**dinheiro global**", até que inflação e regulamentação tendenciosa induzem migração da função:

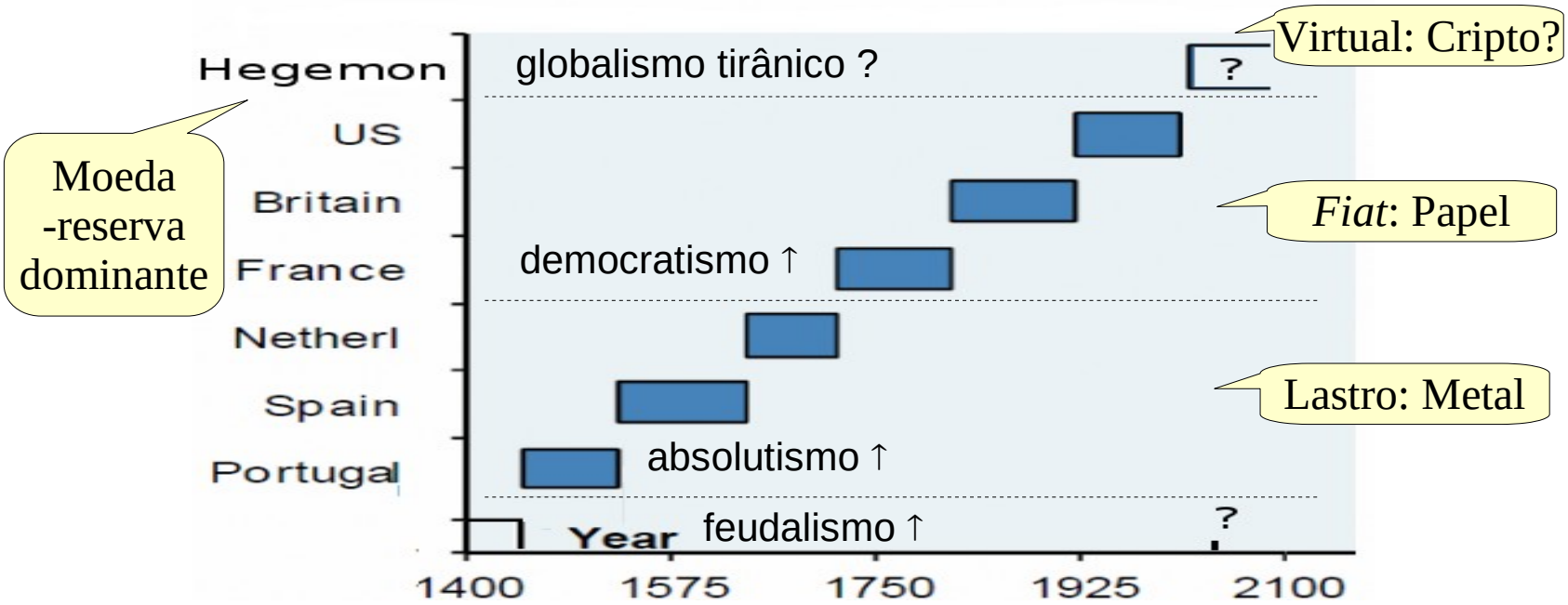
[Von Mises] www.zerohedge.com/news/2013-10-13/chinas-official-press-agency-calls-new-reserve-currency



A História ensina?

Tecnologia para controle de moeda-reserva parece historicamente relacionada ao regime de poder dominante. Períodos de transição política ou tecnológica (imprensa, iluminismo, internet) parecem "resetar" o regime monetário prevalescente. Como será o próximo?

www.youtube.com/watch?v=Pz_mMlWx5wM



Ciberguerra como transição

- Ciberguerra é (pode ser entendida como) um processo de transição, uma espécie de **contrarrevolução digital,** cujo paradigma é:

  "*Como pode ser a virtualização destrutível*"

- Conforme entendida pelo economista neoliberal Joseph Schumpeter, uma forma – histórica – de "**destruição criativa**" [em "*Capitalismo, Socialismo e Democracia*", 1942]

Como surge a Ciberguerra

Evolução da Cibernética

Ciclo Década	Inovação principal	Paradigma: Como pode ser...
1940	Arquiteturas	a máquina programável?
1950	Transistores	a programação viável?
1960	Linguagens	a viabilidade útil?
1970	Algoritmos	a utilidade eficiente?
1980	Redes	a eficiência produtiva?
1990	Internet	a produtividade confiável?
2000	Cibercultura	a confiança virtualizável?
2010	Ciberguerra	a virtualização destrutível?

Como é travada a ciberguerra

[E. L. P., junho 2011] "...Assim como a guerra nuclear era a guerra estratégica da era industrial, a ciberguerra é a **guerra estratégica** da era da informação; e esta se tornou uma forma de batalha **massivamente destrutiva**, que diz respeito à vida e morte de nações...

Uma forma inteiramente nova, invisível e silenciosa, e que está ativa não apenas em conflitos e guerras convencionais, mas também se deflagra em atividades diárias de natureza política, econômica, militar, cultural e científica...

Os alvos da guerra psicológica na Internet se expandiram da esfera militar para a esfera pública... Nenhuma nação ou força armada pode ficar passiva e se prepara para lutar a guerra da Internet."

www.reuters.com/article/2011/06/03/us-china-internet-google-idUSTRE7520OV20110603

Com amplo espectro

investmentwatchblog.com/new-intel-report-states-iran-and-russia-are-combining-forces-to-cyber-attack-the-u-s-financial-system

New Intel Report States Iran And Russia Are Combining Forces To Cyber Attack The U.S. Financial System

March 4th, 2014

Cyprus has now approved the privatization bill which will allow the central bankers to loot the country.

NWO: evento *False-flag* para transição monetária e politica à nova ordem mundial?

investmentwatchblog.com/new-intel-report-states-iran-and-russia-are-combining-forces-to-cyber-attack-the-u-s-financial-system

Com arquiteturas de opressão

O calcanhar de aquiles das moedas virtuais é a conversibilidade com moedas de reserva tradicionais: o cartel proprietário dos banqueiros globalistas pode criminalizá-la

rt.com/usa/157552-defense-pentagon-bitcoin-terrorism/

RT QUESTION MORE. LIVE

US Defense Dept. analyzing Bitcoin as potential terrorism

Published time: May 08, 2014 03:26

Get short URL

The US Defense Department is conducting a counterterrorism program investigation of virtual currencies like Bitcoin and other new technologies, including smartphones and social media,

Tags

Bitcoin. Currencies. Military. Terrorism. USA

Run by the Combating Terrorism Technical Support Office (CTTSO), a division of the Pentagon that analyzes terrorism and irregular warfare capabilities, the program recently ended its open call for agency projects, including one for *"innovative...solutions to develop and/or enhance new concepts and constructs for understanding the role of virtual currencies"* in financing threats to the US.

"The introduction of virtual currency will likely shape threat finance by increasing the opaqueness, transactional velocity, and overall efficiencies of terrorist attacks," the memo stated.

The anonymity offered by virtual currencies is a top point of concern for law enforcement as it aids in the formation of illicit operations like Silk Road, a digital black market thought to be closed down in October

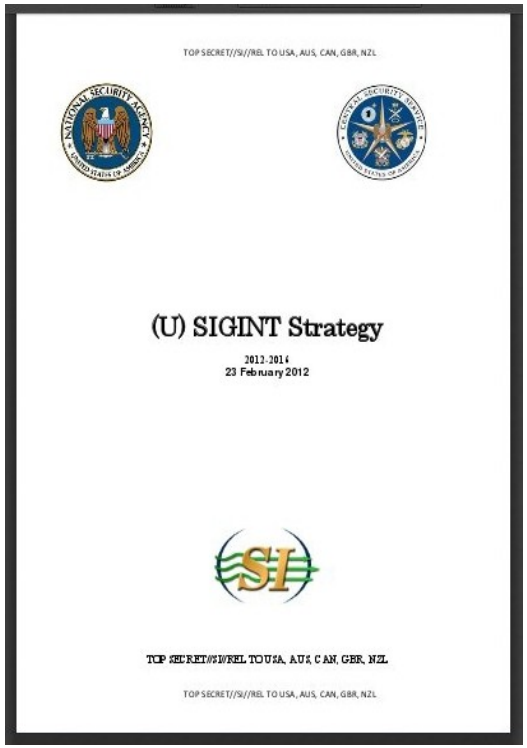
Com estratégias de conquista

Cerco e pilhagem virtual:

... os protocolos da Bitcoin – como os da Blockchain – podem também ser pilhados, pelo cartel dos banqueiros globalistas da NWO: virtualmente, por meio de patentes de software fajutas.

O nome do jogo...

Signals Intelligence - Planejamento 2012-2016 para **5 Olhos**:



s3.amazonaws.com/s3.documentcloud.org/documents/838324/2012-2016-sigint-strategy-23-feb-12.pdf

Vazado para o Wikileaks - Destaque para:

"2.1.3. (TS//SI//REL) *Counter indigenous cryptographic programs by targeting their industrial bases with all available SIGINT + HUMINT (Human Intelligence) capabilities*"

"2.1.4. (TS//SI//REL) *Influence the global commercial encryption market through commercial relationships, HUMINT, and second and third party partners* "

"2.2. (TS//SI//REL) *Defeat adversary cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere*"

Síndrome de Estocolmo Virtual

Síndrome de Estocolmo: "Reação psicológica observável em vítimas de sequestro, em que o refém mostra sinais de lealdade ao algoz, não obstante o perigo sob o qual o refém é colocado."

Virtual: O fim da privacidade na era digital é um perigo real?

- Os riscos alardeados como consequência disto são irreais?

Liberdade pode ser trocada por **proteção**?

Moral nietzcheana da nova ordem mundial:

[Benjamin Franklin] "*Quem troca um pouco de liberdade por mais sentimento de proteção não merece nem uma nem outra.*"

O emergente Hegemon

[Aldous Huxley, em Admirável Mundo Novo]

- *"Um Estado totalitário realmente eficiente seria um no qual os todo-poderosos mandantes da política e seus exércitos de executivos controlam uma população de escravizados que não precisam ser coagidos, porque eles adoram a sua servidão."*

Modelo do PNAC (*Project New American Century*):

en.wikipedia.org/wiki/Project_for_the_New_American_Century

O emergente Hegemon

[Aldous Huxley, em Admirável Mundo Novo]

- *"Um Estado totalitário realmente eficiente seria um no qual os todo-poderosos mandantes da política e seus exércitos de executivos controlam uma população de escravizados que não precisam ser coagidos, porque eles adoram a sua servidão."*

Modelo do PNAC (*Project New American Century*):

en.wikipedia.org/wiki/Project_for_the_New_American_Century

Modelo Bíblico (profecias para o tempo da grande tribulação):

Dn 11; Mt 24; 1Jo 2; Ap 7-13

Escatologia

- Interpretações da profecia sobre Marca da besta em Ap 13:

17 (transição para um novo regime monetário global)

- Interpretações da profecia sobre Gog e Magog em Ez 38, 39

(ofensiva de uma aliança militar entre Rússia, Turquia e Irã)

1- Parte da Sequência para o Armagedon em **Dn 11**
(Hal Lindsay, John Hagee, etc.)

Pré-tribuacionismo => após arrebatamento (*harpazo*)

2- Antes da 70ª Semana determinada sobre Israel em **Dn 9:26**
(Chuck Missler, Grant Jeffrey, etc.)

Pré-tribuacionismo => pré-arrebatamento