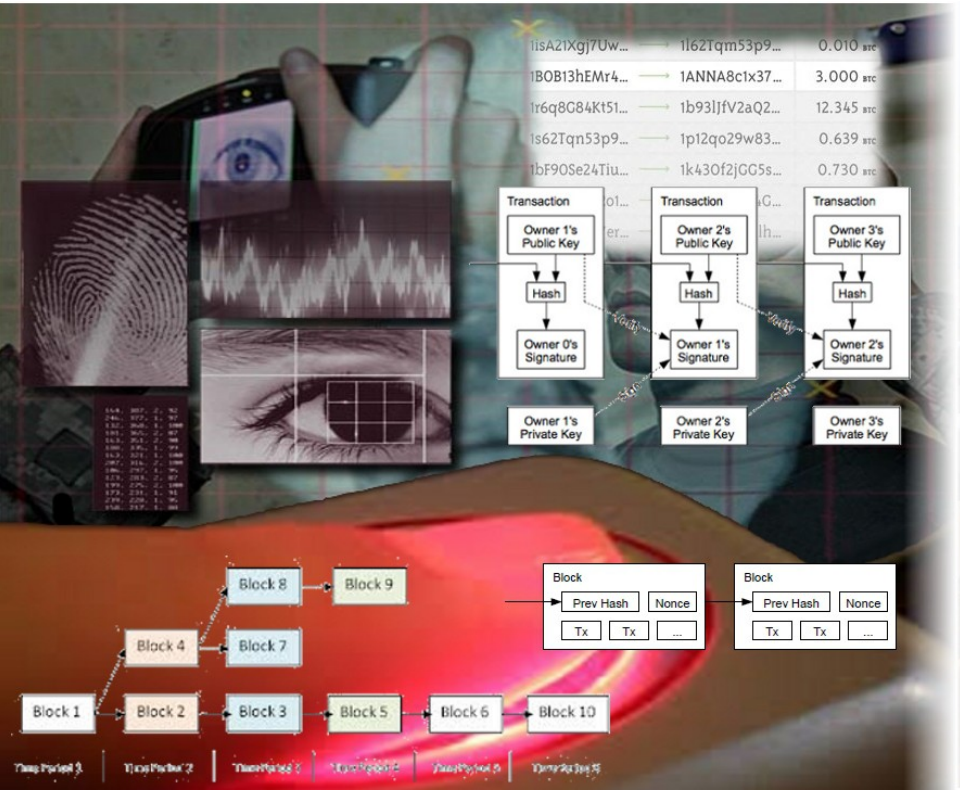


Criptomoedas: um fenômeno evolutivo?

18º FISL, Porto Alegre, RS – 13/07/2018

Pedro A. D. Rezende

Ciência da Computação - Universidade de Brasília

www.cic.unb.br/~rezende/sd.php

Roteiro

1- Evolução das **Tecnologias monetárias**

2- Que é **Cripto-isso/aquilo?**
E **Moeda, Dinheiro, Valor?**

3- Reflexões sobre **Controle e Futuro;** Debate

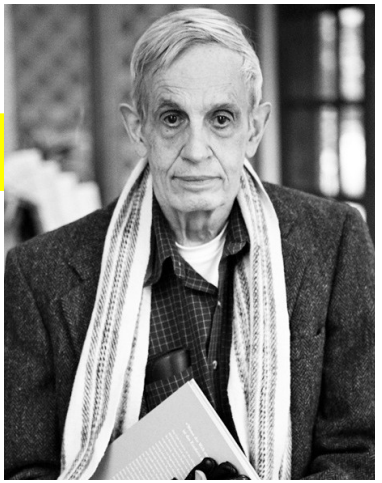
1. Evolução das Tecnologias Monetárias

Conceitos e perspectivas

1. O papel social do dinheiro

John F Nash Jr en.wikipedia.org/wiki/John_Forbes_Nash_Jr.

Pioneiro da Teoria dos Jogos, autor de "*Dinheiro Ideal*"



Peter Badge / Typos1

Desenvolveu o tema *papel do dinheiro na sociedade* sob a premissa de que as pessoas podem ser tão controladas e motivadas pelo dinheiro que podem perder a capacidade de racionar logicamente a respeito (do conceito).

Criticou grupos de interesse que promovem doutrinas baseadas na economia keynesiana, que permitem manipulações de curto prazo e táticas de endividamento, as quais em última análise prejudicam as moedas correntes

Reconheceu que seus pensamentos se assemelham ao do economista e filósofo político Friedrich Hayek (sobre o do conceito de dinheiro) e no ponto de vista – atípico – sobre a função das autoridades (esp. monetárias).

1. Nove Escolas do pensamento econômico

- Conceitos: [Ha-Joon Chang] businessinsider.com/table-different-schools-of-economics-2014-6

Teoria : Economia é	Composta de	Movida por	Indivíduos são	Domínio principal
Clássica	Classes sociais	Acúmulo de capital (investimentos)	Egoístas e racionais (por classe)	Produção
Neoclássica	Indivíduos	Escolhas individuais	Egoístas e racionais	Transações e consumo
Marxista	Classes	Acumulo de capital conflito, progresso	Egoístas e racion. exceto socialistas	Produção
Desenvolvimentista	ênfase em Classes	Acúmulo de capacidade produtiva	[indeterminada]	Produção
Austríaca (von Mises, F. Hayek)	Indivíduos	Escolhas pessoais, tradições	Egoístas e semirracionais (layers)	Transações
Shumpeteriana	[indeterminada]	Inovações técnicas	[indeterminada]	Produção
Keynesiana (Neoliberal)	Classes	[ambígua]	Semirracionais	[ambígua]
Behaviorista / *Institucionalista*	Indivíduos e instituições	Interações entre indiv. e instituições	Instinto + hábito + crença + razão	ênfase em Produção

- Evolução adaptativa:

A Escola Austríaca é que vem mostrando maior poder explicativo e preditivo sobre os fenômenos em torno das criptomoedas e criptoativos.

1. Teoria dos Jogos

- Definição: [Wikipedia] en.wikipedia.org/wiki/Game_theory

Estudo de modelos matemáticos que abordam situações de conflito e cooperação entre agentes capazes de decisões racionais inteligentes.

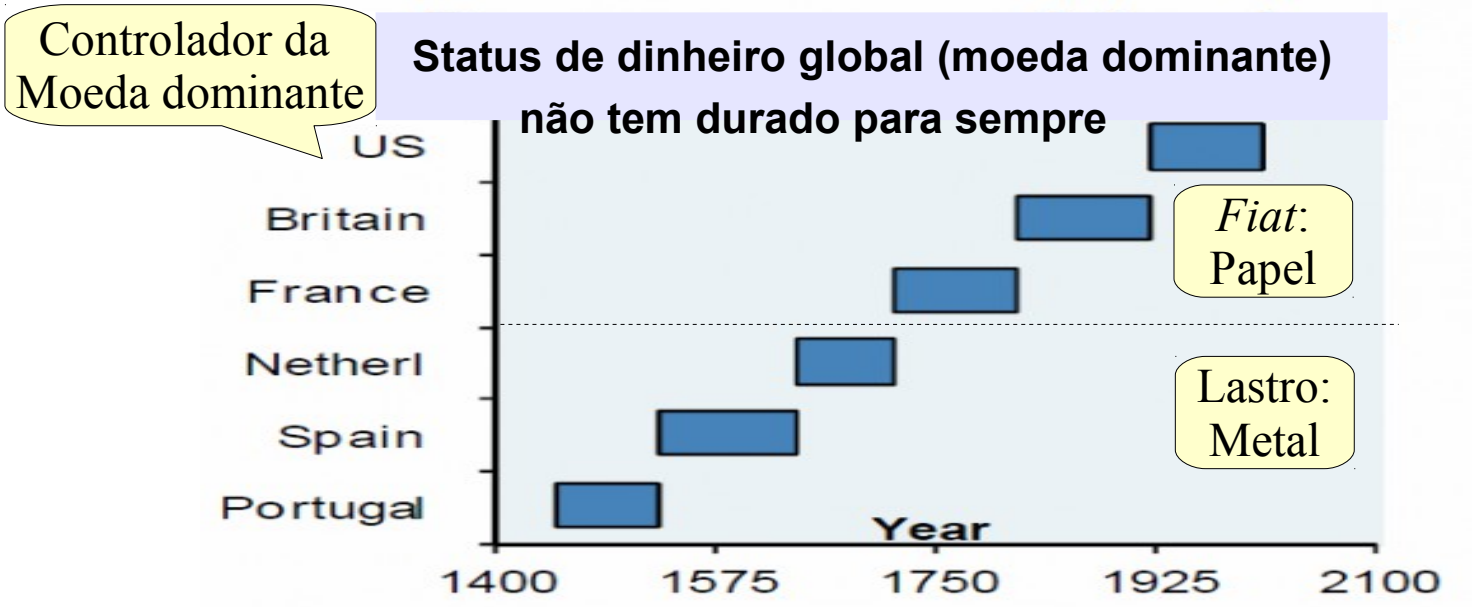
- Evolução:

1713	[rudimentos] aplicação a um jogo de cartas
1838	[rudimentos] aplicação a estratégias fiscais
1928	[teoria matemática] jogos de/com estratégia (von Neumann)
1944 >	aplicação a teorias econômicas quantitativas (11 prem. Nobel)
1950s>	aplicação a estratégias bélicas com armamentos nucleares
1960s>	aplicações na ciência política e na filosofia (jogos infinitos)
1970s>	aplicações à biologia adaptativa/evolutiva e à computação
2008 >	protocolos para criptomoeda descentralizada (Blckchn + PoW)

1. Moedas Dominantes

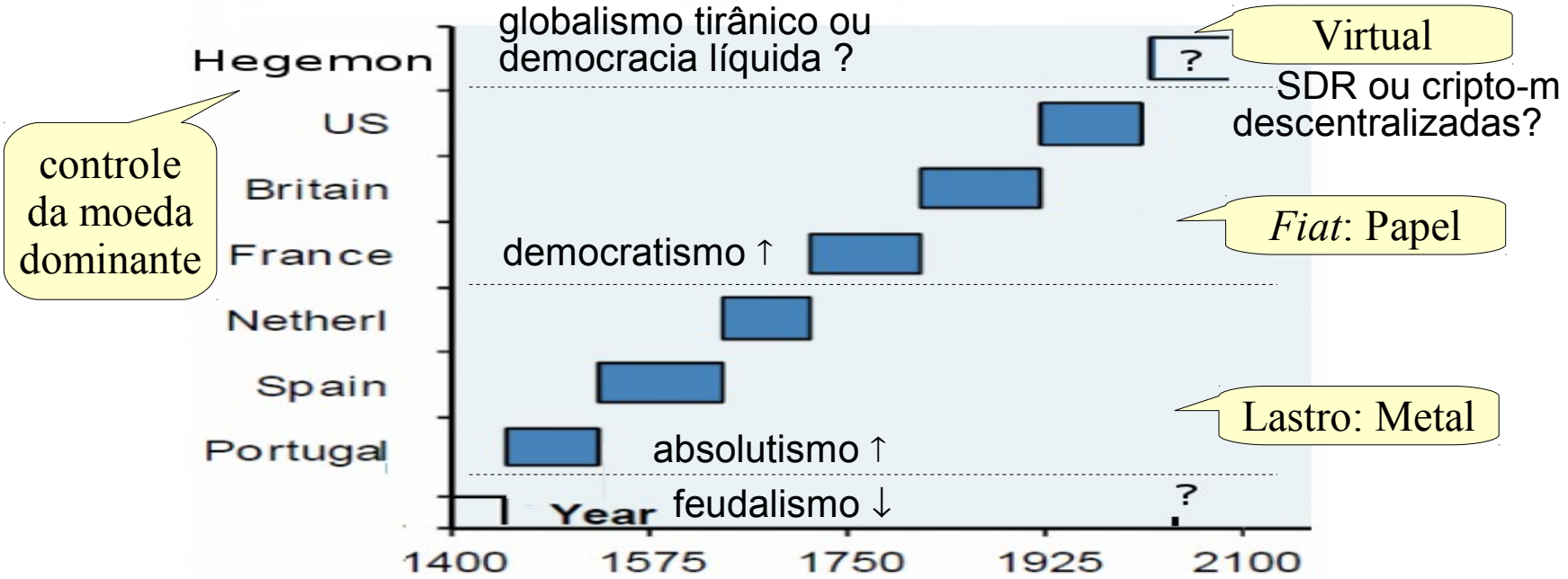
Moedas controladas por banco central de potência dominante tendem a assumir a função de reserva de valor, i.e. "**dinheiro global**", até que inflação e regulamentação tendenciosa induzem migração da função:

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



1. A História ensina?

Tecnologia para controlar a moeda dominante parece historicamente relacionada ao regime de poder hegemônico imperante. Períodos de transição tecnológica (imprensa, eletricidade, internet) parecem precipitar um *reset* na ordem financeira e regime prevalescentes. Como serão os próximos? www.youtube.com/watch?v=Pz_mMlWx5wM



1.*Reset* financeiro e terrorismo econômico

Vários eventos financeiros atuais – QEs, Z/NIRP, AIIB, *Decashing*, Sanções, etc – indicam importante reorientação nos rumos do futuro.

Os donos do poder farão tudo a seu alcance para adiar um colapso, e nisso estão sendo pró-ativos.

O mundo está sufocado em dívida intransponível; se nada for feito, o cenário se desdobra em hiperinflação global. O resultado desse novo rumo inclui desagregação e caos; Quando o desabastecimento e a desobediência civil dispararem e o caos social se espallhar, governos se tornarão ditatoriais na tentativa de salvarem a si mesmos. Alguns acreditam que operações de *guerra híbrida* (no afganistão, síria, ucrânia, iemen, grécia, venezuela) são preliminares em **preparação a um vindouro *reset* financeiro**

modernsurvivalblog.com/current-events-economics-politics/the-crash-the-reset-martial-law-by-this-time-next-year

1. Modelo bélico dos Bancos Centrais

James Turk, financista jamesturkblog.blogspot.com.

Forma de guerra que tem sustentado a ordem financeira mundial nos últimos 400 anos: concentradores financeiros maiores emitem moeda *fiat* sem lastro cuja demanda como meio de pagamento é forçada militarmente sobre agentes, mercados e estados fora de sua jurisdição

Quem emite a moeda na qual é originada sua própria dívida então colhe, em atividade econômica depreciada, renda por dívidas dos que não emitem a moeda de origem da sua. Funciona enquanto a quantia emitida para cobrir as próprias superar os gastos políticos e militares necessários para sustentar essa coerção. Que historicamente tem durado entre 70 e 200 anos.

Quando a eficácia do modelo se esgota, entra-se numa fase crítica do ciclo capitalista que a Escola Schumpeteriana chama de ‘destruição criativa’

1. Modelo bélico dos Bancos Centrais

www.blacklistednews.com/Big_Banks_Want_Power_to_Declare_Cyber_War/

BLACKLISTED NEWS

Congressman Grayson tweets:

Ex-NSA chief Keith Alexander wants to form a joint WH-bank war council. So now Wall Street gets to declare war?

BIG BANKS WANT POWER TO DECLARE CYBER WAR

Published: July 9, 2014 Bloomberg reports:

MERGER OF BIG BANKS AND NATIONAL SECURITY POWER … WHAT COULD POSSIBLY GO WRONG?

> Wall Street's biggest trade group has proposed a government-industry cyber war council to stave off terrorist attacks that could trigger financial panic by temporarily wiping out account balances, according to an internal document.
>
> The proposal by the Securities Industry and Financial Markets Association, known Sifma, calls for a committee of executives and deputy-level representatives from at least eight U.S. agencies including the Treasury Department, the National Security Agency and the Department of Homeland Security, all led by a senior White House official.

Um conselho de guerra híbrida formado pela Casa Branca e os maiores bancos do mundo – como quer ex-diretor da NSA – reeditaria o fascismo (na definição de Mussolini) como forma do regime hegemônico global

2. Dinheiro, moeda, valor, etc

Diferenças? Quais e como admitem virtualização criptográfica?

2. Cripto o quê?

Percepções:

Criptomoedas descentralizadas

[Wikipedia] **Valor** é uma relação entre uma necessidade e uma capacidade

Revolução !
Desintermediação financeira c/ *Open Blockchain + PoW*

Fraude !
Sem *valor* intrínseco, inútil bolha, esquema pirâmide

WTF ?
"O que está acontecendo?"
???


American Register

"*…It is doubtful if electricity will ever be* [*widely*] *used* [*because it was*] *too expensive to generate….*" Editorial do American Register, **29/3/1879**

[3 meses depois do lançamento da lâmpada, 3 anos antes da 1ª distribuidora de energia elétrica, 33 anos antes das casas e prédios utilizando à rede elétrica nos EUA ultrapassarem os 10%]

www.zerohedge.com/news/2018-06-30/bitcoin-soars-most-3-months-back-above-6000

2. Cripto o quê?

Fenômenos:

Revolução?
Latente: Desinter-. mediação c/ *Open Blockchain + PoW*

Novos tipos de fraude: sem valor viável, muitos esque-mas pirâmide

Evolução: Está também acontecendo! **...**

Imutabilidade com *block-chain* distribuída + prova de esforço (PoW) ou prova de interesse (PoS)

Contratos inteligentes, *Lighting Networks, Si-dechains, Tiered chains, Acyclic graphs, etc.*

Tokenização de ativos (DLT), Protocolos para *exchanges* (bolsas) des-centralizadas (ex: 0X), Aplicativos autônomos distribuídos (DAO),etc

"*Criptocurrencies…can not assume the funcions of money* [*3 purposes*]..."
Agustin Carstens, chefe do BIS (o BC dos bancos centrais), **4/7/2018**

[9 anos depois do lançamento do Bitcoin e 7 meses depois das bolsas de futuros (ex: Chicago Mer-cantile Exchange) começarem a negociar com instrumentos de aposta em valores de criptomoedas]

cointelegraph.com/news/bis-chief-bashes-cryptocurrency-again-in-scathing-review-of-its-failure-as-money

2. Moeda corrente e Dinheiro

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

} *ambas necessárias numa economia*

- **Moeda corrente** (*currency*) é métrica de valor **aplicável no espaço**: aquilo que opera como meio de troca para bens intercambiáveis;

- **Dinheiro** (*money*) é métrica de valor **através do tempo**: aquilo que se retém para poupança ou negócio futuro.

?

Lei de Oresme/Gresham:
"bad money drives out good"

2. Virtualizáveis criptograficamente?

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

} *ambas necessárias numa economia*

- **Moeda corrente** (*currency*) é métrica de valor **aplicável no espaço**: aquilo que opera como meio de troca para bens intercambiáveis;

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

características

> *Métrica de valor para trocas* [1]

[**>**] *Reconhecibilidade* [1, *]

> *Divisibilidade* [2]

[**>**] *Transportabilidade*

} Versati-lidade

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

[ ]- requer hardware, energia, conexão TCP/IP

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

2. Moeda no tempo

Moeda *pode ser* dinheiro se for **estável no tempo**: Antes da invenção da imprensa, cunhagens reais (*seigniorage*) autenticavam a métrica de valor pelo peso de metal nobre no lastro físico da moeda corrente.

[E.Austr] http://austrianeconomics.wikia.com/wiki/Money_and_banking_in_Ancient_Rome

- **Depreciação do valor** (que causa inflação) já ocorria com as moedas romanas. Elas foram perdendo sua parte em cobre (*aes*, a partir de 212 AC), prata ou ouro (*denarium* e *aureus*, após 54 BC). Ficou mais fácil com moedas *fiat* impressas (a 1ª na dinastia Song da China, no sec. XI)

denarium

aureus

Jeng-Zi paper note

2. Moeda no tempo

Moeda *pode ser* dinheiro se for **estável no tempo**: Antes da invenção da imprensa, cunhagens reais (*seigniorage*) autenticavam a métrica de valor pelo peso de metal nobre no lastro físico da moeda corrente.

[E.Austr] http://austrianeconomics.wikia.com/wiki/Money_and_banking_in_Ancient_Rome

- **Depreciação do valor** (que causa inflação) já ocorria com as moedas romanas. Elas foram perdendo sua parte em cobre (*aes*, a partir de 212 AC), prata ou ouro (*denarium* e *aureus*, após 54 AC). Ficou mais fácil com moedas *fiat* impressas (a 1ª na dinastia Song da China, no sec. XI)

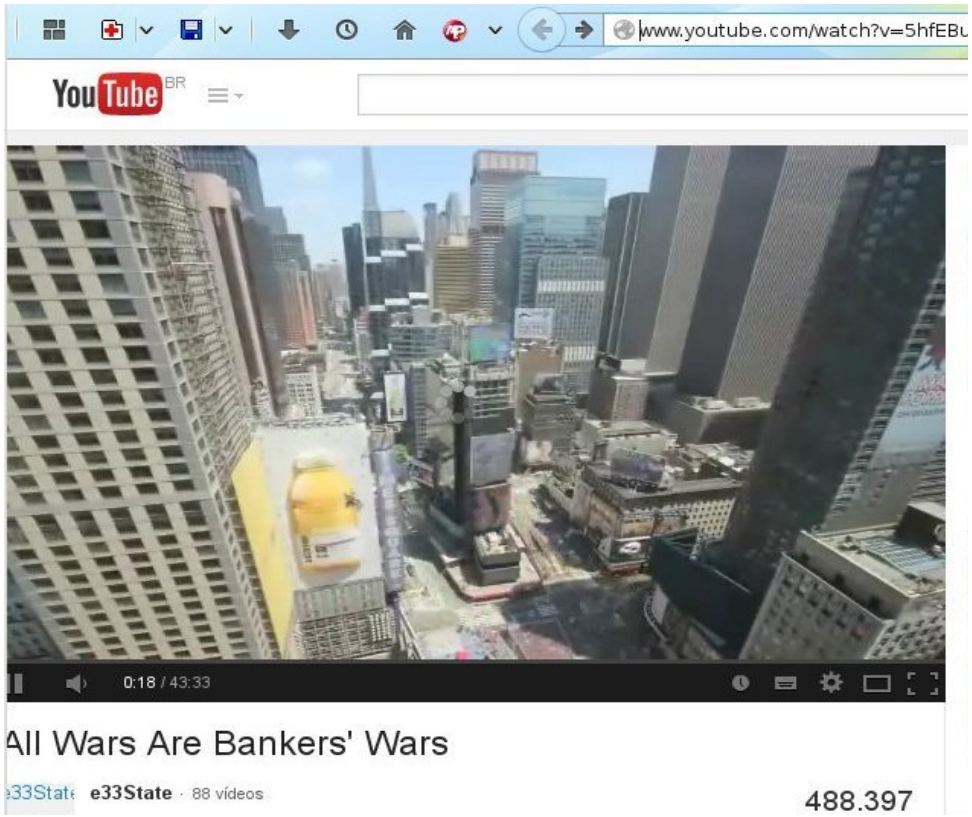
[Edward Griffin] tinyurl.com/cak346q#17 www.youtube.com/watch?v=lu_VqX6J93k

- Na Europa do sec. XV, grandes bancos coludiram com governos para criar "bancos centrais" (a exemplo do *Bank of England*, em 1694). Imprimindo moeda *fiat,* eles podem diluir com inflação (imposto indireto no tempo) a resistência de povos contra impostos exorbitantes (>43%).

3. Moedas *fiat* no tempo

[Michael Rivero, abril 2014] - www.youtube.com/watch?v=5hfEBupAeo4

Com o advento dos bancos centrais controlando a emissão, circulação e escassez de moedas *fiat*, todas as guerras se tornaram guerras de banqueiros. Elas começam com ataques de bandeira falsa, são financiadas pelos mesmos nos dois lados, e se tornaram ciber/híbridas.



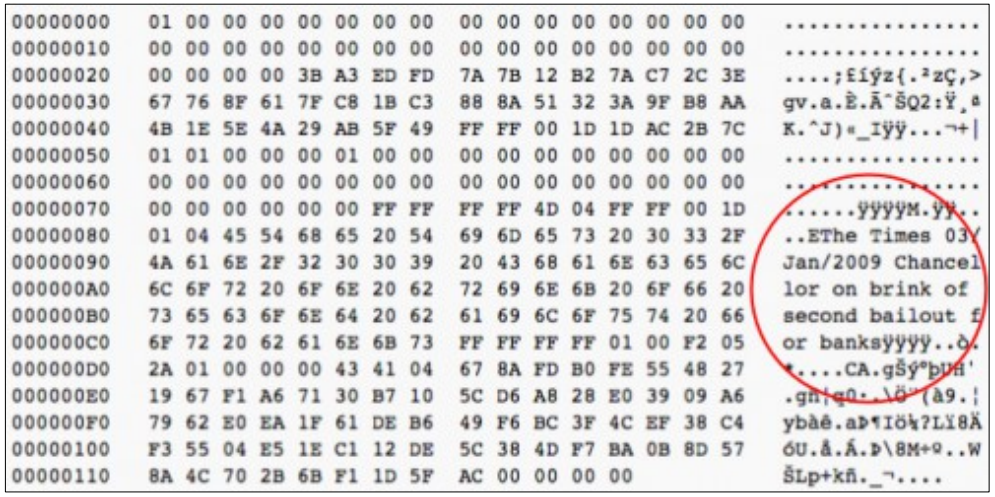
O verdadeiro *casus belli* é reter o controle em *resets* da ordem financeira, e induzir a 'destruição criativa' [Schumpeter]. Para sucesso na atual/próxima, precisam anular as criptomoedas descentralizadas

3. Reflexões sobre controle, futuro

Conhecendo nosso tempo (que está passando...)

3. Qual (foi) o propósito do Bitcoin?

No bloco gênese do blockchain do Bincoin, minerado por Satoshi Nakamoto em 3/1/2009 (lançamento), havia uma mensagem que se tornou conhecida na comunidade: Tirada do jornal *The Times* do mesmo dia, diz: "Chanceler à beira de segundo resgate dos bancos"



A mensagem pode ser vista como um comentário desfavorável acerca da natureza parasitária, instável e inflacionária do sistema bancário contemporâneo, bem como uma “declaração de princípio” do Bitcoin, a propiciar um meio de transferência equitativo, livre de qualquer instermediação financeira tradicional.

/www.zerohedge.com/news/2017-12-09/new-cme-bitcoin-futures-and-goldman-sachs-connection

3. Qual (será o) futuro c/após o Bitcoin?

Mike Goldin, ConsenSys, 28/07/2017 - Manifesto dos Criptossistemas

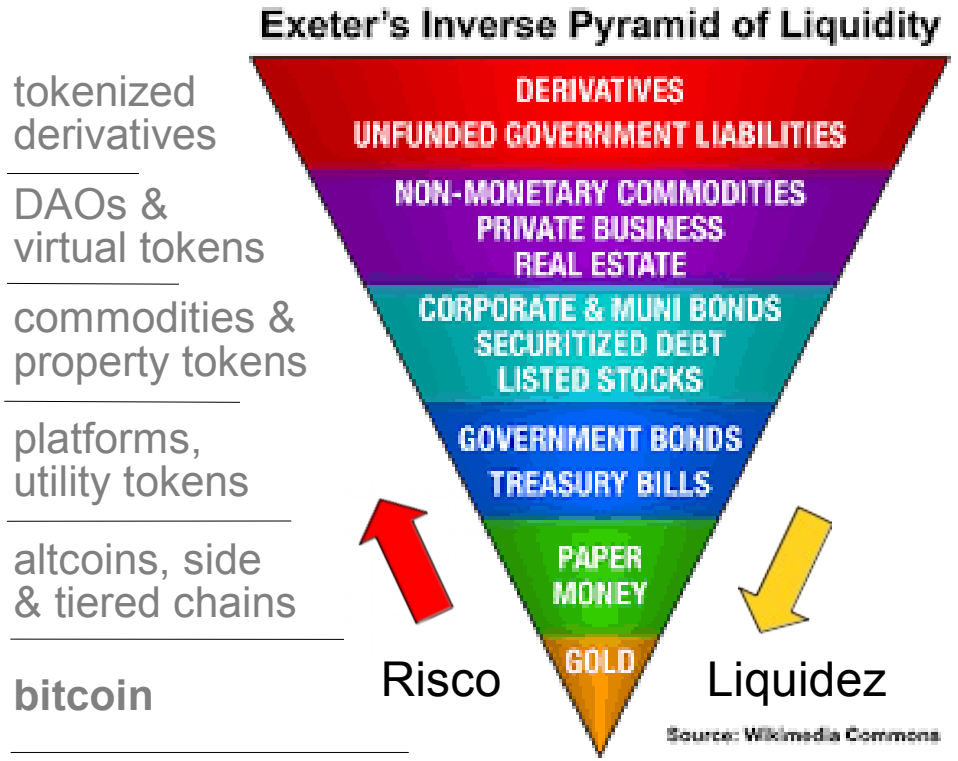
- Um *token* (tipo de prova, passe, ficha, mensagem) *criptográfico* deve funcionar como elemento necessário de um sistema auto-sustentável que seja de utilidade pública (0)
- Um token é um elemento *necessário* de um tal sistema (CriptoSys) se o uso de qualquer outro em seu lugar danificaria o funcionamento normal desse sistema. (1)
- Um tal sistema é *auto-sustentável* se continuar a funcionar normalmente na ausência indefinida de seus criadores – pela convenção de Berna (*copyright*): software livre. (2)
- Um tal sistema é de *utilidade pública* se for livre de "catracas virtuais" (não exige permissão), livre de aluguel e faz algo útil. https://hidden.computer/about.html (3)

Alguns parâmetros estruturantes para CriptoSys			
Arquitetura blockchain(s)	Cadeia de blocos	Grafo acíclico	
CriptoProva imutabilidade	por Esforço (PoW)	*e/ou* por Interesse (PoS)	
Regras para concenso	por Acordo bizantino [*ou outro(s)*?]		
Forma de governança	Democracia líquida	Curadoria c/ token	Centralizada
Forma de interação	Permissiva (aberta)	Permissionada	Fechada
Ling. máquina virtual	Livre de contexto	Turing-completa	

3. Como o atual paradigma financeiro pode evoluir

Jehan Chu (Kinetic Capital) Cointelegraph, 01/07/2018:

"*Bitcoin will never go to zero because it is a hedge against falling currencies, inefficient economies, and increasingly systemic inequality. Bitcoin represents the currency of a better future for society, and people will always invest in their future.*"



Dinheiro descentralizado, adaptativo, autônomo e democrático tem muitos interesses envolvidos e características fortes: difícil eliminar

cointelegraph.com/news/mythbusting-why-bitcoin-can-never-go-to-zero
steemit.com/cryptocurrency/@goldgoatsnguns/the-next-phase-of-the-cryptocurrncy-bull-market-is-beginning

3. Front econômico da guerra híbrida

[Nesara News, out 2011] - No *front* econômico da atual guerra híbrida, rumo a um *reset* financeiro, a estratégia de dominação mostra a seguinte evolução no teatro do controle regulatório na esfera monetária:

Países cujo banco central não é(ra) controlado pelo clã Rothschild (ano)

2000	2003	2011
Afghanistão	~~Afghanistão~~	~~Afghanistão~~
Iraque	~~Iraque~~	~~Iraque~~
Sudão	Sudão	~~Sudão~~
Libia	Libia	~~Libia~~
Cuba	Cuba	Cuba
Coreia do Norte	Coreia do Norte	Coreia do Norte
Iran	Iran	Iran

~~xxxx~~ : asfixiados com regulação *anti-money-laundering* (AML) ou capturados

nesaranews.blogspot.com.br/2011/10/only-3-countries-left-wo-rothschild.html
http://www.youtube.com/watch?v=R-4Jd0o-Emw

3. Front econômico da guerra híbrida

Preparativos no *front* midiático para eventos de bandeira falsa, em preparo à transição da ordem monetária rumo ao *reset* financeiro, 'normalizam' tais políticas como a (inevitável) Nova Ordem Mundial.

J Bloomberg, Forbes, 28/03/2018:

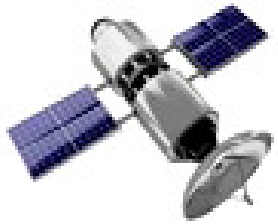
"*We need to shut Bitcoin and all other cryptocurrencies down... There's only one way to slay this beast. We must make all cryptocurrency as we know it today illegal…Enjoy the world of permissionless block chain cryptocurrencies while you can, because its days are numbered*."

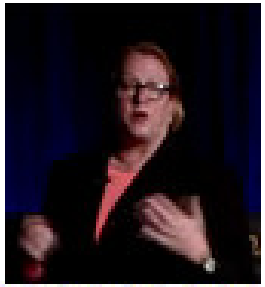
www.forbes.com/sites/jasonbloomberg/2018/03/10/we-need-to-shut-bitcoin-and-all-other-cryptocurrencies-down-heres-why/

3. Interface cibernética da guerra híbrida

The Digital Infrastructure

- *IT and Payment Systems Run by Private Corporations*
- *Non-Transparent Contracting Budgets*
- *Suppression & Destruction of Place-Based Financial Systems*
- *Centralized Clearance, Payments and Wire Systems*
- *Integration of NSA into the Telecommunications Backbone*
- *Globalized Satelite Services and Systems*
- *The Patriot Act (+ Snoope's charter, etc)*
- *Smart Phones, Cell Towers (5ª gen) and Internet of Things*





– Catherine Austin-Fitts: (junho 2014) O cerne da guerra "na internet" é pela centralização do controle de sistemas e fluxos de pagamentos: O colapso controlado do dólar, e a ascensão de uma nova moeda para reserva de valor e no comércio global dependem desse controle:

"*quem controlar as vias digiais, os cabos submarinos e canais satelitais, controlará a moeda global. O que tem requerido cada vez mais violência.*"

https://www.youtube.com/watch?v=w0mimIp8mr8
en.wikipedia.org/wiki/Investigatory_Powers_Act_2016

3. Origem do Bitcoin e a guerra híbrida

A tese mais consistente aponta para as entranhas da NSA. Ou por iniciativa despistada de *white-hats,* ou como *psyop* em prepararo para normalização do *de-cashing**, passo necessário a qualquer estratégia viável para implosão controlada (com juros negativos) da atual ordem financeira, inviabilizada.

A "isca" seria para os espíritos libertários e seus gênios programarem, testarem, implementarem e depurarem protocolos numa rede de transição monetária inicialmente independente, mas destinada a ser depois capturada por violência normativa ou bélica.

*- www.imf.org/~/media/Files/Publications/WP/2017/wp1771.ashxl
tradutoresdedireita.org/evidencias-sugerem-que-o-bitcoin-seja-um-plano-psicologico-da-nsa-para-implantar-uma-moeda-digital-mundial/

3. Origem do Bitcoin e a guerra híbrida

A tese mais consistente aponta para as entranhas da NSA. Ou por iniciativa despistada de *white-hats,* ou como *psyop* em prepararo para normalização do *de-cashing**, passo necessário a qualquer estratégia viável para implosão controlada (com juros negativos) da atual ordem financeira, inviabilizada.

A "isca" seria para os espíritos libertários e seus gênios programarem, testarem, implementarem e depurarem protocolos numa rede de transição monetária inicialmente independente, mas destinada a ser depois capturada por violência normativa ou bélica. Neste caso, restaria saber se o feitiço vira contra o feiticeiro, e que papel nos cabe nessa virada.

*- www.imf.org/~/media/Files/Publications/WP/2017/wp1771.ashxl
tradutoresdedireita.org/evidencias-sugerem-que-o-bitcoin-seja-um-plano-psicologico-da-nsa-para-implantar-uma-moeda-digital-mundial/

3. A aposta seria esta:

[na hipótese do Bitcoin como *psyop*]

Aldous Huxley (em "Admirável Mundo Novo"), 1936

- "*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 (em "*Project New American Century*"):

en.wikipedia.org/wiki/Project_for_the_New_American_Century

3. Quem pode ganhar essa aposta?

Aldous Huxley (em "Admirável Mundo Novo"), 1936

- "*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 (em "*Project New American Century*"):

en.wikipedia.org/wiki/Project_for_the_New_American_Century

Modelo Bíblico nas profecias para o tempo da grande tribulação:

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