NET BR

COLISÕES NO RADIOAMADORISMO

NOVAS TECNOLOGIAS EM QRG

#NetBR Ed.257

https://www.radiomuseum.org/forum/15v_am_tube_transmitter.html

NOSSO PARQUINHO...

Radio Amadorismo não é apenas um *hobby*. Dentre seus objetivos também incluem-se a pesquisa científica, comunicação *backup*, apoio em desastres e emergências, comunicação em áreas remotas, até mesmo rede de apoio social, dentre outras aplicações.

Radioamadores adoram a tecnologia, e vice-versa: os entusiastas de tecnologia encontram um campo fértil no radioamadorismo.

Nos últimos meses pudemos notar o avanço de duas novas **aplicações** dentro das frequências destinadas ao radioamadorismo: **robôs de voz, e criptomoedas**.

Na apresentação de hoje não faremos juízos nem chegaremos à conclusões: forneceremos informações e conhecimentos de forma que cada Radioamador possa chegar às suas próprias conclusões.

https://archive.org/details/73-magazine-1976-07

AJUDANTE OU OPERADOR?

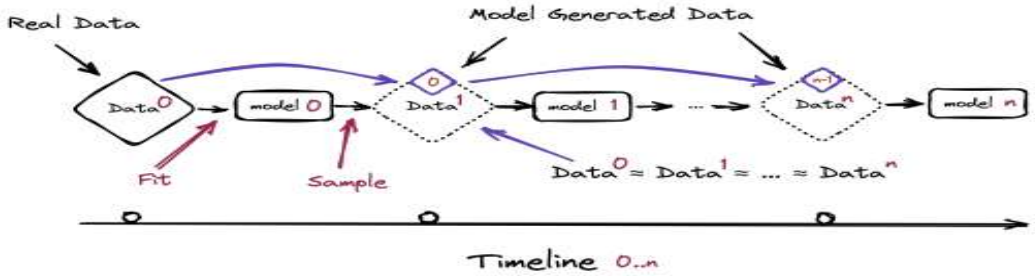
Usar um computador para "modular" não é novidade. Em 1976 o periódico "73 Amateur Radio" já contava com as "*computer section*", edições dedicadas ao uso de computadores no radioamadorismo. A novidade atual é o uso de Inteligência Artificial, onde o próprio sistema toma decisões como operador. Uma pesquisa em logs QSL, como PSKReporter ou CLubLog, mostram centenas de estações atualmente operando CW e FT8 de forma autônoma: 24 horas por dia, por dezenas de dias.

Apesar de fortes indícios em logs e de muitos rumores em fóruns, existe a suspeita de que alguns operadores estão valendo-se de "Robôs de Voz" operados por AI durante contestes e CQs. Opiniões contrárias, ou favoráveis, chega-se a cogitar que havendo licenciamento futuro, a AI de voz poderia coordenar CQs e *Pilleups* - e até mesmo ser um operador 24X7 em QRGs de emergência. Independente da veracidade deste tipo de ocorrência, a tecnologia existe, é barata, e está ao alcance de todos.

Portanto, plausível.

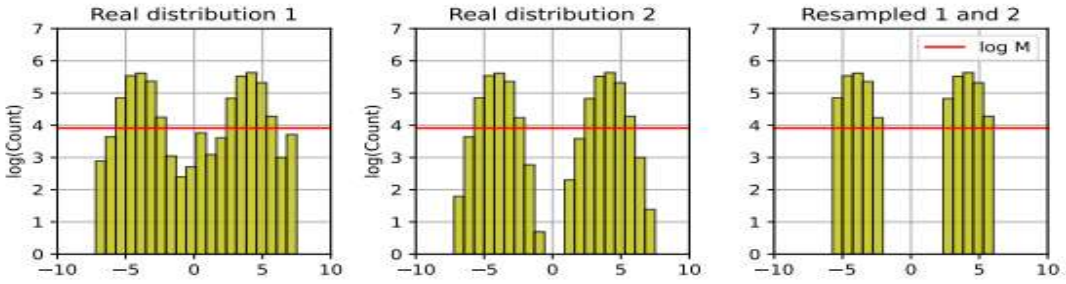
DEMENCIA DA A.I.?

Vista como grande promessa para a tecnologia e desenvolvimento da humanidade, diversos estudos científicos estão mostrando fraquezas da A.I. como conhecemos: sim, está ficando “menos inteligente”.



Os mecanismos de AI acabam se retroalimentando, ou sendo alimentados por outros modelos de AI, e aos poucos perde-se os parâmetros de tempo, de realidade, de humanidade, e de naturalidade.

Para a AI, gatos verdes são comuns.



REALIDADES DISTINTAS

A maioria dos modelos de AI já perderam a capacidade de listar e comprender ironias. A existência de drones da WW2 ou de redes sociais na Revolução Francesa, estão na mesa. Carros autônomos ainda confundem-se com paisagens não naturais ou com sinalizações falsas. Se existem gatos azulados, e gatos amarelados, então gatos verdes são comuns. Programadores de computador já não confiam em AI devido aos códigos incorretos e em linguagens inventadas. Sem contar o problema do "*horse-talking*", quando dois robôs se encontram, mas não identificam-se como robôs, e começam a **conversar em loop infinito**: o que poderia travar uma QRG por dezenas de horas ou dias....

QUAL SUA OPINIÃO?

-Você deixaria um robô de voz operando em seu indicativo?

-Um robô AI conseguiria coordenar uma operação de emergência?

-Operações automatizadas em RA são nocivas? Ou são toleradas?

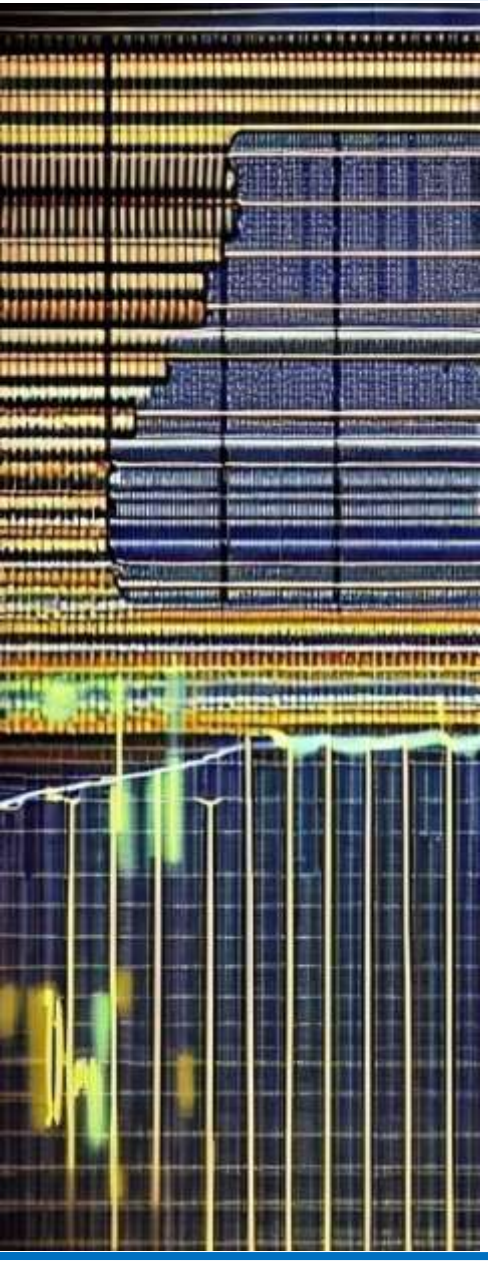
CULTURA DOOMSDAY

Muitos norte-americanos e asiáticos adotam a “cultura *doomsday*” no cotidiano: estão sempre preparados para uma possível catástrofe que irá cortar as cadeias de suprimentos, de energia, e de telecomunicações. Sendo então o radioamadorismo a alternativa para a questão das comunicações e contatos.

QSJ NA QRG

Situações prolongadas de catástrofes generalizadas e em larga escala “podem” causar a falências dos sistemas monetários e bancários. Muitos adeptos desta cultura então adotam as “moedas digitais” como alternativa para troca de valores. Dois mundos encontram-se aqui.

Antes de iniciar: vale lembrar que **todas** as legislações globais proibem o tráfego de dados criptografados pelas frequências destinadas ao radioamadorismo, e a maioria dos países (inclusive o Brasil) proíbe o exercício de quaisquer atividades comerciais e/ou financeiras no radioamadorismo.



DIZEM OS DEFENSORES

Com certa periodicidade surgem *whitepapers* (projetos) com operações bem sucedidas do envio de moedas digitais através de ondas de rádio por longas distâncias. Existem inclusive sugestões de padronização destes envios em 144.8mHz FM modulação PSK/RTTY, ou usando modulação Lora em 433.8 ou 918Mhz. Dentre estes projetos estão o “Hamradiocoin”, “Vertais”, “Kryptoradio”, “CoinKite”, dentre outras. Algumas chegaram a usar JS8Call em 40 metros, outras até usaram a faixa do cidadão (CB). Empresas privadas elevaram a sofisticação, como a Blockstream, que licenciou frequências de TV analógica, e criou transceptores de Bitcoins.

Os defensores afirmam que não estão a transmitir a moeda em si, mas uma PST (*Partially-Signed-Transaction*, uma espécie de ordem de pagamento), que todas as informações contidas na mensagens são públicas e não possuem criptografia, e que a efetivação da transação via criptografia ocorre na *blockchain*, a qual também contém dados públicos. Seria algo análogo a dois radioamadores combinando voluntariamente a compra/venda de um equipamento...

Verdade??? Podemos entender os conceitos, antes de concluir...

Criptografia simétrica

J	O	Ã	O
K	5	X	5

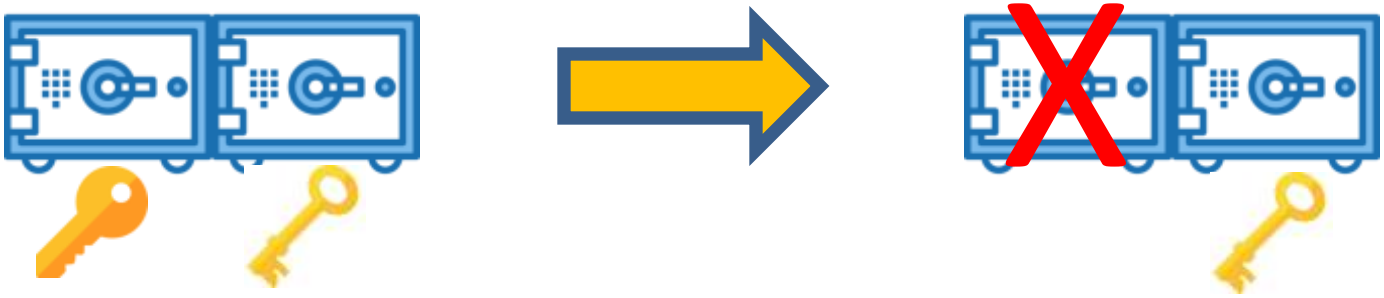
K	5	X	5
J	O	Ã	O

Neste tipo de criptografia (codificação de dados), emissor e receptor compartilham a mesma chave, que codifica uma mensagem, e depois decodifica a mensagem. Esta chave pode ser uma tabela de conversão, ou um cálculo pré-definido.

Imagine um pequeno cofre que o emissor deseja enviar para um receptor contendo uma mensagem secreta dentro. O emissor envia antes uma cópia da chave ao receptor, para que este possa abrir o cofre e ler a mensagem, e também consiga devolver o cofre com uma nova mensagem secreta dentro.

Criptografia Assimétrica (e assinaturas digitais)

Este tipo de criptografia utiliza um **par de chaves**, uma privada (secreta) e uma pública. A chave privada codifica uma mensagem de forma que qualquer um que tenha uma cópia da chave pública consiga abrir, e ao mesmo tempo garantindo que somente o detentor da chave privada tenha conseguido codificar (por isso é usada como assinatura digital). A chave pública também consegue codificar uma mensagem, porém somente o detentor da chave privada conseguirá ler.



Imagine um cofre com dois compartimentos, separados por um vidro transparente com uma ranhura. Somente a chave privada consegue abrir e fechar ambos os compartimentos. A chave pública consegue abrir somente o segundo compartimento para ver através do vidro, a mensagem inserida pela chave privada. E também consegue inserir uma nova mensagem pela ranhura – que somente a chave privada conseguirá acessar.

Criptografia Assimétrica (para leigos)

3 7	7 21	10	210
CHAVE PRIVADA	**CHAVE PÚBLICA**	**MENSAGEM**	**RESULTADO**

Imagine os números 3 e 7, números primos, **porém muito muito grandes** (+100 casas)

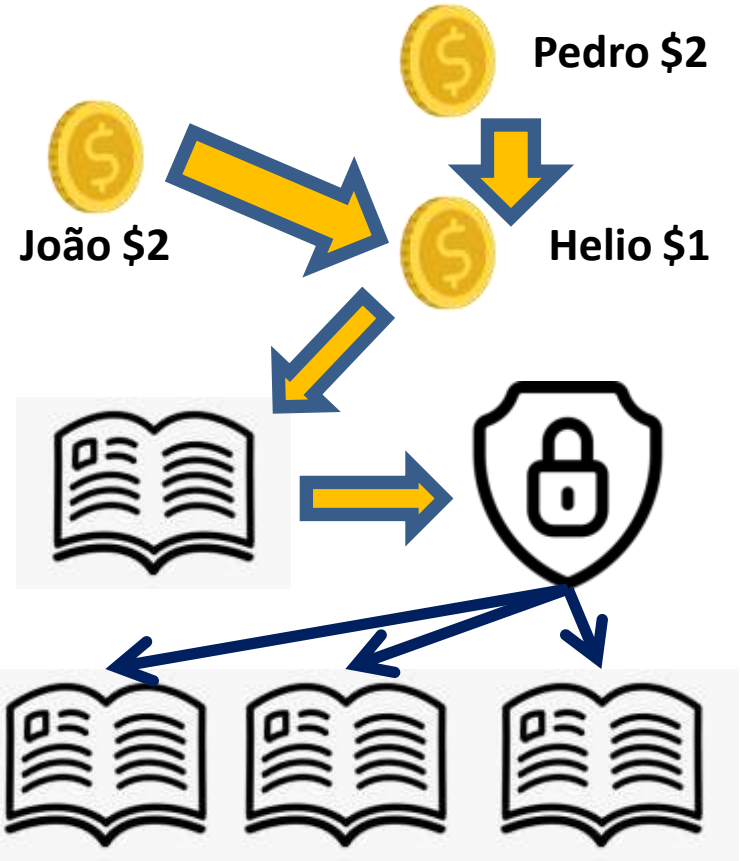
3X7=21. A chave privada é composta de 3 e 7, e a chave pública, é 7 e 21. 7+21 é reconhecida como uma chave pública pois 21 é fatorável por 7.

E emissor deseja codificar/assinar a mensagem “10”. Ele usará a chave privada: 3x7x10=“210”.

Somente o emissor (chave privada) consegue transformar “10” em “210”, mas todos os que sabem a chave pública “7+21” conseguirão fatorar 210/21=10 e então descobrir a mensagem.

Quem possui a chave pública também consegue enviar mensagens de forma que somente a chave privada consiga abrir. Ex: transformando a mensagem “5” em “2205”, somente a chave privada conseguirá fazer 2205/21/7/3=“5”.

Moeda Digital (*e a Blockchain*)



A moeda, na verdade, só existe como escrituração na Blockchain...

João possui 2 unidades de uma moeda digital, anteriormente recebidas de outras pessoas. João transfere 1 moeda para Helio, o qual já possuia 1 moeda recebida de Pedro. João cria esta transação de 1 moeda **assinando com sua chave privada indicando o destinatário (Helio) e o valor**, e a envia para a "*blockchain*", que é um livro contábil público, a qual contém as chaves públicas de todos os participantes.

Um validador (ou minerador) vai checar se João e Pedro realmente são os detentores destas moedas, checando todas as transações anteriores com estas moedas, e então vai atestar que a transação é válida: que agora João possui 1 moeda e que Helio passa a ter 2 moedas. O validador então assina esta transação na *blockchain* utilizando sua chave pública, autorizando a distribuição às milhares de cópias descentralizadas – abertas ao público.

A PST e as ondas do rádio

PST = 1 Moeda + De João + Para Helio + Assinatura de João

PST + Assinatura de Helio

A PST (*Partially Signed Transaction*) é, resumidamente, uma transação que trafega "por fora" das eswcriturações até que todos os participantes a assinem. João consegue mandar uma PST para Helio de várias formas: morse, rádio, voz, papel, pendrive, pombo correio, SMS, fumaça, etc... Por fim, basta Helio receber, assinar e enviar a PST para a *blockchain,* para que seja validada. Uma PST simples contém de 220 a 250 bytes. Abaixo um exemplo:

9jA5FbNcE7D3RvX6qYhGzP1mI8tVpLbW2oU4xTfCkSdZnMlOaQeHrJ0uKwXsNlYcWvLbTnMjPqHrEaKzSdZfXcVbN

A mensagem PST depois de decodificada (demodulada) realmente **não contém informação confidencial nem criptografada**: contém dados do emissor, do receceptor, valor, e assinatura.

A questão sobre criptografia... é a assinatura. Como vimos, a mensagem carrega uma chave pública ou uma assinatura , que por sua vez é gerada somente por uma chave privada - desconhecida. Portanto pode-se afirmar que há alguma criptografia na mensagem.

QUAL SUA OPINIÃO?

Agora que você compreende os conceitos básicos de criptografia e moedas digitais, poderá chegar em suas próprias conclusões.

-Um radioamador mandando sua moeda digital para outro radioamador, por meio de frequências de radioamadorismo, seria considerada uma transação comercial / financeira?

-Uma transmissão de PST contém ou não contém dados criptografados?

- Este tipo de tráfego é nocivo? Ou é tolerável?

Agradecemos pela audiência e atenção.

73

CONSIDERACOES FINAIS

-Independente do disposto em legislações e regulamentos, **operações automatizadas para estabelecer contatos** com outros radioamadores (QSOs) é vista como “anti-ética” dentre os radioamadores.

- As moedas digitais (a.k.a. Criptomoedas, Ativos Digitais, CryptoAtivos, Cryptos, etc) **não são investimentos, sua posse e operação incorrem em riscos de prejuízos** financeiros. Independente do disposto em legislações e regulamentos, transmissões de PSTs (bem como qualquer mensagem de caráter pecuniário) não são bem vindas no radioamadorismo.

- Lembre: no radioamadorismo, se você não não sabe se é permitido, **não faça!** Se não têm certeza de como fazer algo, **aprenda antes de fazer**.

https://www.e-farsas.com/parede-desenhada-com-o-tunel-papa-leguas-causou-um-acidente.html
https://scholar.google.com.br/scholar?q=artificial+intelligence+failing+feedback&hl=pt-BR&as_sdt=0&as_vis=1&oi=scholart
https://www.youtube.com/watch?v=DPXtrJ59jus
https://venturebeat.com/ai/the-ai-feedback-loop-researchers-warn-of-model-collapse-as-ai-trains-on-ai-generated-content/
https://heinonline.org/HOL/LandingPage?handle=hein.journals/hjlt31&div=30&id=&page=
https://arxiv.org/abs/2305.17493
https://arxiv.org/pdf/2305.17493.pdf
https://www.cl.cam.ac.uk/~is410/Papers/dementia_arxiv.pdf
https://www.politico.com/newsletters/digital-future-daily/2023/03/02/psst-when-ais-talk-among-themselves-00085282
https://www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/
https://www.cryptopolitan.com/how-to-send-bitcoin-without-internet/
https://news.bitcoin.com/devs-send-the-first-dogecoin-transaction-without-internet-via-radio-doge/
https://news.bitcoin.com/bitcoin-and-weak-signals-bypass-network-censorship-with-radio/
https://medium.com/@mnegociacoes/sem-internet-sem-problema-como-enviar-bitcoin-por-r%C3%A1dio-amador-532445100589#:~:text=2014%20viu%20as%20primeiras%20men%C3%A7%C3%B5es,para%20a%20ind%C3%BAstria%20de%20radioamadores.