

CONSTRUÇÃO DE

ATIVOS DIGITAIS

GUSTAVO XAVIER DE CAMARGO



TOKENS

TOKENOMICS

Tokenomics, também conhecida como economia de tokens, é o estudo dos parâmetros que determinam as características das criptomoedas (cryptos) e dos tokens criptográficos relacionados à criação de valor econômico. Ambos, criptomoedas e tokens são subclasses de ativos digitais que utilizam tecnologia de criptografia.

<https://en.wikipedia.org/wiki/Tokenomics>





FICHA TELEFÔNICA

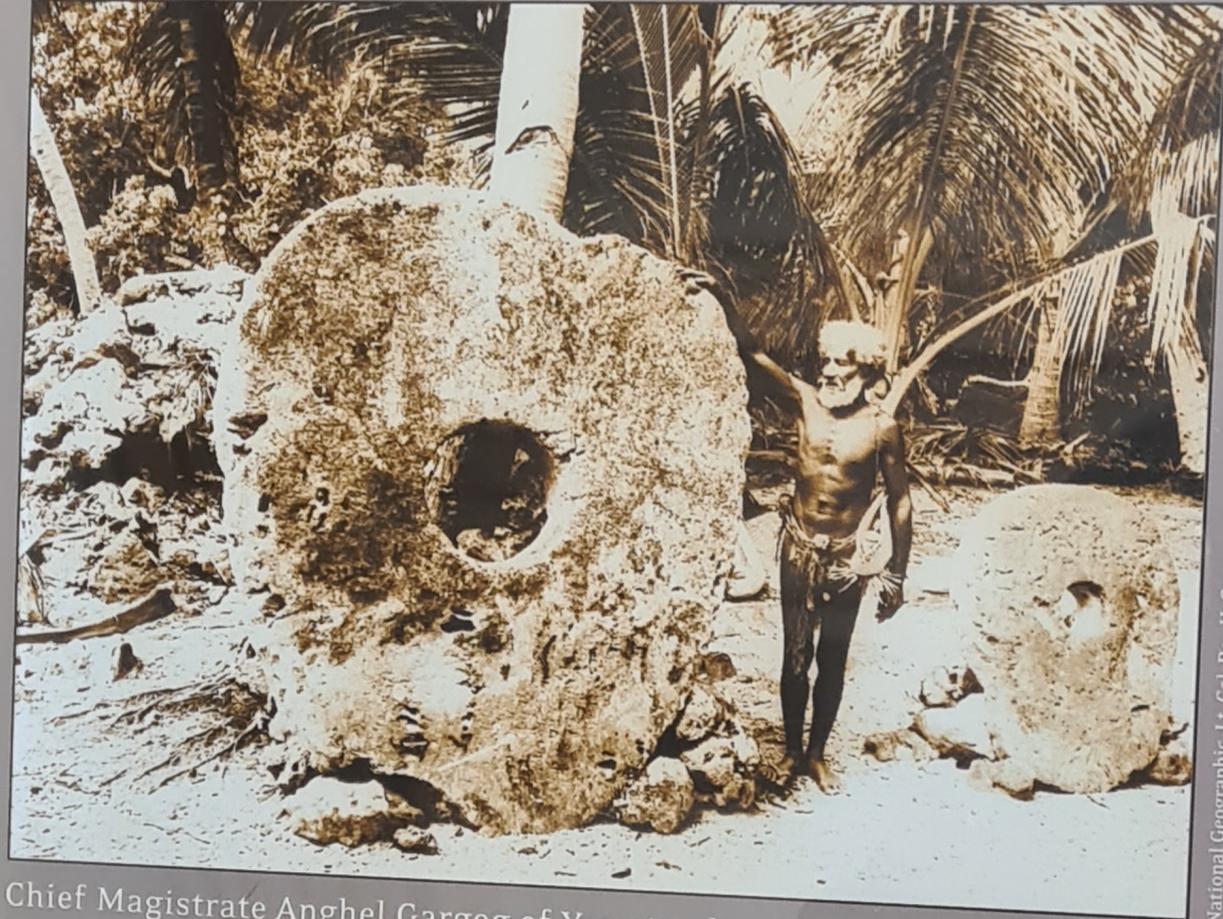
FICHA TELEFÔNICA

As fichas de telefone são fichas utilizadas para fazer ligações de telefones públicos.

Elas surgiram no Brasil nos anos 60. (...) Em 1970, a Companhia Telefônica Brasileira fez com que as fichas tivessem um padrão exclusivo para cada área de atendimento.

https://pt.wikipedia.org/wiki/Ficha_de_telefone





National Geographic, Lt. Col. Roy H. Goss

Chief Magistrate Anghel Gargog of Yap stands with the Smithsonian stone in 1962. To make it more stable, the stone is displayed in a different position from that in the photograph.

At
pr
ar
co
da

W
Obj
stor
on Y
trad
dan

Stones of Status

This stone (or *rai*) is a symbol of status on the Micronesian island of Yap. At the Museum stores here, you can exchange round pieces of metal and printed paper called "money" for other objects. These large stone disks are often called "stone money" but they are only exchanged by Yapese communities and families during important social occasions, not in daily, commercial transactions.

What Makes a Rai Valuable?

Objects of value vary from culture to culture. The value of each stone is determined by its history, which includes when it arrived on Yap, who owned it, and how it was used. Exchanges of *rai* honor traditional ceremonies such as marriages, funerals, competitive dancing, feasting, and construction of community buildings.



Micronesian Island of Yap

Incredible Journey of the Yap Stones

For centuries stone disks (or rai) were exchanged...



EMANCIPATION

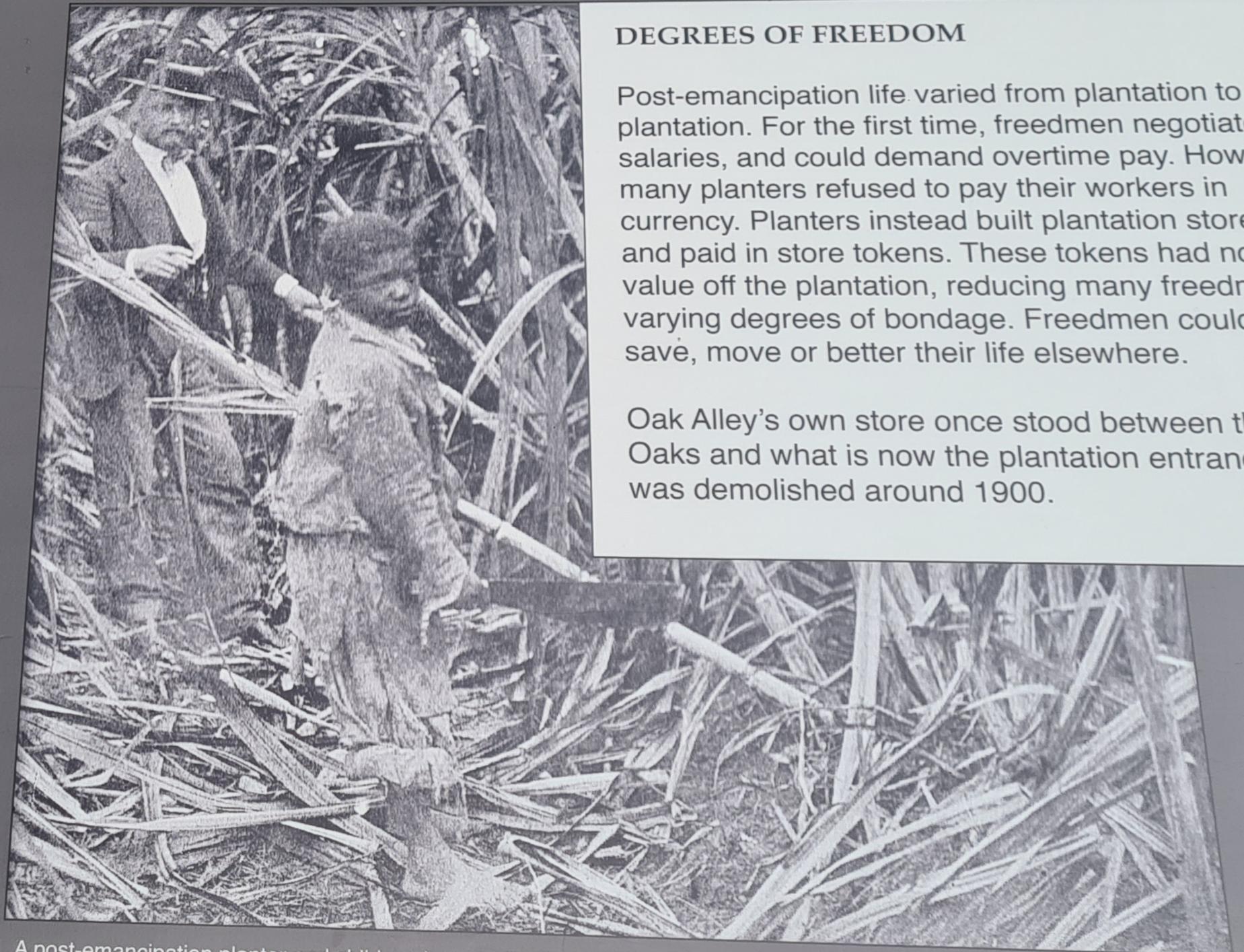
The end of slavery was not a single moment but a series of events. After the Civil War, they sought to build new lives in the economically and politically turbulent period of Reconstruction.

At the onset of the Civil War, house slaves at Oak Alley ran away as "self-emancipation." While only a few years earlier they were punished as fugitives, slaves could now disappear into the woods.

General Butler ordered slaves to return to their owners, stating that they would be paid. Most disregarded his order and the question of compensation. By the time Lincoln issued the Emancipation Proclamation, many slaves already considered themselves "freedmen."

An Oak Alley payroll after Butler's order shows former slaves and other workers being paid. The records are also filled with notes of workers being jailed, conscripted to work on the levees, or leaving.

St. James Parish Records, H. Roman vs. Mr. Fisker 1864



DEGREES OF FREEDOM

Post-emancipation life varied from plantation to plantation. For the first time, freedmen negotiated salaries, and could demand overtime pay. However, many planters refused to pay their workers in currency. Planters instead built plantation stores and paid in store tokens. These tokens had no value off the plantation, reducing many freedmen to varying degrees of bondage. Freedmen could not save, move or better their life elsewhere.

Oak Alley's own store once stood between the Oaks and what is now the plantation entrance. It was demolished around 1900.

A post-emancipation planter and child worker. "Cutting the Sugar—Louisiana 1876"

TUDO TOKEN POSSUI UMA MOTIVAÇÃO
ECONÔMICA, SOCIAL OU CULTURAL.

O BITCOIN NASCE DO MOVIMENTO CYPHERPUNK



CRYPTO REBELS

The battle is engaged.

It's the FBI's, NSA's, and Equifax's of the world versus a swelling movement of Cypherpunks, civil libertarians, and millionaire hackers. At stake: Whether privacy will exist in the 21st century.

Steven Levy reports on the Pretty Good Revolution.

Supporting a non-profit company that turns its dollars by providing support to users of free software, seems like a time warp to the days when hackers ran free. Though Cygnus is located in a mall-like business park within earshot of US 101, it features a spacious cathedral ceiling overhanging a cluttered warren of workstations arranged in an irregular spherical configuration. A mattress is nestled in the rafters. In a hallway behind the reception desk is a kitchen laden with snack food and soft drinks.

Today, a Saturday, only a few show up for work. The action instead is in a small conference room overlooking the back of the complex—a "physical meeting" of a group whose members most often gather in the corridors of cyberspace. Their mutual interest is the arcane field of cryptography—the study of secret codes and cyphers. The very fact that this group exists, however, is indication that the field is about to shift into overdrive. This is crypto with an attitude, best embodied by the group's moniker: Cypherpunks.

The one o'clock meeting doesn't really get underway until almost three. By that time around fifteen techie-cum-civil libertarians are sitting around a table, wandering around the room, or just lying on the floor staring at the ceiling while listening to the conversations. Most have beards and long hair—Smith Brothers gone digital.

The talk today ranges from reports on a recent cryptography conference to an explanation of how entropy degrades information systems. There is an ad hoc demonstration of a new product, an AT&T "secure" phone, supposedly the first conversation-scrambler that's as simple to use as a standard-issue phone. The group watches in amusement as two of their members, including one of the country's best cryptographic minds, have

room represents the vanguard of the pro-crypto forces. Though the battle-ground seems remote, the stakes are not: The outcome of this struggle may determine the amount of freedom our society will grant us in the 21st century. To the Cypherpunks, freedom is an issue worth some risk.

"Arise," urges one of their numbers. "You have nothing to lose but your barbed-wire fences."

Crashing the Crypto Monopoly
As the Cold War drifts into deep memory, one might think that the American body charged with keeping our secret codes and breaking the

code of our enemies—the National Security Agency (NSA)—might finally breathe easy for the first time in its 30-year existence. Instead, it is sweating out its worst nightmare.

The NSA's cryptographic monopoly has evaporated. Two decades ago, no one outside the government, or at least outside the government's control, performed any serious work in cryptography. That ended abruptly in 1975 when a 31-year-old computer wizard named Whitfield Diffie came up with a new system, called "public-key" cryptography, that hit the world of cyphers with the force of an unshelved nuke. The shock wave was undoubtedly felt most acutely in the fortress-like NSA headquarters at Fort Meade, Maryland.

As a child, Diffie devoured all the books he could find on the subject of cryptography. Certainly there is something about codes—secret rings, intrigue, Hardy Boys mysteries—that appeals to youngsters. Diffie, son of an historian, took them very seriously. Though his interest went dormant after he exhausted all the offerings of the local city college library, it resurfaced in the mid-1960s, when he became part of the computer hacker community at the Massachusetts Institute of Technology.

Even as a young man, Diffie's passion for technical, math-oriented problems was matched by a keen interest in the privacy of individuals. So it was natural that as one of the tilters of a complicated multi-user computer system at MIT, he became troubled with the problem of how to make the system, which held a person's work and sometimes his or her intimate secrets, truly secure. The traditional, top-down approach to the problem—protecting the files by user passwords, which in turn were stored in the electronic equivalent of vaults tended by trusted system administrators—was not satisfying. The weakness of the system was clear: The user's privacy depended on the

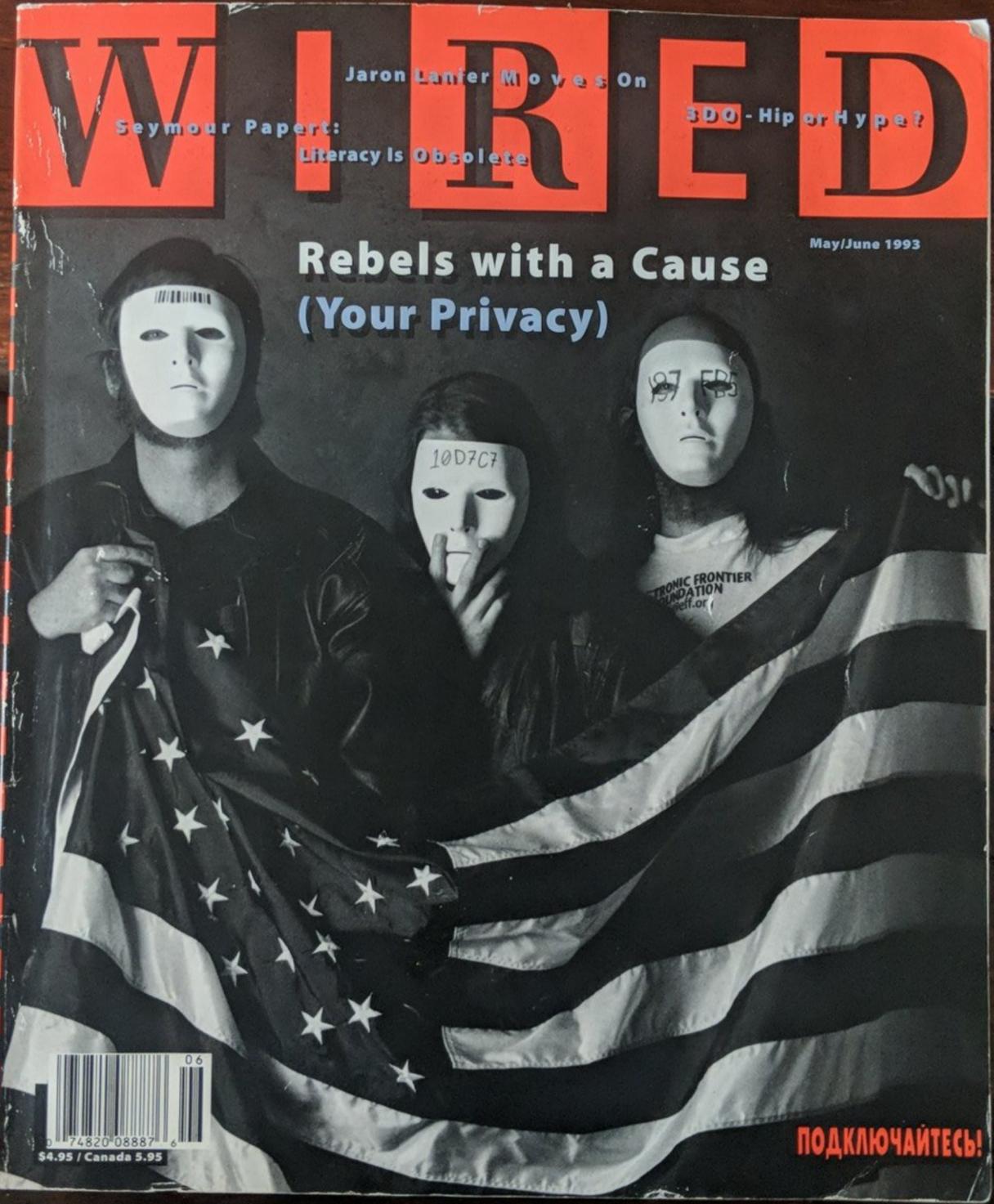
degree to which the administrator was willing to protect it. "You may have protected files, but if a subpoena was served to the system manager, it wouldn't do you any good," Diffie notes with withering accuracy. "The administrators would sell you out, because they'd have no interest in going to jail."

Diffie recognized that the solution rested in a decentralized system in which each person held the literal key to his or her own privacy. He tried to get people interested in taking on the mathematical challenge of discovering such a system, but there were no takers. It was not until the 1970s, when the people running the ARPAnet (destined to become the Internet) were exploring security options for their members, that Diffie decided to take it on himself. By then he was at Stanford, under the thrall of David Kahn's 1967 work, *The Codebreakers*. It was a revelatory, well-written, and meticulously documented history of cryptography, focusing on 20th century American military activities, including those at the NSA.

"It brought people out of the woodwork and I certainly was one of them," recalls Diffie. "I probably read it more carefully than anyone had ever read it. By the end of 1973, I was thinking about nothing else." He embarked on what was planned to be a worldwide journey in search of information on the subject. Gaining access to it was a difficult task, since almost everything about modern cryptography was classified, available only to NSA-types and academics. Diffie's sojourn took him as far as the East Coast, where he met the woman he would eventually marry. With his future bride, he moved back to Stanford. It was then that he created a revolution in cryptography.

Specifically, the problem with the existing system of cryptography was that secure information traveled over insecure channels. In other words, a message could be intercepted before reaching its recipient. The traditional method for securing information involved encoding an original message—known as a "plaintext," by use of a "key." The key would change all the letters of the message to anyone who tried to read it would see only an impenetrable "cyphertext," when the cyphertext message arrived at its destination, the recipient would use the same key to decipher the code.

Founding members of the Cypherpunk group (right) remove their masks: from left, Tim May, Eric Hughes, and John Gilmore. Other Cypherpunks gathered to discuss cryptography for the people (left) pose with an emblem of privacy: a face mask bearing the digits of their personal public key. The key is used to decode highly secure messages sent to them on public networks.



"IF PRIVACY IS OUTLAWED, ONLY OUTLAWS WILL HAVE PRIVACY."

“Se desejamos privacidade, devemos garantir que cada parte de uma transação tenha conhecimento apenas daquilo que é necessário para a transação. (...) Na maioria dos casos, a identidade não é essencial. (...) Quando minha identidade é revelada pelo mecanismo subjacente da transação, não tenho privacidade. Não posso, aqui, me revelar seletivamente; eu devo sempre me revelar.”

Eric Rughe, A Cypherpunk's Manifesto

“O modelo bancário tradicional alcança certo nível de privacidade pela limitação do acesso à informação para as partes envolvidas e o terceiro conviver. O anúncio necessário de todas as transações, publicamente, derruba a eficácia deste método, mas a privacidade pode ser mantida quebrando-se o fluxo de informação em outro local: por meio de chaves públicas anônimas. O público pode ver que alguém está enviando um valor para outro indivíduo, mas sem uma informação relacionando a transação a alguém”

Satoshi Nakamoto, Bitcoin: a peer-to-peer electronic cash system.

Traditional Privacy Model



New Privacy Model



Satoshi Nakamoto, Bitcoin: a peer-to-peer electronic cash system.

COMO RESOLVER O PROBLEMA DO GASTO DUPLO?

**DIFERENTE DOS BENS FÍSICOS,
DADOS SÃO BENS NÃO RIVAIS.**

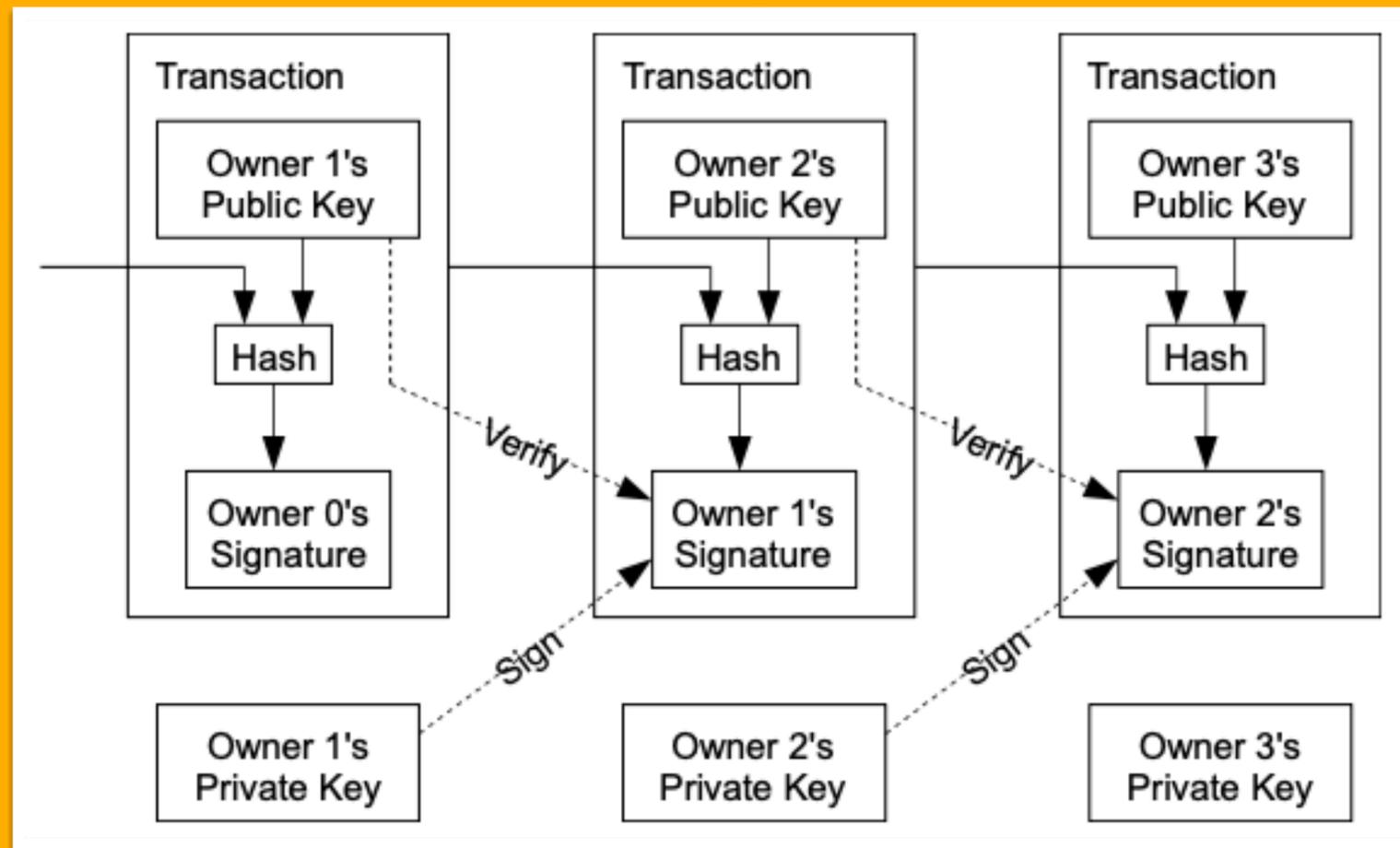


**Para resolver o
problema do duplo gasto,**

**foi implementado um sistema baseado em
registro de transações e não em emissão.**

“Nós definimos uma moeda eletrônica como uma cadeia de assinaturas digitais”

Satoshi Nakamoto, Bitcoin: a peer-to-peer electronic cash system.



Onde são armazenadas as chaves privadas?

Em carteiras (wallets)

_ paper wallets

_ hardware wallets

_ online wallets; mobile wallets; desktop wallets

Para transferir bitcoins de um proprietário para outro é necessário ter acesso a uma chave privada...

que, como todo dado, pode ter infinitas cópias.

**CRIPTOATIVOS SÃO MUITO EFICIENTES
PARA A OCULTAÇÃO DE PATRIMÔNIO.**





Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

LEI Nº 14.478, DE 21 DE DEZEMBRO DE 2022

Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições.

Vigência

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais.

Parágrafo único. O disposto nesta Lei não se aplica aos ativos representativos de valores mobiliários sujeitos ao regime da [Lei nº 6.385, de 7 de dezembro de 1976](#), e não altera nenhuma competência da Comissão de Valores Mobiliários.

Art. 2º As prestadoras de serviços de ativos virtuais somente poderão funcionar no País mediante prévia autorização de órgão ou entidade da Administração Pública federal.

Parágrafo único. Ato do órgão ou da entidade da Administração Pública federal a que se refere o **caput** estabelecerá as hipóteses e os parâmetros em que a autorização de que trata o **caput** deste artigo poderá ser concedida mediante procedimento simplificado.

Art. 3º Para os efeitos desta Lei, considera-se ativo virtual a representação digital de qualquer ativo financeiro ou transferida

NA REALIDADE...

a lei trata de diretrizes a serem observadas na prestação de serviços de ativos digitais e na regulamentação das prestadoras de serviços de ativos digitais.

LEI "DOS CRIPTOATIVOS"

Art. 5º Considera-se **prestadora de serviços de ativos virtuais** a pessoa jurídica que executa, em nome de terceiros, pelo menos um dos serviços de ativos virtuais, entendidos como:

- I - troca entre ativos virtuais e moeda nacional ou moeda estrangeira;**
- II - troca entre um ou mais ativos virtuais;**
- III - transferência de ativos virtuais;**
- IV - custódia ou administração de ativos virtuais ou de instrumentos que possibilitem controle sobre ativos virtuais; ou**
- V - participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais.**

**CRIPTOATIVOS
VS.
SALDO EM CRIPTOATIVOS**

Transações utilizando prestadores de serviço de ativos digitais (exchanges) não envolvem, necessariamente, transações nas cadeias blockchain. Mas envolvem, necessariamente, registros nos sistemas internos do prestador de serviço.

INSTRUÇÃO NORMATIVA RFB Nº 1888, DE 03 DE MAIO DE 2019

Art. 1º Esta Instrução Normativa institui e disciplina a obrigatoriedade de prestação de informações relativas às **operações realizadas com criptoativos** à Secretaria Especial da Receita Federal do Brasil (RFB).

(...)

Art. 6º Fica **obrigada à prestação das informações** a que se refere o art. 1º:

- I - a exchange de criptoativos domiciliada para fins tributários no Brasil;**
- II - a pessoa física ou jurídica residente ou domiciliada no Brasil quando:**
 - a) as operações forem realizadas em exchange domiciliada no exterior; ou**
 - b) as operações não forem realizadas em exchange.**

Informações contidas no SIMBA (Sistema de Investigação de Movimentações Bancárias)

- **Afastamento do sigilo fiscal** de operações com criptoativos;
- **Afastamento do sigilo telemático** de operações com criptoativos.

Identificada a existência de saldo,
em uma exchange...

é possível ordenar
a sua **indisponibilidade**
(congelamento de ordens de saque,
transferências ou movimentações)
ou até mesmo seu **arresto**.

**Identificada a existência de saldo,
em uma exchange...**

**é possível ordenar
a alienação dos criptoativos
e conversão em moeda fiduciária?
Como se deve proceder?
Por leilão?
Por exchange?
Qual exchange?**

Também é possível...

- **Busca e apreensão** de chaves e wallets.
A velocidade na transferência dos ativos é fundamental para a eficácia da medida.

ROTEIRO DE ATUAÇÃO CRIPTOATIVOS

PERSECUÇÃO PATRIMONIAL



MINISTÉRIO PÚBLICO FEDERAL

ÍNDICE

Introdução	5
PARTE I	
Criptoativos	7
Blockchain	10
Bitcoin	12
Onde ficam os criptoativos?	17
Para além do Bitcoin: Blockchains públicos e pseudônimos	20
Armazenamento de criptoativos	24
Movimentação de criptoativos	26
Negociação de criptoativos	32
PARTE II	
Lei de Criptoativos Brasileira	35
Investigação financeira de crimes envolvendo criptoativos	42
Busca e apreensão de criptoativos	65
Sequestro e indisponibilidade de criptoativos	69
Alienação de criptoativos	72
DeFi e suas particularidades	76
NFTs e suas particularidades	80
PARTE III	
Modelos	83

Documento disponível em:

<https://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/criptoativos-persecucao-patrimonial>

Construção de criptoativos é, por natureza, complexa e difícil.

E o combate à ocultação de patrimônio passa, necessariamente, por...

- _ evoluções legislativas,**
- _ melhoria do aparato estatal para lidar com este tipo de ativos e**
- _ aumento da cooperação internacional.**



OBRIGADO!

GUSTAVO XAVIER DE CAMARGO

gustavo@xavierdecamargo.com.br