William Ribeiro de Paula

Blockchain e sua Correlação com Teoria dos Jogos

São Paulo

Fevereiro de 2019

William Ribeiro de Paula

Blockchain e sua Correlação com Teoria dos Jogos

Dispor de maneira clara e objetiva quais âmbitos da teoria dos jogos corroboram para a evolução e confiabilidade da estrutura mais importante das criptomoedas: o Blockchain.

Universidade de São Paulo - USP

Instituto de Matemática e Estatística - IME

Bacharelado em Matemática Aplicada e Computacional

Orientador: Pedro Aladar Tonelli

São Paulo

Fevereiro de 2019

William Ribeiro de Paula
Blockchain e sua Correlação com Teoria dos JogosWilliam Ribeiro de Paula. São Paulo, Fevereiro de 2019
65 p. : il. (algumas color.) ; 30 cm.

Orientador: Pedro Aladar Tonelli

Trabalho de Conclusão de Curso - TCC – Universidade de São Paulo - USP
Instituto de Matemática e Estatística - IME
Bacharelado em Matemática Aplicada e Computacional, Fevereiro de 2019.

1. Blockchain. 2. Teoria dos Jogos. I. Pedro Aladar Tonelli. II. Universidade de São Paulo. III. Instituto de Matemática e Estatística. IV. Blockchain e sua Correlação com Teoria dos Jogos.

William Ribeiro de Paula

Blockchain e sua Correlação com Teoria dos Jogos

Dispor de maneira clara e objetiva quais âmbitos da teoria dos jogos corroboram para a evolução e confiabilidade da estrutura mais importante das criptomoedas: o Blockchain.

São Paulo, 14 de Fevereiro de 2019.

Pedro Aladar Tonelli
Orientador

Professor
Sonia Regina Leite Garcia

Professor
Nelson Mugayar Kuhl

São Paulo
Fevereiro de 2019

Este trabalho é dedicado à minha família, que sempre me incentivou a buscar a felicidade e o equilíbrio em todas as fases da minha vida.

Agradecimentos

Gostaria de agradecer em primeiro lugar à Deus, por ter me dado discernimento e sabedoria ao longo desta jornada e sem ele acredito que não teria alcaçando meus objetivos. Agradeço à minha família por ter me dado todo suporte necessário e que sempre estiveram ao meu lado.

Gostaria de agradecer ao meu orientador Pelro Aladar Tonelli pela oportunidade e confiança, me aceitando como orientando do trabalho de conclusão de curso. Agradeço também a todas as amizades do IME-USP, que de certa forma estiveram ao meu lado tanto em momentos de distração quanto de dificuldades e de aprendizado.

Concluo agradecendo a todos os professores do IME-USP que de alguma forma contribuíram para a minha formação acadêmica.

"Esse é o principal ponto da tecnologia.
Por um lado, ela cria um apetite por imortalidade
e, por outro, ameaça extinção universal.
Tecnologia é a luxúria removida da natureza."
(Don DeLillo – escritor norte-americano)

Resumo

Esse presente trabalho visa mostrar uma reflexão quanto ao entendimento da teoria dos jogos contribuindo para a evolução de uma nova tecnologia, o blockchain.

A teoria dos jogos prevê a busca por uma maximização da satisfação do jogador, baseado em suas preferências, onde o jogador sempre será racional, a fim de atingir esse objetivo. Quanto ao blockchain, mesmo sendo um tema relativamente novo, está mais cada dia mais forte no mercado mundial, trazendo à tona a importância da confiabilidade dessa transição das informações.

A teoria dos jogos explora como pessoas racionais tomam decisões estratégicas em diferentes cenários. Embora muitas vezes confundida com a lógica geral, a teoria dos jogos é baseada em termos puramente matemáticos e tem aplicações em qualquer domínio onde as pessoas devem coordenar ou competir umas com as outras.

Observaremos diversos fatores para a tomada de decisão no que tange à teoria dos jogos, onde demonstraremos que os jogadores não pensam somente na sua decisão e benefício, pensando assim também no outro jogador e na consequência de sua tomada de decisão.

Podemos chamar de blockchain uma inovação tecnológica simples, atualmente está centralizada nas criptomoedas, que gera uma rede de confiabilidade e escalabilidade notórios para seus usuários.

Palavras-chave: Teoria dos Jogos. Blockchain. Criptomoeda.

Abstract

This present study aims to show a reflection on the understanding of game theory contributing to the evolution of a new technology, the blockchain.

Game theory predicts the pursuit of a maximization of player satisfaction, based on their preferences, where the player will always be rational in order to achieve that goal. As for the blockchain, even being a theme relatively new, is growing stronger in the world market, bringing to light the importance of reliability. information.

Game theory explores how rational people make strategic decisions in different settings. Although often confused with general logic, game theory is based on purely mathematical terms and has applications in any domain where people must coordinate or compete with each other.

We will observe several factors for the decision making regarding the theory of games, where we will demonstrate that the players do not think only in their decision and benefit, thinking thus also in the other player and in consequence of his decision making.

We can call blockchain a simple technological innovation, currently centralized in crypto-coins, which generates a network of reliability and scalability notorious for its users.

Keywords: Game theory. Blockchain. Criptocurrency.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

PoW	Proof of Work - Prova de Trabalho
PoS	Proof of Stake - Prova de Participação

Sumário

Introdução

Desde o fim da década de 2000, poucas tecnologias têm causado tanto furor quanto o blockchain e as criptomoedas. Além de invadirem um território que era anteriormente o monopólio único dos bancos centrais nacionais, permitiram que qualquer pessoa com acesso à internet dispusesse de meios para armazenar e trocar valores sem depender de moeda física.

Embora muitos já tenham essa possibilidade a bastante tempo com seus cartões de crédito e débito e com suas ferramentas de internet banking, ainda havia uma parcela significativa da população mundial sem acesso a métodos de pagamento digitais. As criptomoedas mudaram isso.

Mas as mudanças não param por aí. Embora a ideia de criar um dinheiro digital seja quase tão antiga quanto à própria internet, foi apenas com a inovação do blockchain que os principais problemas inerentes à confiança em uma entidade central foram contornados. E então se percebeu que este mecanismo de confiança implementado pelo blockchain tinha potencial para ser muito mais do que só um livro-razão de uma moeda virtual.

Temos em mãos uma descoberta tecnológica com um grande potencial, e esse trabalho tem o objetivo de desmembrar a correlação técnica da teoria dos jogos com essa simples, porém eficaz tecnologia. O trabalho trará alguns conceitos importantes para clarificar a conclusão geral.

O que é que faz com que a tecnologia blockchain seja tão inovadora? Vejamos o mundo real e como a moeda fiduciária é mantida e armazenada. Não importa quem você é, seu dinheiro será armazenado em um local centralizado, ou seja, o banco. O problema com este modelo é que você está dando seu dinheiro para uma entidade e corre o risco de ficar comprometido por uma série de razões. O blockchain resolve esse problema sendo completamente descentralizado e livre de corrupção internamente. A maneira como consegue isso é pela incorporação da criptografia e da teoria dos jogos.

Com o intuito de contextualizar essa conexão, segue abaixo uma breve explanação das **estruturas de mercado**.

1 MERCADO

A organização e características fundamentais de qualquer mercado são chamadas de estrutura de mercado. As estruturas de mercado são diferenciadas com base em muitos fatores, como vários produtores, controle sobre preços e barreiras à entrada. Com base nesses fatores, existem quatro tipos diferentes de estruturas de mercado:

1.1 Competição perfeita

A concorrência perfeita é um mercado onde é fácil para qualquer pessoa entrar no mercado e os vendedores individuais não têm poder sobre o preço do produto. Pense em mangas. É fácil para qualquer um entrar no mercado, tudo que alguém precisa fazer é cultivar mangas. Além disso, eles não podem de bom grado mudar o preço das mangas. Se uma pessoa vender uma manga por R$ 10, o comprador pode simplesmente comprá-la de alguém que esteja vendendo mangas por R$ 5.

1.2 Monopólio

Um monopólio é o oposto polar de uma competição perfeita. Este é um mercado que é dominado por uma corporação e as barreiras à entrada são tão altas que ninguém mais pode entrar nela. Os diamantes de cervejas são um ótimo exemplo de um mercado monopolista.

1.3 Competição monopolística

Este é um mercado que tem muitos vendedores e barreiras muito baixas. Seus produtos são semelhantes, mas não são idênticos. Pense no serviço de entrega de pizza. Agora, dominós e pizzarias têm o mesmo produto com diferenças sutis. Obviamente, pode-se avaliar um pouco o preço do produto com base em fatores como as preferências do cliente. No entanto, se o preço dos dominós for muito alto, as pessoas simplesmente passarão para a pizzaria. Consequentemente, se Dominós e Pizza Hut começarem a cobrar demais, já que as barreiras à entrada são tão baixas, outro jogador pode entrar e levar todos os clientes.

1.4 Oligopólio

Os oligopólios são mercados que são dominados por poucos mercados e as barreiras de entrada são altas. Um dos melhores exemplos de um oligopólio é o mercado de smartphones. O mercado é dominado por poucas empresas como Samsung, Apple e LG. Assim como as competições monopolísticas, os produtos são semelhantes, mas não idênticos. Enquanto isso lhes dá algum controle sobre seus preços, eles realmente não têm muita margem de manobra. Se amanhã a Apple decidir vender seus iPhones por R$ 7.000, além dos fanáticos da Apple, a maioria simplesmente optará por um telefone Android. Obviamente, eles podem sempre se reunir e decidir, como um grupo, aumentar os preços mutuamente, mas isso é chamado de "conluio" e é ilegal em muitos países, inclusive nos Brasil.

Então, quando eles não podem competir mudando os preços, como eles podem ter vantagem sobre seus concorrentes? Eles o fazem por "concorrência sem preço", o que significa competir sem alterar o preço. Como eles fizeram isso? Eles fazem isso mudando a aparência e o estilo de seus produtos e proporcionando uma experiência única. No entanto, a forma mais reconhecível de concorrência sem preço é a publicidade.

A publicidade é uma das formas mais eficazes de mostrar qualidades únicas de seus produtos e introduzir novos produtos. Mas, novamente, há um problema. Quantos anúncios você assiste? As chances são de que você foi bombardeado por toneladas de anúncios hoje em si, quantos deles você realmente se lembra? Se você é um jogador em um oligopólio e mantém uma publicidade cega, vai gastar muito dinheiro.

Como resultado disso, para compensar todo esse dinheiro, você vai invariavelmente aumentar o preço de seus produtos. Se isso acontecer, seus compradores simplesmente irão para seus concorrentes. Então, como você faz isso? Como você anuncia seus produtos sem perder seus clientes? Você terá que basicamente tomar decisões com base nas ações que seus concorrentes tomarão. Para fazer isso, você terá que usar a **teoria dos jogos**.

2 BLOCKCHAIN

2.1 Introdução

Em sua essência, Blockchain é uma tecnologia que armazena transações permanentemente, de forma que as informações não podem ser apagadas posteriormente, somente atualizadas, mantendo para sempre os registros anteriores (MOUGAYAR, 2016).

Segundo (TAPSCOTT; TAPSCOTT, 2016), esta nova forma de armazenamento de dados de transações financeiras pode ser programada para armazenar virtualmente qualquer coisa com valor e importância para a humanidade, como certidões de nascimento e de óbito, certidões de casamento, escrituras e títulos de propriedade, diplomas de cursos educacionais, dados contábeis, registros médicos, requerimentos de seguros, registros de votos, rastreabilidade de alimentos, entre outras coisas que possam ser expressas em código de computador.

Segundo artigo Hyperledger Goes to School, publicado no site da Nasdaq, os blockchains atuais, utilizados pelas moedas digitais com maior participação no mercado, como o Blockchain do Bitcoin (BTC) e a rede Ethereum do Ether (ETH) não possuem um padrão. Por este motivo, a Linux Foundation, que é referência em implementação de padrões, decidiu iniciar o projeto Hyperledger como padronização para a indústria (BRADBURRY, 2017).

2.2 Contextualizando o conceito

Embora a moeda bitcoin seja para alguns uma coisa anárquica, usadas por traficantes, degenerados, muitos a associam a *DarkWeb*. A flutuação selvagem da moeda também é bastante questionável. Seria injusto não reconhecer o potencial revolucionário nas relações humanas e a evolução tecnológica que Nakamoto (NAKAMOTO, 2008) alcançou com sua solução.

Seria ainda mais injusto fechar os olhos para o potencial de aplicações que os blockchains proporcionam (ECONOMIST, 2015). Essa associação do Bitcoin a criminosos tem um viés difamatório. Como associar uma moeda virtual a meliantes ignorando o fato que durante séculos os meliantes sempre usaram as moedas convencionais?

No mesmo artigo a The Economist, conceitua o blockchain como "a máquina da confiança". O artigo afirma que seria injusto associá-lo a insegurança e volatilidade dos bitcoins. Os negócios baseados em blockchains proporcionam confiar em usuários

anônimos e em canais não confiáveis, como a internet.

Para Swan os novos paradigmas da computação surgem a cada década. Nos anos 70 surgem os mainframes, em 80 os computadores pessoais (Pcs), na década de 90 se populariza a internet, já no início do século XXI surgem as mídia sociais e dispositivos móveis com internet. Ao fim, os Blockchains seriam a revolução da década de 2010 (SWAN, 2015).

2.3 Funcionamento

Zheng (ZHENG et al., 2016) esclarece que o blockchain é essencialmente um livro razão ou conhecidos como *ledger* público no qual todas as transações realizadas são armazenadas em uma cadeia (ou uma lista).

Essa cadeia cresce progressivamente quando as novas transações são confirmadas. A fim de proteger o blockchain de adulteração em sistemas distribuídos um mecanismo complicado, mas seguro e baseado em criptografia assimétrica e consenso distribuído é utilizado para criptografar os registros das transações. A tecnologia de cadeias de blocos tem essencialmente as características chave como, a descentralização, a resistência, o anonimato, tolerância a falhas e a auditabilidade, o que permite que uma transação ocorra de forma descentralizada sem a necessidade de um intermediário central.

Para se entender a radical mudança de paradigma do blockchain é importante entender o conceito de "consenso descentralizado" e entender que ele quebra o velho paradigma de conformidade unificada, no qual uma base centralizada valida e controla as transações. Este modelo retira a entidade central e transfere a todos os usuários o controle e validação para uma rede *peer-to-peer* (P2P). (MOUGAYAR, 2016)

Todas as transações de bitcoins são enviadas para os usuários do blockchain, que contabilizam as operações em seus registro individuais de transações, os *ledgers*. Esse livro contábil ao se tornar público e compartilhado se mantém atualizado por meio dos blockchains. As transações que não forem reconhecidas pelos *ledgers* dos usuários do bloco não são validas. (STEINER et al., 2016)

Todos os usuários interagem com a rede blockchain através de um nodo no qual um usuário blockchain está instalado. Um grande número de nodos em toda a rede formam uma rede descentralizada. Uma vez que um nodo recebe dados de outro nodo, ele verifica a autenticação dos dados em seus *ledgers*.

Em seguida, transmite os dados validados para cada outro nó conectado a ele. Desta forma, os dados são espalhados por toda a rede. (ZHENG et al., 2016)

Segue na figura abaixo o processo de consenso dos blockchains de transações válidas.

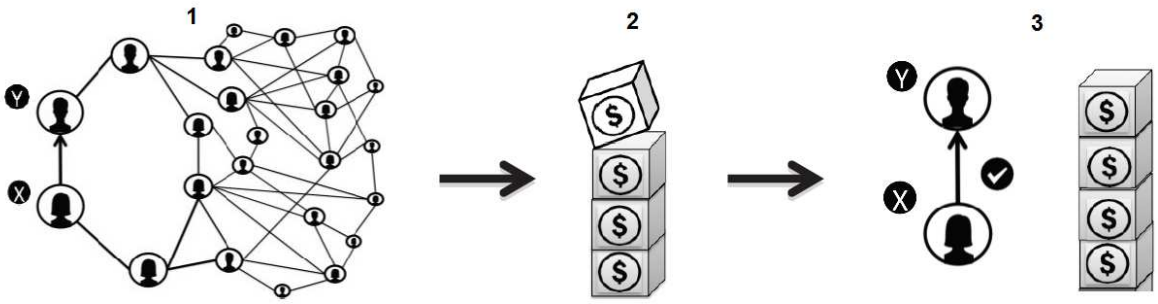


Figura 1 – Processo de consenso no blockchain

1. X realiza transação para Y, e a transação sendo aceita pelos nodos, é propagada para os outros nodos.
2. A validação dos nodos geraconsenso, que propagam a transação até o bloco em formação.
3. Quando o bloco se completade transações validas , B recebe a transação valida de A.

Já na hipótese de uma transação invalidada, ao consultar os próprios registros, caso o nodo não reconheça a transação, este retorna a transação ao emissor, não propagando uma informação invalida ao sistema todo. (ANTONOPOULOS, 2014)

Este *ledger* público, esta cadeia de blocos com registro imutáveis que é o blockchain, armazena o histórico de todas as transações já realizadas e validadas na cadeia de blocos. As transações que se propagam por estas redes estão todas criptografadas, sendo preservadas as identidades e as chaves de seguranças dos usuários, fato que não ocorre nas atuais transações de cartões de créditos. Dessa forma, não importa a confiabilidade do usuário e as redes que recebem as informações de uma transação de bitcoin. O fato mais importante é que as transações sejam propagadas e validadas entres os nodos do sistema. (ANTONOPOULOS, 2014). Mougayar (MOUGAYAR, 2017) ainda ressalta que o maior caminho da transação não é empecilho para o modelo blockchain, pelo contrário, quanto mais validada e reconhecida a transação, mais confiável ela será.

Este consenso compartilhado é que descentraliza o sistema e o transforma numa rede ponto a ponto (P2P). Não há usuários especiais. Todos os computadores conectados ao blockchain participam da rede e validações do sistema.

O sistema descentralizado evita a duplicidade de pagamentos, porém, torna as transações irreversíveis. Não há como mandar uma mensagem de cancelamento da transação a todos os nodos, nem interromper a propagação de informações válidas aos blockchains. Uma analogia ao modelo tradicional de comércio seria o pagamento errôneo, em notas de dinheiro, a um taxista. Dificilmente conseguiríamos encontrar o condutor novamente, e mais impossível ainda, seria impossibilitar o repasse da nota

de dinheiro. A irreversibilidade das operações se deve ao alto nível de segurança da criptografia do sistema.

As informações no Bitcoin só podem ser compartilhadas de forma pública graças a criptografia utilizada. A criptografia das transações de bitcoins utiliza o modelo de curvas elípticas, sendo assimétricas, baseadas em logaritmos discretos, expressado pela adição e multiplicação nos pontos de uma curva elíptica. Essas funções matemáticas não podem ser derivadas. São funções que podem produzir novos resultados, mas não voltam ao resultado anterior. Simplificando a ideia, os cálculos só andam pra frente. (ANTONOPOULOS, 2017)

O modelo utilizado no Bitcoin é a curva secp256k1, estabelecida pelo Instituto Nacional de Padronização e Tecnologia (NIST). Sendo que, o mod p (módulo de número primo) indica que essa curva está sobre um campo finito de números primos p, também escrito em formato latex: [$\mathbb{F}_p$], onde $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, um número primo muito grande. (ANTONOPOULOS, 2014)

A criptografia do Bitcoin é utilizada para criação dos endereços e senhas dos usuários, para os códigos das transações e para a formação dos blocos da cadeia. Essas criptografias são conhecidas como hash.

No sistema Bitcoin, para se gerar um novo bloco e manter a descentralização do sistema é necessário a resolução de uma prova-de-trabalho. Os nodos que buscam a solução das prova-de-trabalho (PoW) para a criação de um novo bloco são conhecidos como mineradores. Para se criar os blocos há um desafio a ser resolvido pelos mineradores. Se parece com uma corrida, em que o minerador que consegue aglutinar as transações e resolver o desafio primeiro se torna o criador de um novo bloco. Esse trabalho é recompensado pelo sistema com bitcoins. Também é dessa forma que são emitidos os novos bitcoins. Hoje para cada novo bloco descoberto o minerador recebe 12,5 bitcoins, e taxas sobre as transações no bloco minerado. Esse valor chegará a zero em 2040, quando os mineradores somente receberão as taxas sobre as transações. (ANTONOPOULOS, 2014)

3 TEORIA DOS JOGOS

3.1 Introdução

A Teoria dos Jogos, a qual poderia se chamar muito apropriadamente de Teoria das Decisões Interdependentes, tem como objeto de análise situações onde o resultado da ação de indivíduos, grupo de indivíduos, ou instituições, depende substancialmente das ações dos outros envolvidos. Em outras palavras, trata de situações onde nenhum indivíduo pode convenientemente tomar decisão sem levar em conta as possíveis decisões dos outros.

O primeiro passo para o seu desenvolvimento foi dado por von Neumann, em 1928, com a demonstração do teorema minimax. Contudo, só chamou a atenção do público em 1944, quando em parceria com Morgenstern, propôs a análise do comportamento econômico via perspectiva do "jogo de estratégia"criando assim a expectativa de reformulação da teoria econômica numa base totalmente nova, na qual o conceito de "processo competitivo"seria reestruturado em termos de mecanismos onde os agentes econômicos atuam estrategicamente. (NEUMANN; MORGENSTERN, 2007)

Neste primeiro momento, as aplicações mais bem sucedidas se realizaram no campo da análise de mercados oligopolistas, onde obtiveram resultados interessantes, contudo ainda limitados pelos recursos matemáticos específicos disponíveis.

Na década de 50 surgem novos horizontes. Em 1950, John F. Nash demonstra o teorema minimax para grandes números de agentes. Em 1952, Lloyd Shapley apresenta o conceito de "núcleo". E em 1959, Martin Shubik demonstra que a clássica "curva de contrato"de Edgeworth era idêntica ao conceito de solução desenvolvido por Shapley permitindo a teoria neoclássica se livrar de um dos seus principais problemas metodológicos. Naquele momento, enquanto a análise do problema do equilíbrio geral, conduzida principalmente por Arrow, Debreu e McKenzie, era estritamente paramétrica, ao considerar os agentes econômicos como "tomadores de preços", a Teoria dos Jogos, de posse de novos recursos técnicos, permitia analisar a questão da formação de preços como produto de um amplo processo de barganha multilateral.

Nos anos 60 a popularidade da teoria entrou novamente em estado latente. Seu debate ficou restrito apenas a alguns pequenos grupos de pesquisadores desmotivados a publicar os resultados de suas pesquisas. Esse fenômeno já havia, de certa forma acontecido nos anos 50, quando por alguns anos tornou-se praxe publicar apenas partes dos resultados das pesquisas realizadas. Os resultados foram muito pouco divulgados. Um exemplo importante foi o Folk Theorem que, devido a esse tipo de comportamento,

ficou praticamente desconhecido por um período de tempo considerável.

A partir da segunda metade dos anos 60, engenheiros e economistas começaram a perceber a Teoria dos Jogos como um instrumento de considerável alcance para uma velha questão que voltara a tomar fôlego: a análise, projeto e implementação de mecanismos de alocação de recursos. O principal protagonista desta questão foi HURVICZ (1973). Sua preocupação central estava voltada para a análise institucional, especialmente em economias informalmente descentralizadas. Para tal propósito, se envolveu na construção de mecanismos de alocação ou de planejamento que produzissem resultados "satisfatórios". Como cada mecanismo de alocação de recursos contém implicitamente definido um jogo, abre-se assim um novo campo de pesquisa: a análise e projetos de mecanismos de alocação de recursos através das técnicas da Teoria dos Jogos.

A literatura concernente à teoria da escolha social também acabou se constituindo em uma fonte de pesquisa para a Teoria dos Jogos. Este campo de pesquisa teve origem quando GIBBARD (1973) e SATHERHWAITE (1975), independentemente, resolveram indagar o que aconteceria se os agentes estudados por ARROW (1965) votassem estrategicamente ou de uma forma que não fosse isomórfica em relação às suas verdadeiras preferências. A resposta encontrada foi como era de se esperar, que as regras de votação usualmente utilizadas podem permitir escolhas sociais que não sejam "ótimos de Pareto". A análise desta questão acabou gerando um campo de pesquisa onde se procura desenvolver jogos que possam representar mecanismos de escolha, onde os agentes envolvidos são incentivados a votarem estrategicamente. (ARROW, 2012)

Outro campo de pesquisa também desenvolvido na década de 70 diz respeito à distribuição de custo conjunto. A Teoria dos Jogos tem se dedicado de forma brilhante também a essa questão e tem se destacado ao analisar e propor soluções para situações concretas.

Cabe ressaltar que a análise do equilíbrio geral desenvolvida pela Teoria Neoclássica tem sido suplantada quase que completamente pela Teoria de Jogos não cooperativos, principalmente a partir da segunda metade década de 80, quando a atenção de muitos pesquisadores tais como, por exemplo, JACQUEMIN (1987), TIROLE (1988), FARREL e MASKIN, (1989), KREPS (1990) e FUDENBERG (1991), vêm sendo dirigida para modelagem de jogos dinâmicos, levando em conta a hipótese de informação imperfeita e de informação incompleta. A possibilidade das firmas fazerem coalizões, em modelos dinâmicos, tem se mostrado maior que em modelos estáticos e oferecido razoáveis subsídios para estabelecimento de política antitruste.

Dada a necessidade de entendermos melhor a amplitude das aplicações que citamos acima, as quais em sua maioria serão detalhadas em (FIGUEIREDO; SALOMÃO, 1993), vejamos como ela pode ser formalizada.

Um jogo pode ser exposto matematicamente de diversas maneiras, isto é, de acordo com as propriedades dele que desejamos explorar. Nosso objetivo aqui é dar-lhe a expressão mais geral possível sem deixar escapar as suas propriedades mais essenciais.

A forma mais detalhada de se apresentar um jogo é na forma extensiva a qual se refere à descrição concentrada no movimento sequencial do mesmo. Nessa forma as decisões são tomadas uma após a outra. O conceito de estratégia tomado como a descrição completa de como uma pessoa que participa de um jogo pode agir sob quaisquer circunstâncias, ou um curso de ação qualquer de um agente em um jogo na forma extensiva, nos permite definir e expressar o jogo em uma forma mais simples e objetiva, e por isso de maior importância teórica, chamada forma normal ou forma estratégica. Podemos expressar um jogo na forma normal utilizando apenas as estratégias disponíveis para cada jogador e os respectivos resultados associados a cada elemento do conjunto constituído do produto cartesiano dos conjuntos de estratégias individuais. Podemos dizer ainda que um jogo está na forma normal quando toda a sequência de decisões que devem ser tomadas enquanto ele se processa na forma extensiva pode ser reunida em uma única e particular decisão para o jogador: a escolha de uma estratégia. Todo jogo na forma extensiva pode ser expresso na forma normal (RAIFFA; LUCE, 1957). Representa-se o jogo na forma extensiva só quando se faz necessário, para seu tratamento teórico, o conhecimento de certas propriedades que estão associadas ao movimento sequencial do processo de tomada de decisão.

Muitas vezes o tratamento da questão em análise exige muito menos informação do que as apresentadas pela forma normal, necessitando apenas o conhecimento do conjunto de resultados que cada jogador ou coligação de jogadores pode garantir para eles próprios, se eles agem como equipe, independentemente do que o restante dos jogadores possa fazer contra eles. Quando representamos o jogo fazendo uso apenas dessas informações dizemos que o mesmo está na forma de função característica.

Um jogo também pode se diferenciar de acordo com o conjunto de informações que os jogadores possuem. Um jogo é de informação completa ou de informação incompleta se cada jogador conhece ou não as seguintes informações: (a) o conjunto de jogadores; (b) as estratégias disponíveis para cada jogador; e (c) todos possíveis jogador conhece (a), (b) e (c) e é informação de incompleta quando um ou mais jogadores desconhecem alguma das informações citadas. Em relação aos lances ou movimentos, um jogo pode ser de informação perfeita e de informação imperfeita. Um jogo é de informação perfeita se a cada movimento todos os jogadores conhecem as escolhas feitas nos movimentos anteriores. Caso esta condição não ocorra, o jogo é de informação imperfeita.

Uma situação para ser considerada como jogo, teria que apresentar a existência de conflito e interdependência entre as decisões dos participantes. Esta é a caracterização

mais abstrata que podemos fazer de um jogo. No entanto, num plano mais concreto, podemos identificar dois tipos de jogo: (1) o jogo não cooperativo, quando as condições orgânicas do mesmo não permitem a formação de coalizões que possam determinar o resultado do jogo, e (2) o jogo cooperativo, quando as próprias condições orgânicas do jogo permitem a possibilidade dos participantes atuarem por meio de coalizões.

Iremos ilustrar a serventia da teoria dos jogos utilizando como exemplo uma das mais importantes batalhas da Segunda Guerra Mundial: a batalha do mar de Bismarck.

O alto comando do exército japonês decidiu transferir um maciço reforço, com a finalidade de se recuperar de uma derrota e preparar uma próxima ofensiva. Contudo, a movimentação de um volume grande de tropas por mar tinha um risco elevado: o poderio aéreo aliado na área era fortíssimo.

Um dado importante da situação era o fato de que o comboio japonês dispunha de duas rotas alternativas: a rota pelo sul, que apresentava tempo bom e boa visibilidade, e a rota pelo norte, que apresentava tempo ruim e baixa visibilidade. As forças aliadas, porém, somente possuíam aviões de reconhecimento para pesquisar uma rota por vez, sendo que a busca em qualquer uma das rotas consumiria um dia inteiro.

Dessa forma, se as forças aliadas enviassem seus aviões para a rota certa, poderiam começar a atacar de imediato. Porém, se mandassem os aviões para a rota errada, perderiam um dia de bombardeios. Os aliados também sabiam que se os japoneses escolhessem a rota sul e fossem localizados de imediato, o tempo bom garantiria três dias de bombardeio.

A melhor situação para os aliados aconteceria se eles escolhessem a rota sul e os japoneses também tivessem escolhido essa rota, uma vez que seria possível efetuar os ataques por três dias. A pior situação para os aliados seria se eles fossem para o sul e os japoneses fossem para o norte, onde perderiam um dia por ter escolhido a rota errada e outro dia devido ao mal tempo, dispondo de apenas um dia para o bombardeio.

Caso os japoneses tivessem escolhido a rota norte e os aliados também, estes perderiam apenas um dia de bombardeio devido ao mau tempo. Por último, se os japoneses escolhessem a rota sul e os aliados escolhessem a rota norte, perderiam um dia em função do engano e teriam dois dias para o bombardeio.

A tabela 1 abaixo demonstra as possibilidades que podem ocorrer no evento.

Tabela 1

Forças Aliadas	Comboio Japonês	
	Rota Sul	Rota Norte
Rota Sul	Três dias de bombardeio	Um dia de bombardeio
Rota Norte	Dois dias de bombardeio	Dois dias de bombardeio

Fonte: (FIANI, 2006)

Conforme o demonstrado acima, se você fosse do comando aéreo aliado, qual rota escolheria?

Verificando a tabela acima, fica clara a resposta: você deve mandar os aviões fazerem a busca primeiramente pela rota norte. Isso por que enquanto para os aliados a melhor estratégia depende da escolha dos japoneses, e para os japoneses a rota norte era a melhor escolha caso os aliados escolhessem a rota sul e era uma opção tão boa quanto a rota sul caso os aliados escolhessem a rota norte.

A rota norte acarretaria um número menor de dias de bombardeio em um caso e igual número de dias de bombardeio em outro, a rota norte era a melhor opção para o comboio japonês, dado que o objetivo era minimizar suas perdas. Consciente disso, os aliados enviaram seus aviões para a rota norte.

Assim, os aliados "adivinharam" por aonde os japoneses viriam considerando principalmente dois pontos: (1) que os japoneses agiriam racionalmente (não se exporiam a perdas desnecessárias); e (2) os dados da situação (o número de dias de bombardeio que o tempo em cada rotina permitiria). Era uma boa aposta, e como a história demonstrou, foi bem-sucedida.

3.2 Elementos Constituintes

A Teoria dos jogos é formada por um conjunto de elementos que constroem a sua estrutura e aplicabilidade, estes componentes são: os jogadores, as estratégias, as regras e os payoffs (D'AMICO, 2008).

3.2.1 Jogadores

Jogadores são agentes que tomam decisões. De acordo com Souza (SOUZA, 2003), o "homem como jogador se comporta de forma a atingir seus objetivos, planejando diferentes estratégias, decidindo ao mesmo tempo como agir nos segmentos sociais em que está inserido". Contudo, mesmo que os jogadores possuam interesses divergentes, estes não são necessariamente opostos, podem convergir, em lugar de sempre divergir (BÊRNI, 2004). Convém destacar, que o enfoque político descrito por Simões (1993) e exposto no capitulo dois, encontra-se implícito no exercício de poder entre os jogadores em interação estratégica, na medida em que, estas interações preveem a possibilidade de um sujeito, grupo, organização ou partido, denominado A, decidir ou influenciar a decisão de B, também entendido como um sujeito, grupo, organização ou partido (D'AMICO, 2008).

3.2.2 Estratégias

Sob o enfoque da Teoria dos Jogos as estratégias são entendidas como um plano de ações que especifica, para determinado jogador, que atitude considerar nos momentos em que ele terá de decidir o que fazer (FIANI, 2006). Percebemos que o conceito está relacionado à tomada de decisão do agente frente às situações vivenciadas no momento e no futuro, referindo-se à decisão do que e porque fazer, assim como jogar o jogo em cada contingência. Vincula-se com os preceitos da escola do planejamento, pois pressupõe um plano, uma formalização de como agir; e a escola do posicionamento, na medida em que cada escolha busca o alcance de uma posição mais favorável estrategicamente para o jogador.

Estratégia é um plano contingente, deve-se estudar o antes, o durante e o depois de todas as partidas, atuando de forma ativa e preventiva, simulando cenários que tragam mais segurança e otimização, em vez de ser reativo.

3.2.3 Regras

As regras são um conjunto de princípios, normas e preceitos que norteiam as ações dos jogadores. Em Teoria dos Jogos inexiste um conjunto universal de regras, estas são estipuladas de acordo com o tipo de jogo, as características dos jogadores envolvidos, as estratégias estipuladas, as formas de interação abarcadas, e as relações de poder exercidas.

3.2.4 Payoffs

Fiani (2006) refere-se ao payoff como a função de recompensa a cada jogador, aquilo que obtém depois de encerrado o jogo, de acordo com as próprias escolhas e as dos demais jogadores. Em alguns jogos isso é simples como declarar um vencedor ou um vencido; em outros, pode traduzir-se em um valor numérico, numa quantidade de dinheiro ou de pontos; enfim, o que seja capaz de ajudar o jogador a perceber como ele avalia determinado resultado do jogo (FIANI, 2006).

A hipótese de racionalidade, implícita na Teoria dos Jogos, envolve a busca de recompensas, fazendo-se necessário que cada jogador tenha conhecimento do perfil do "oponente" e saiba quais são os objetivos destes jogadores e seus possíveis payoffs, ou melhor, as buscas que estão almejando, os resultados que estão esperando (FIANI, 2006).

A Teoria dos Jogos consiste, portanto, num processo no qual dois ou mais agentes sociais (jogadores), tomam decisões, a partir de uma estrutura de regras que pode ser formal ou informal. Cada combinação de decisões e ações, são entendidas como um conjunto de movimentos a partir de estratégias, e determinam uma situação. Ao

pressupor as diversas possibilidades de escolha dos agentes implicados no processo de ação e reação, pode ser obtida uma variedade de combinações possíveis. O papel dos objetivos é fundamental, pois mesmo que estes sejam inicialmente conflitantes, existe a probabilidade dos agentes rumarem à cooperação, e a convergência pode tornar-se mais favorável do que a divergência na obtenção de payoff (D'AMICO, 2008). É exatamente esta uma das perspectivas que aproximam a Teoria dos Jogos do papel estratégico das relações públicas.

Uma vez conhecidos os elementos que compõem a Teoria dos Jogos (jogadores, estratégias, regras e payoffs), interessa-nos entender como estes são assimilados nos jogos (situações de interação) que constituem esta teoria.

3.3 Classificação e Natureza dos Jogos

Este item busca evidenciar a ligação da Teoria dos Jogos com a cooperação. Assim a classificação e a natureza dos jogos estudados pela Teoria dos Jogos evidenciam as condições que favorecem a cooperação. Para D'Amico (2008): *"Tem-se, assim, na busca pela cooperação, forças diferentes, mas que podem ser unificadas. Isso porque o ser humano não é movido somente por forças divisoras, isto é, conflitantes, de competição, nem somente por forças unificadoras, de cooperação. Constata-se assim, que é do equilíbrio, da busca por igualdade de forças em oposição de que vivem as sociedades (D'AMICO, 2008)."*

Souza (2003) acrescenta que a comunicação entre as partes que interagem, em jogos cooperativos, é fundamental conciliando os interesses dos participantes. Em Teoria dos Jogos, classificam-se os jogos com base dois critérios: um em que inexiste comunicação efetiva entre os jogadores, os jogos não-cooperativos, e outro nos quais os jogadores podem comunicar-se livremente, os jogos cooperativos. (SOUZA, 2003)

De acordo com Fiani (2006) e Bêrni (2004), em jogos cooperativos as coalizões existem e são permitidas. O termo coalizão possui inúmeros sinônimos em jogos cooperativos, e podem ser usados termos como acordo, contrato, pacto e/ou compromisso. Essa coalizão, contudo, necessita exprimir as relações mútuas, o que vem ao encontro do princípio de simetria nos relacionamentos destacado por Grunig (2009). Para que isso ocorra é imperativo que nos jogos cooperativos sejam possíveis a ordenação e à aplicação de planejamento e estratégias em conjunto pelos jogadores (BÊRNI, 2004). De acordo com D'Amico (2008) aponta-se, portanto, a evidência de que em jogos cooperativos a comunicação entre as partes é componente fundamental. Esta abordagem dos autores permite inferir que os jogos cooperativos encontram-se pautados pelos pressupostos da escola cultural (MINTZBERG, 2000) onde o processo de desenvolvimento de estratégias é descrito como sendo essencialmente coletivo e cooperativo. Enfatizam também, a importância da comunicação simétrica que viabiliza a possibilidade de jogos cooperativos.

(BÊRNI, 2004), (CASTRO; RIBEIRO, 2000), (FERRARI; FRANÇA; GRUNIG, 2009)

Os jogos não-cooperativos incluem um confronto de interesses estritamente competitivos. Nesse tipo de jogo, apresentam-se situações extremas, nas quais, para um jogador ganhar, o outro tem de necessariamente perder, ou então as partes terminam o jogo (processo de interação) sem saldo algum. Nasch (1953) evidenciava que cada participante, ao atuar independentemente, sem colaboração, não se comunicava com os demais jogadores; jogos não-cooperativos proíbem que a comunicação prévia seja estabelecida. Uma vez que a comunicação é proibida, conforme discorre Almeida (2005), os jogadores não podem entrar em acordos ou firmar compromissos com os demais, estando impossibilitados de buscar a maximização de payoffs coletivos, sem beneficiar os outros envolvidos, alicerçando seus ganhos somente de forma individual. Este tipo de jogo, de conduta egoísta, não se enquadra nos preceitos das relações públicas, pois uma organização com tal postura, só faria ampliar as divergências e os conflitos com outros agentes com os quais estivesse em interação. (FRIEDMAN, 1977)

Além de diferentes tipos de classificação, os jogos possuem naturezas distintas em termos de soma de todos os payoffs dos participantes. Por isso, de acordo com D'Amico (2008), os jogos dividem-se em: de soma zero e de soma não-zero.

Em jogos de soma zero inexiste a possibilidade de cooperação, pois há dois agentes egoístas competindo (SILVA, 2004). Estes jogos são do tipo tudo ou nada. Os jogadores estão preocupados em infligir, segundo Fiani (2006), o maior dano possível uns aos outros, pois os lucros de um jogador são exatamente iguais às perdas de seu oponente, por isso recebem a denominação de jogos de soma zero. Esta classificação de jogos (interações) pode ser relacionada aos princípios da estratégia competitiva em negociação, pois conduz a um resultado ganha-perde, distanciando-se da possibilidade de desenvolvimento de relacionamentos simétricos que possibilitem o surgimento de confiança e cooperação entre os agentes envolvidos. (SOUZA, 2003)

Em contraponto, em jogos de soma não-zero os jogadores podem se beneficiar mutuamente. Para Souza (2003), jogos de soma não-zero indicam situações em que a colaboração é favorável, e o desenvolvimento de confiança entre as partes que interagem aparece neste tipo de jogo, pois não há nem ganhadores nem perdedores, as partes ganham ou perdem juntas. Em termos de payoffs, todos os jogadores se empenham para que ocorra, sendo ele de maior alcance possível, pois a vitória de um jogador não é necessariamente desfavorável à outra parte (SOUZA, 2003). Os jogos de soma não-zero estão relacionados à estratégia colaborativa em negociação, pois direcionam os resultados a um ganha-ganha. Quando isso não ocorre, tem-se no mínimo, o desenvolvimento de uma estratégia de compromisso, onde os agentes envolvidos mantém o relacionamento e buscam melhores resultados em futuras interações.

É, portanto, um estilo de interação (jogo, em Teoria dos Jogos) mais apropriado

à prática das relações públicas, que buscam promover a colaboração entre agentes do sistema social organização-públicos, pautada pela simetria e confiança mútua. D'Amico (2008) corrobora com esta ideia, e destaca:

"Para ter mais sucesso, portanto, num mundo em que a competição é extrema, Wright (2001) acredita que ele deve fazer mais uso dos conceitos de jogos de soma não-zero, aplicando os seus princípios no dia-dia de maneira planejada. Como a medida do êxito não é proporcional ao tanto que o indivíduo A ganhou (a mais) que o indivíduo B, mas se A adquiriu o que queria porque B permitiu-lhe realizar seus sonhos e fazer o que quisesse, tem se aí o caminho por onde todos podem ganhar (D'AMICO, 2008)."

Quanto aos exemplos dos jogos de soma não-zero, destacamos o mais conhecido, o Dilema dos Prisioneiros, que apresentaremos a seguir, bem como o Equilíbrio de Nash, teoria responsável pelo avanço nos estudos dos jogos de soma não-zero.

3.4 Teoria da Escolha Racional

A teoria dos jogos visa explicar como esses jogadores fazem as suas escolhas em situações de interação estratégica. Para verificar como os jogadores tomam as suas decisões, temos de considerar as preferências desses jogadores, pois essas preferências é que irão nortear suas escolhas.

Apresentaremos a teoria da escolha racional, essa teoria parte das preferências dos jogadores para entender suas escolhas, assumindo como princípio básico a ideia de que os jogadores são racionais.

Grande parte dos modelos de teoria dos jogos parte do pressuposto de que os jogadores são supostamente racionais. Afirmar que os jogadores são racionais em teoria dos jogos significa afirmar que as suas preferências são racionais.

A teoria econômica clássica nunca foi projetada para descrever a tomada de decisão quando se enfrenta um adversário inteligente, onde as ações também são influenciadas pelas ações de um concorrente. Isso ocorre por que, no mundo real, duas pessoas em competição, suas ações e a ações de seu adversário formam um sistema dinâmico. Compreender o funcionamento desse sistema e a incertezas que o cercam não é possível utilizando as abordagens contidas na economia clássica.

A teoria da escolha racional envolve quatro pressupostos principais (faremos as devidas críticas mais adiante) que são: (1) as pessoas possuem conhecimento exato sobre o jogo em questão; (2) as pessoas possuem racionalidade ilimitada; (3) os equilíbrios são atingidos de imediato e (4) as pessoas são motivadas puramente por interesses próprios.

3.5 Estratégias Mistas

Antes de falarmos sobre as estratégias mistas, falaremos brevemente sobre o conceito de estratégias puras. Este tipo de estratégia ocorre quando um jogador escolhe uma estratégia de forma definitiva, ou seja, cada agente faz uma escolha e a mantém.

Todavia, outra forma de pensar é permitir que os agentes randomizem (veremos mais à frente esse item detalhadamente) suas escolhas, atribuindo uma probabilidade para cada escolha e joguem suas escolhas de acordo com essas probabilidades.

Para um melhor entendimento do funcionamento desse tipo de estratégia, usaremos um exemplo que consiste em um jogo de fácil entendimento, o conhecido "pedra, papel e tesoura". Nesse jogo, cada jogador escolhe simultaneamente entre pedra, papel e tesoura. As regras são bastante simples: pedra vence a tesoura; tesoura vence o papel e papel vence a pedra.

É de conhecimento comum que a melhor estratégia para obter um melhor resultado é escolher de forma aleatória um dos três resultados possíveis. Porém segundo Varian (2009) "os seres humanos não são necessariamente tão bons em escolher resultados de forma totalmente aleatória". Sendo assim, é possível prever, com algum grau de acerto, as escolhas de seu oponente, levando vantagem no decorrer do jogo. (VARIAN, 2006)

3.6 Equilíbrio de Nash

Podemos definir o equilíbrio de Nash como sendo a situação em que cada estratégia é a melhor resposta possível às estratégias dos demais jogadores, e isso é verdade para todos os jogadores. Lembramos que nenhuma pessoa sabe o que a outra fará quando for sua vez de escolher a estratégia. Porém, cada pessoa tem suas expectativas a respeito de qual será a escolha do outro jogador.

O equilíbrio de Nash pode ser interpretado com um par de expectativas sobre as escolhas da outra pessoa, de modo que, quando a escolha de uma pessoa for revelada, nenhuma delas quererá mudar seu próprio comportamento. Outro modo de visualizar o equilíbrio de Nash é a situação onde todas as estratégias adotadas por todos os jogadores sejam as melhores respostas às estratégias dos demais. Isso tem implicações enormes em um sistema de computador distribuído como o blockchain. Na verdade, o blockchain é "livre de fraude"porque todo o protocolo está em um Equilíbrio de Nash. Vamos discutir isso mais tarde, mas por enquanto, vamos ver o Equilíbrio de Nash em ação em um dos mais famosos conceitos da teoria dos jogos.

Embora sendo bastante utilizado, o equilíbrio de Nash possui alguns problemas. Primeiro, um jogo pode ter mais de um equilíbrio de Nash. Essa situação ocorre quando

mais de uma combinação de estratégias maximiza a utilidade dos jogadores. O segundo problema é que há jogos que não possuem equilíbrio de Nash.

Para um melhor entendimento, serão expostas abaixo duas situações: uma onde há mais de um equilíbrio de Nash e uma situação onde não existe equilíbrio de Nash.

O jogo da tabela 2 abaixo representa uma situação de interação estratégica em que um fabricante de sistemas operacionais (SOp) tem que decidir se desenvolve ou não uma nova ferramenta em seu sistema operacional, e uma empresa que produz um software antivírus (AV) tem de decidir, simultaneamente, se atualiza seu software para a nova ferramenta a ser introduzida no sistema operacional. (NASH, 1951)

Tabela 2

Sistema Operacional	Antivírus	
	Atualizar	Não Atualizar
Desenvolver	2,1	-1,-2
Não Desenvolver	0,-1	1,2

Fonte: (FIANI, 2009)

Nesse jogo, embora as empresas não mantenham contato para coordenar suas decisões, ambas têm interesse em uma solução conjunta, uma vez que decisões divergentes (se SOp desenvolve a nova ferramenta e a AV não atualiza seu programa, ou se a SOp não desenvolve a nova ferramenta enquanto AV atualiza seu programa) trazem prejuízos para ambas.

A presença de mais de um equilíbrio de Nash é o que ocorre nesse jogo. Assim como temos um equilíbrio de Nash na combinação (desenvolver, atualizar), temos outro equilíbrio de Nash na situação (não desenvolver, não atualizar).

Vejamos agora um caso em que não há equilíbrio de Nash. Usaremos um jogo conhecido por ter que combinar moedas. Neste jogo, dois jogadores exibem, ao mesmo tempo, uma moeda que esconde em sua mão. Se ambas apresentarem o mesmo resultado (cara – cara ou coroa-coroa), o jogador 2 dará a sua moeda ao jogador 1. Caso apresentem resultados diferentes, o jogador 1 dará a sua moeda ao jogador 2. Esse jogo está representado abaixo.

Tabela 3

Jogador 1	Jogador 2	
	Cara	Coroa
Cara	1,-1	-1,1
Coroa	-1,1	1,-1

Fonte: (FIANI, 2009)

Como pode ser visto, não existe combinação de estratégias que atendam os requisitos para ocorrer o equilíbrio de Nash, uma vez que, qual seja a combinação, algum dos jogadores não terá sua utilidade maximizada.

3.7 Jogos Sequenciais

Definiremos jogos sequenciais como a situação em que o jogador toma a sua decisão já conhecendo a escolha do outro jogador. Dessa forma, ao ter que tomar a sua decisão, o jogador possui maior informação sobre o outro jogador.

A situação exposta acima, juntamente com o fato de considerarmos que os jogadores são racionais, não nos permite supor que os jogadores tomem suas decisões ignorando o que o outro jogador decidiu em etapas anteriores, uma vez que ele terá conhecimento dessa situação.

Em teoria dos jogos, um jogador que ignorasse os acontecimentos do jogo até o momento em que tem de tomar a sua decisão, estaria agindo de forma irracional, uma vez que ele não estaria empregando de forma eficiente um dos meios que dispõe para alcançar o seu objetivo.

Trataremos a questão dos jogos sequenciais por meio de um exemplo econômico.

Nosso exemplo consiste na interação estratégica entre duas empresas – uma que deseja entrar em um mercado qualquer e outra que já encontra neste mercado. Chamaremos a primeira de desafiante e a segunda de dominante.

A empresa Desafiante possui duas estratégias: (1) entrar no mercado e (2) não entrar no mercado. Quanto à Dominante, a mesma também possui duas possibilidades de ação: (1) luta ou (2) acomoda.

Com o dito acima, caracterizaremos a seguinte situação: Caso a empresa Desafiante decida não entrar, seu lucro será zero, enquanto o lucro da Dominante é máximo, 10 milhões. Caso a desafiante decida entrar no mercado e a dominante decidir lutar, a desafiante terá um prejuízo de um milhão (-1), e os lucros da dominante será reduzido para a quantia de dois milhões. Por fim, se a dominante optar pela acomodação à entrada da desafiante, os lucros desta serão de três milhões, enquanto do daquela será de sete milhões.

Para efeito ilustrativo, segue tabela com as possibilidades do jogo.

Tabela 4

Desafiante	Dominante	
	Luta	Acomoda
Entra	-1,2	3,7
Não Entra	0,10	0,10

Fonte: (FIANI, 2009)

Analisaremos primeiramente a situação do desafiante. Caso o dominante decida lutar, o melhor que o desafiante tem que fazer é não entrar, pois nesta situação ela obtém uma recompensa de zero, contra uma recompensa de -1 caso decida entrar. Caso

a dominante decida acomodar, o melhor que a desafiante tem de fazer é entrar, já que obterá uma recompensa de 3 milhões.

Vejamos agora o caso da dominante. Caso a desafiante decida entrar, o melhor que a dominante tem a fazer é acomodar, pois obterá um lucro de 7 milhões, valor superior aos 2 milhões caso opte por lutar. Por outro lado, caso a desafiante decida não entrar, não há uma estratégia que unicamente seja a melhor para a dominante, pois em qualquer caso, ela terá um lucro de 10 milhões.

Caso a desafiante decida entrar, o melhor que a dominante tem a fazer, conhecendo essa decisão da desafiante, é acomodar. Já tendo à empresa dominante tomado a decisão de acomodar, a decisão da desafiante de entrar no mercado torna-se uma escolha racional.

Verificando a tabela 4 acima, será razoável concluir que a estratégia "Luta" nunca será decidida pela empresa dominante. Caso se apresente a situação em que seja necessário empregar a estratégia "Luta", essa escolha seria irracional por parte da empresa dominante. Mas por que isso ocorre?

Essa situação ocorre pelo fato de que o equilíbrio de Nash apenas exige que as estratégias empregadas pelos jogadores sejam as melhores respostas umas às outras, sem considerar a ordem em que os jogadores tomam suas decisões. Mais especificamente, caso o desafiante escolha não entrar, a resposta da dominante de torna irrelevante para a determinação dos lucros.

3.8 Jogos Repetidos

São processos que envolvem etapas que repetem. Nesse caso existem novas possibilidades estratégicas abertas para os jogadores. Esse tipo de jogo pode ser com um número fixo de vezes ou com um número de vezes indefinido.

Em contrapartida, nos jogos repetidos com um número fixo de vezes temos uma situação em que "burlar" pode ser a melhor alternativa para os jogadores. Consideremos uma situação em que os jogadores sabem a quantidade de "rodadas" que irão ocorrer. Neste caso será de dez. Onde chegamos à última rodada. Assim sendo, caso "burlar" for a estratégia que maximize a utilidade do jogador, ele a adotará, uma vez que não terá possibilidade do outro jogador retaliar essa escolha.

Para o melhor entendimento dos jogos com um número indefinido de vezes, trataremos a definição acima por meio de um exemplo.

Temos uma relação comercial entre duas empresas, em que uma das empresas adquire matéria-prima da outra, onde deverá ser entregue com determinada característica e em um dado prazo. Ao mesmo tempo, para poder oferecer essa matéria-prima, a

empresa produtora tem de realizar alguns investimentos, deixando de certa forma a empresa produtora na dependência de que seus compradores cumpram o acordado.

Nessa situação, percebemos que para o funcionamento e o consequente lucro das empresas em questão, se faz necessário que ambas cumpram com o combinado, acarretando assim em uma maximização da utilidade.

3.9 Jogos de Coordenação

São os jogos em que os ganhos dos participantes são maiores quando existe uma coordenação em suas estratégias. Porém, como veremos mais adiante, desenvolver essa coordenação é um entrave para o aumento dos ganhos dos jogadores.

Daremos como exemplo de jogos de coordenação o conhecido dilema do prisioneiro.

A discussão original do jogo trata de uma situação em que dois prisioneiros, comparsas em um crime, eram interrogados em locais separados. Cada prisioneiro tinha a opção de confessar o crime (envolvendo o companheiro) ou negar sua participação no crime.

Deste modo, teremos a seguinte situação: se apenas um prisioneiro confessar o crime, ele seria libertado e o outro condenado a seis meses de prisão; se ambos negassem envolvimento com o crime, seriam presos por apenas um mês (questões burocráticas); e se ambos confessassem, seriam presos por três meses.

Demonstraremos a situação por meio da seguinte tabela 5 abaixo:

Tabela 5

Suspeito 1	Suspeito 2	
	Confessa	Nega
Confessa	-3,-3	0,-6
Nega	-6,0	-1,-1

Fonte: (FIANI, 2009)

Vamos verificar a situação do suspeito 1. Se o suspeito 2 negar ter cometido o crime, ele estará melhor se confessar, uma vez que será libertado. Caso o suspeito 2 confessar, ele estará melhor se confessar, onde obterá uma pena de três meses ao invés de uma pena de seis meses. Sendo assim, independentemente do que o suspeito 2 fizer, a melhor opção para o suspeito 1 será confessar.

O mesmo ocorre com o suspeito 2, ele estará melhor se confessar. Portanto, o único equilíbrio de Nash nesse jogo para ambos os suspeitos é confessar o crime.

Todavia, se ambos pudessem ter a certeza de que o outro não confessaria, eles ficariam apenas um mês presos. Conforme exposto acima, não existem meios dos

suspeitos coordenarem suas ações.

Um fator importante para o tratamento deste tipo de situação é a quantidade de vezes que o jogo é jogado. Onde podemos adotar uma estratégia caso o jogo ocorra uma única vez ou se for repetido uma quantidade de vezes. Analisaremos situações onde ocorrem jogos sequenciais e jogos repetidos.

3.10 Jogos de Competição

É o oposto dos jogos de cooperação. Têm como principal característica os ganhos de um jogador ser exatamente iguais às perdas do outro jogador, por isso também é conhecido como jogos de soma zero. Esse pode ser o caso se duas empresas estiverem disputando, por exemplo, aumentar suas participações em um dado mercado, onde o esse aumento se dará somente à custa da redução da participação da outra empresa.

Vamos ilustrar os jogos de competição a partir de uma disputa de pênaltis do futebol. Teremos dois jogadores, o goleiro e o chutador. O chutador pode escolher entre chutar para a direita ou chutar para a esquerda, e o goleiro pode optar pelos mesmos movimentos. Vamos representar os ganhos dessas estratégias em termos de pontos esperados. Obviamente, o chutador terá mais êxito se o goleiro escolher o lado contrário do qual ele bateu.

Todavia, o jogo pode não ser perfeitamente simétrico por que o chutador pode chutar melhor para determinado lado e o goleiro defender melhor em um dos lados. Vamos supor que o chutador faça o gol em 80% das vezes se chutar para esquerda e o goleiro pular para a direita, e apenas 50% das vezes, se o goleiro também pular para a esquerda. Caso o chutador escolha chutar para a direita, suporemos que ele terá êxito em 90% das vezes se o goleiro pular para a esquerda, mas apenas 20% caso o goleiro decida pular para a direita. Exporemos a situação conforme tabela seguinte.

Tabela 6

Chutador	Goleiro	
	Defende à Esquerda	Defende à Direita
Chuta para Esquerda	50,-50	80,-80
Chuta para Direita	90,-90	20,-20

Fonte: (FIANI, 2009)

3.11 Jogos com Punição

E se houver um cenário em que a solução ótima para ambos os jogadores esteja no cenário que tem má implicação para a sociedade? Pense nesse cenário em que Rob e

Ben (dois jogadores do novo exemplo) planejam um assalto a banco. Vamos fazer uma matriz de resultados positivos que eles obterão neste cenário:

Tabela 7

Rob	Ben	
	Não Rouba	Rouba
Não Rouba	3,3	0,6
Rouba	6,0	7,7

Como você pode ver, neste cenário hipotético, a melhor e mais ótima estratégia está em Rob e Ben roubando. Embora isso possa ser bom para ambos, não é um bom cenário para a sociedade.

É aí que entra a ideia de "punição".

O mundo não é necessariamente um lugar amável e justo. Os homens geralmente são muito corruptíveis e, se não forem mantidos sob controle. No mundo real, as pessoas geralmente terão muitas oportunidades de serem corrompidas sem qualquer consideração pela sociedade em geral. Então, a maneira como mantemos as coisas assim sob controle é implementando uma estratégia de punição.

Então, suponha que no exemplo mostrado acima nós tenhamos uma estratégia de punição que seja assim:

- Para cada -0,5 de utilidade tirada do público, um fator de punição de -7 será dado.

Em outras palavras, todo ato considerado "ruim"para a sociedade terá seu pagamento deduzido por 7 e custará -0,5 em utilidades para a sociedade. Agora, você pode estar pensando por que a sociedade fará algo assim? Há uma perda de utilidade para a sociedade, que pode ser dinheiro, tempo, qualquer coisa e, por outro lado, as pessoas que estão cometendo um crime estão recebendo uma punição terrível também.

Mas a verdade é que nós, como sociedade, sempre integramos isso em nossa vida diária. O que adicionar o fator de punição é reduzir o retorno das atividades “ruins” e alterar a matriz da seguinte forma:

Tabela 8

Rob	Ben	
	Não Rouba	Rouba
Não Rouba	3,3	0,-1
Rouba	-1,0	0,0

Veja como a recompensa da atividade “ruim” é deduzida por um fator de 7?

Como podemos observar, adicionando o fator de punição, o Equilíbrio de Nash muda de algo que poderia ter sido ruim para a sociedade para algo que é bom para a

sociedade. Então isso muda, Ben e Rob fazendo o assalto a Ben e Rob fazendo o assalto a banco, mas também enfrentando as conseqüências de uma punição.

Então, voltando à questão, qual o incentivo para uma sociedade passar pela punição? Por que eles vão querer desperdiçar suas utilidades? A maneira como as pessoas responderam a essa questão é tornando a punição obrigatória. Em outras palavras, se alguém é uma sociedade não concorda com a punição, então eles mesmos se tornam criminosos e estão sujeitos à punição.

Como isso se aplica em uma sociedade civilizada? Pense em uma força policial que é financiada por impostos tirados das pessoas. Neste caso, temos uma força especializada que distribuirá a punição e a forma como a sociedade participa dela é pagando seus impostos que financiam a força. Se você não pagar os impostos, estará sujeito a punição também.

Outro exemplo interessante de “punir os não-puníveis” é o ostracismo social. Pense em uma sociedade em que uma pessoa, diz Max, cometeu um crime. Instantaneamente ele se torna um pária na sociedade. Este é um cenário em que todos nessa sociedade estão participando da punição. Agora, suponha que alguém se misture com Max, essa pessoa também, por associação, se tornará “má” e, por sua vez, também será banida pela sociedade.

Não seria exagero dizer que esse mesmo conceito é a razão pela qual não estamos todos mortos agora.

O conceito de Equilíbrio e Punição de Nash tem implicações fundamentais no blockchain e mantém os mineiros ("jogadores"da rede) honestos. Vamos explorar isso mais a frente. (NASH, 1951)

4 DESENVOLVIMENTO DA RELAÇÃO

Como já mencionamos anteriormente, os blockchains são sistemas inerentemente descentralizados que consistem em diferentes atores que agem dependendo de seus incentivos e da informação que está disponível para eles.

Sempre que uma nova transação é transmitida para a rede, os nós têm a opção de incluir essa transação em sua cópia de seu livro ou ignorá-la. Quando a maioria dos atores que compõem a rede decide sobre um único estado, o **consenso** é alcançado.

Um problema fundamental nos sistemas de computação distribuída e multiagentes é alcançar a confiabilidade geral do sistema na presença de vários processos defeituosos. Isso geralmente requer que os processos concordem com algum valor de dados necessário durante o cálculo.

Esses processos são descritos como **consenso**.

- O que acontece quando esses atores são uma grande parte da rede, mas não a maioria?
- Para criar um protocolo de consenso seguro, ele deve ser tolerante a falhas.

Em primeiro lugar, falaremos brevemente sobre o Problema dos Dois Generais insolúvel. Depois, estenderemos isso ao problema dos generais bizantinos e discutiremos a tolerância a faltas bizantinas em sistemas distribuídos e descentralizados. Finalmente, discutiremos como tudo isso está relacionado ao espaço do blockchain.

4.1 O problema dos dois generais

Esse problema, publicado pela primeira vez em 1975 e dado seu nome em 1978 (AKKOYUNLU; EKANADHAM; HUBER, 1975), descreve um cenário em que dois generais estão atacando um inimigo comum. O general 1 é considerado o líder e o outro é considerado o seguidor. O exército de cada general por si só não é suficiente para derrotar o exército inimigo com sucesso, portanto eles precisam cooperar e atacar ao mesmo tempo. Este parece ser um cenário simples, mas há uma ressalva:

Para que eles se comuniquem e decidam por um tempo, o General 1 tem que enviar um mensageiro através do acampamento inimigo que irá entregar o tempo do ataque ao General 2. No entanto, existe a possibilidade de que o mensageiro seja capturado pelos inimigos. e assim a mensagem não será entregue. Isso resultará em atacar o General 1 enquanto o General 2 e seu exército mantêm suas bases.

Pela lógica, não podemos afirmar, com certeza, que ambos exércitos irão atacar simultaneamente às 6 horas da manhã do dia seguinte. Podemos afirmar que o general do General 2 nunca terá certeza que o mensageiro chegou até o exército General 1 confirmando o acordo de ataque.

Para provar nossa afirmação anterior, considere o seguinte contra exemplo, dentro do universo de possibilidades, em que o mensageiro foi atacado pelo exército B no meio do vale e não chegou até o exército General 1.

Logo, o general em General 1 irá achar que seu mensageiro foi atacado na ida e abortará o plano uma vez que o mensageiro nunca voltou. Se o general do General 2 executar o plano ele correrá o risco de perder a batalha, uma vez que o exército General 1 não irá atacar conforme o combinado. Anulando assim a certeza que os dois exércitos irão atacar conforme o suposto combinado.

Mesmo que a primeira mensagem passe, o General 2 tem que reconhecer (ACK, notar a semelhança com o handshake de 3 vias do TCP) que ele recebeu a mensagem, então ele envia um mensageiro de volta, repetindo o cenário anterior onde o mensageiro pode ser apanhado. Isso se estende a infinitos ACKs e, portanto, os generais não conseguem chegar a um acordo.

Com um protocolo determinístico, suponha que haja uma sequência de um número fixo de mensagens, uma ou mais entregues com sucesso e uma ou mais não. A suposição é que deve haver uma certeza compartilhada para ambos os generais atacarem. Considere a última mensagem desse tipo que foi entregue com sucesso. Se essa última mensagem não tivesse sido entregue com sucesso, então pelo menos um general (presumivelmente o receptor) decidiria não atacar. Do ponto de vista do remetente daquela última mensagem, entretanto, a sequência de mensagens enviadas e entregadas é exatamente a mesma que teria sido, se essa mensagem fosse entregue.

Como o protocolo é determinístico, o envio geral dessa última mensagem ainda decidirá atacar. Criamos agora uma situação em que o protocolo sugerido leva um general a atacar e o outro a não atacar - contradizendo a suposição de que o protocolo foi uma solução para o problema.

Com um protocolo não determinístico, suponha que uma contagem de mensagens variáveis. Dessa forma o contexto pode ser comparado a uma árvore finita, onde cada folha ou ramificação (nó) da árvore representa um exemplo explorado até um ponto especificado.

As raízes dessa árvore são rotuladas com as possíveis mensagens iniciais, e os nós das ramificações que derivam dessas raízes são rotulados com as possíveis próximas mensagens. Nós de folha representam exemplos que terminam depois de enviar a última mensagem. Um protocolo que termina antes de enviar qualquer mensagem é

representado por uma árvore nula.

Suponha que exista um protocolo não determinístico que resolva o problema. Então, por um argumento similar ao exemplo determinístico na seção anterior, onde um protocolo determinístico pode ser obtido a partir do não determinístico, removendo todos os nós foliares, o protocolo determinístico deve então também resolver o problema.

Como o protocolo não determinístico é finito , segue-se que o protocolo representado pela árvore vazia resolveria o problema. Claramente isso não é possível. Portanto, um protocolo não determinístico que resolve o problema não pode existir.

Dessa forma o problema dos dois generais provou ser insolúvel.

4.2 O problema dos generais bizantinos

Famosamente descrito em 1982 por Lamport, Shostak e Pease , é uma versão generalizada do Problema dos Dois Generais com uma reviravolta. Descreve o mesmo cenário, onde, em vez disso, mais de dois generais precisam chegar a um acordo sobre o momento de atacar seu inimigo comum. A complicação adicional aqui é que um ou mais dos generais pode ser um traidor , o que significa que eles podem mentir sobre a sua escolha (por exemplo, eles dizem que concordam em atacar às 9h00, mas em vez disso não o fazem). (LAMPORT; SHOSTAK; PEASE, 1982)

O paradigma líder-seguidor descrito no Problema dos Dois Generais é transformado em uma configuração de comandante-tenente. Para obter consenso aqui, o comandante e todos os tenentes devem concordar com a mesma decisão (por simplicidade de ataque ou recuo).

Byzantine Generals Problem. **A commanding general must send an order to his $n - 1$ lieutenant generals such that**

IC1. All loyal lieutenants obey the same order.
IC2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.

Figura 2 – Página 3, O problema dos generais bizantinos

Somando-se ao IC2, fica interessante que, se o comandante é um traidor, o consenso ainda deve ser alcançado. Como resultado, todos os tenentes tomam o voto majoritário.

O algoritmo para chegar a um consenso neste caso é baseado no valor da maioria das decisões que um tenente observa.

Teorema: Para qualquer m , o algoritmo OM (m) alcança um consenso se houver mais de 3 milhões de generais e no máximo m traidores.

Isso implica que o algoritmo pode chegar a um consenso, desde que 2/3 dos atores sejam honestos. Se os traidores são mais de 1/3, o consenso não é alcançado, os exércitos não coordenam seu ataque e o inimigo vence.

Algorithm OM(0).

(1) The commander sends his value to every lieutenant.
(2) Each lieutenant uses the value he receives from the commander, or uses the value RETREAT if he receives no value.

Algorithm OM(m), $m > 0$.

(1) The commander sends his value to every lieutenant.
(2) For each i, let v_i be the value Lieutenant i receives from the commander, or else be RETREAT if he receives no value. Lieutenant i acts as the commander in Algorithm OM($m - 1$) to send the value v_i to each of the $n - 2$ other lieutenants.
(3) For each i, and each $j \neq i$, let v_j be the value Lieutenant i received from Lieutenant j in step (2) (using Algorithm OM($m - 1$)), or else RETREAT if he received no such value. Lieutenant i uses the value *majority*($v_1, \ldots, v_{n-1}$).

Figura 3 – m = 0 → nenhum traidor, cada tenente obedece | m > 0 → a escolha final de cada tenente vem da maioria das escolhas de todos os tenentes

Isto deveria ser mais claro com um exemplo visual do ponto de vista do tenente 2 - Seja C Comandante e L (i) seja Tenente I:

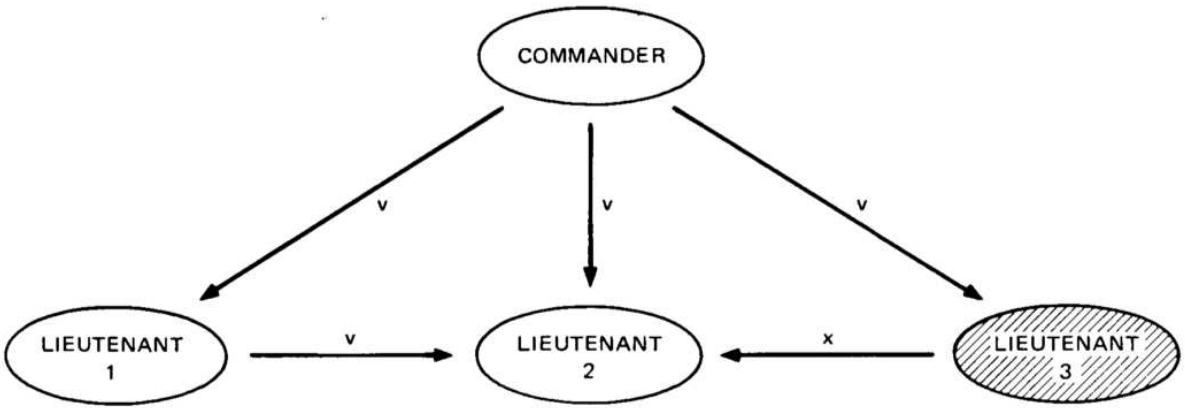


Figura 4 – OM (1): O tenente 3 é um traidor - ponto de vista L2

Passos:

1. Comandante envia v para todos os tenentes
2. L1 envia v para L2 | L3 envia x para L2
3. L2 ← maioria $(v, v, x) == v$ A decisão final é o voto majoritário de L1, L2, L3 e, como resultado, o consenso foi alcançado

O importante é lembrar que o objetivo é que a maioria dos tenentes escolha a ***mesma*** *decisão, e não uma decisão específica.*

Vamos examinar o caso do comandante ser um traidor:

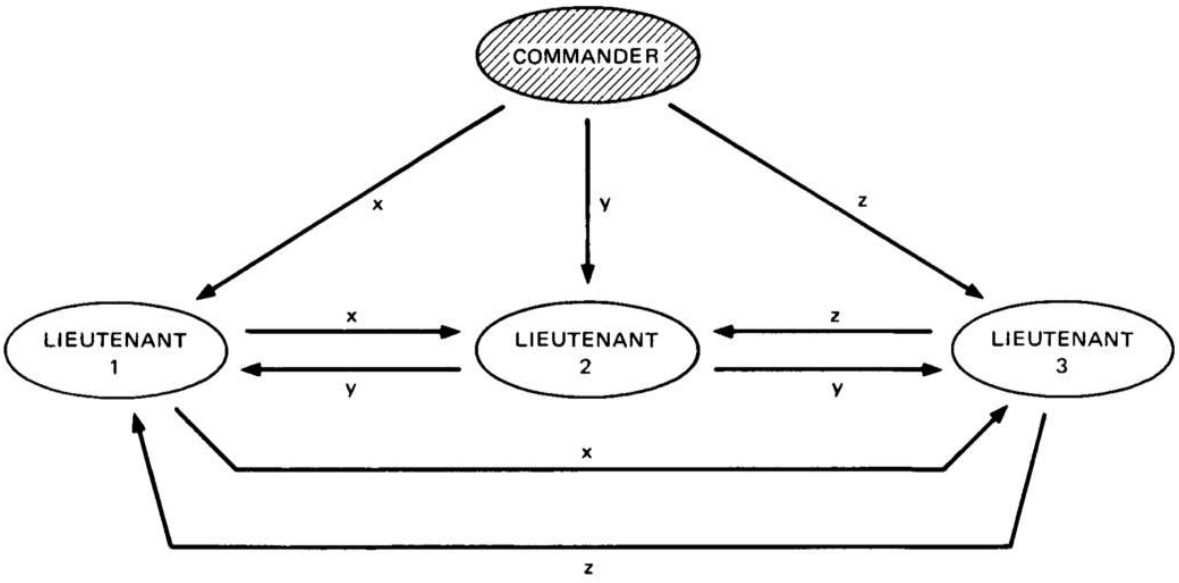


Figura 5 – OM (1): Comandante é um traidor

Passos:

1. Comandante envia x, y, z para L1, L2, L3 respectivamente
2. L1 envia x para L2, L3 | L2 envia y para L1, L3 | L3 envia z para L1, L2
3. L1 ← maioria (x, y, z) | L2 ← maioria (x, y, z) | L3 ← maioria (x, y, z)

Todos eles têm o mesmo valor e, portanto, o consenso é alcançado. Reserve um momento para refletir que, mesmo que x, y, z sejam todos diferentes, o valor da maioria (x, y, z) é o mesmo para todos os 3 tenentes. No caso x, y, z são comandos totalmente diferentes, podemos assumir que eles atuam no retiro de opção padrão. (NELSON, 2007)

4.3 Um pouco das Falhas Bizantinas

A identificação das falhas bizantinas é caracterizada pela satisfação de dois requisitos:

1. Os processos corretos devem possuir uma visão coerente das mensagens enviadas por cada processo
2. Os processos corretos devem poder verificar se as mensagens enviadas pelos demais processos estão consistentes com os requisitos do algoritmo sendo executado.

Isso evidencia que a detecção de falhas bizantinas é definida em função de determinado algoritmo ou protocolo. O primeiro requisito pode ser atendido utilizando duas técnicas distintas:

1. A redundância da informação e o uso de assinaturas digitais não-forjáveis
2. A adição de informação às mensagens, na forma de certificados, que possam ser utilizados para validar o conteúdo sendo transmitido

Existem duas super classes de falhas bizantinas descritas por (KIHLSTROM; MOSER; MELLIAR-SMITH, 2003):

1. Detectáveis, quando comportamento externo do processo faltoso fornece evidências de que o mesmo falhou.
2. Não-detectáveis, caso contrário.

Falhas não detectáveis podem ser subdivididas em não-observáveis, quando os demais processos não podem notar a ocorrência da falha (por exemplo, um processo faltoso informa um parâmetro fornecido pelo usuário incorretamente) e não-diagnosticáveis, quando não é possível identificar o processo que gerou a falha (por exemplo, os processos recebem uma mensagem não assinada). As falhas detectáveis são classificadas em falhas de progresso (ou falhas por omissão) e falhas de segurança (ou falhas por comissão). Falhas de progresso atrapalham a terminação da computação, uma vez que o processo faltoso não envia mensagens requeridas por sua especificação ou as envia a apenas parte dos processos do sistema. Falhas de segurança violam propriedades invariantes às quais os processos devem atender, podendo ser definidas como o não-cumprimento de uma das seguintes restrições:

1. Um processo deve enviar as mesmas mensagens para todos os outros (um processo faltoso poderia, portanto, enviar a mesma mensagem com valores distintos para processos distintos).
2. As mensagens enviadas devem estar de acordo com o algoritmo sendo executado.

4.4 Tolerância de Falta Bizantina

A tolerância a falhas bizantinas é a característica que define um sistema que tolera a classe de falhas que pertencem ao problema dos generais bizantinos. Falha Bizantina é a classe mais difícil dos modos de falha . Isso não implica restrições, e não

faz suposições sobre o tipo de comportamento que um nó pode ter (por exemplo, um nó pode gerar qualquer tipo de dados arbitrários enquanto posa como um ator honesto).

As falhas bizantinas são as mais severas e difíceis de lidar. Tolerância de Falta Bizantina tem sido necessária em sistemas de motor de avião, usinas de energia nuclear e praticamente qualquer sistema cujas ações dependem dos resultados de uma grande quantidade de sensores. Até mesmo a SpaceX estava considerando isso como um requisito potencial para seus sistemas. (EDGE, 2013)

O algoritmo mencionado no item anterior é Tolerante a Falhas Bizantinas, desde que o número de traidores não exceda um terço dos generais. Existem outras variações que facilitam a solução do problema, incluindo o uso de assinaturas digitais ou a imposição de restrições de comunicação entre os pares na rede.

4.5 Relação com o blockchain?

Os blockchains são *ledgers* descentralizados que, por definição, não são controlados por uma autoridade central. Devido ao valor armazenado nesses registros, os agentes mal-intencionados têm enormes incentivos econômicos para tentar causar falhas. Dito isto, a tolerância a faltas bizantinas e, portanto, uma solução para o problema dos generais bizantinos para blockchains é muito necessária.

Contudo, como todo sistema distribuído, sistemas blockchain são desafiadores quando se trata de latência na rede, tramissão de erros, bugs de software, falhas de segurança e ataques hackers. Além do mais, sua natureza descentralizada sugere que nenhum participante do sistema possa ser confiável. Nós maliciosos podem surgir, bem como disparidades de dados devido a conflitos de interesses.

Para prevenir estes erros em potencial, uma blockchain, obrigatoriamente, necessita um mecanismo de consenso eficiente que garanta que todo nó tenha uma cópia válida do registro, ou livro de contas, da rede. Os mecanismos tradicionais de tolerância a falhas não são totalmente capazes de lidar com os problemas que sistemas distribuidos e de blockchain enfrentam. Uma solução universal se faz necessária.

Na ausência de BFT (*Byzantine Fault Tolerance* - Tolerância a Falhas Bizantinas), um par é capaz de transmitir e postar falsas transações efetivamente anulando a confiabilidade do blockchain. Para piorar as coisas, não há autoridade central para assumir e reparar o dano.

O grande avanço quando o Bitcoin foi inventado, foi o uso da Prova de Trabalho como uma solução probabilística para o Problema dos Generais Bizantinos conforme descrito em profundidade por Satoshi Nakamoto. (NAKAMOTO, 2008)

Discutindo o problema dos generais bizantinos, em como alcançar a tolerância a

falhas bizantinas e como isso tudo se relaciona com a blockchain.

O algoritmo tratado anterior é na verdade uma solução que atinge a tolerância a falhas bizantinas. No entanto, essa solução não é eficiente o suficiente, e suas variações têm restrições, ou seja, menos de um terço da rede é desonesta.

m	Messages Sent
0	O(n)
1	O(n^2)
2	O(n^3)
3	O(n^4)

Figura 6 – Tempo de execução da Resolução dos Generais Bizantinos Problema com o algoritmo proposto por Lamport, Shostak e Pease (n = número de atores, m = número de traidores)

Isso nos leva a uma pergunta clássica em Ciência da Computação: *Podemos fazer melhor?*

Trataremos de algoritmos alternativos que atingem a tolerância a falhas bizantinas.

Nota: Por favor, tenha em mente todas as simplificações que eu fizer. Esses algoritmos têm muita pesquisa complexa por trás deles. (MARTIN, 2018)

Os blockchains usam algoritmos de consenso para eleger um líder que decidirá o conteúdo do próximo bloco.

Esse líder também é responsável pela transmissão do bloco para a rede, para que os outros pares possam verificar a validade de seu conteúdo.

Nas exemplificações dos algorítimos para o tratamento dessas falhas bizantinas, utilizaremos as criptomoedas.

4.6 PoW - Prova de Trabalho

Este é o algoritmo mais popular usado por moedas como Bitcoin e Ethereum, cada uma com suas próprias diferenças. O processo envolve tomar a Função Hash Criptografada (no caso do Bitcoin é usado o algoritmo SHA-256) do último bloco do Blockchain, adicionar novas transações e resolver uma nova função criptografada. Resolver a função seria o trabalho, daí o nome PoW, Prova de Trabalho.

Uma função hash é qualquer função que pode ser usada para mapear dados de tamanho arbitrário para dados de tamanho fixo. Se uma função hash é segura, sua saída é indistinguível de aleatória.

Em Prova de Trabalho , para que um ator seja eleito como líder e escolha o próximo bloco a ser adicionado ao blockchain, ele precisa encontrar uma solução para um problema matemático específico.

Deixe esse problema matemático ser:

Dados dados X, encontre um número n tal que o hash de n anexado aos resultados X seja um número menor que Y.

Exemplo - hash é uma função hash hipotética que tem as saídas listadas abaixo

Y = 10, X = 'teste'
hash (X) = hash ('teste') = 0x0f = 15> 10
hash (X + 1) = hash ('test1') = 0xff = 255> 10
hash (X + 2) = hash ('test2') = 0x09 = 9 <10 OK, Resolvido.

Dado que a função hash usada é criptograficamente segura, a única maneira de encontrar uma solução para esse problema é por força bruta (tentando todas as combinações possíveis). Em outras palavras, probabilisticamente falando, o ator que resolverá o problema mencionado primeiro, na maioria das vezes, é aquele que tem acesso ao maior poder de computação. Esses atores também são chamados de **mineiros**.

É fácil verificar se o resultado da função é correto, porém muito difícil, quase impossível de resolver, portanto resta chutar até acertar. Assim, inicialmente eram usados a força computacional do CPU (Central Processing Unit) para as tentativas, e mais tarde foram usadas GPU (Graphic Processing Unit). Hoje em dia se usam equipamentos mais sofisticados chamados ASIC (Application-specific Integrated Circuit) desenvolvidos especificamente para este fim.

Quem resolver a função será o criador do próximo bloco e receberá uma recompensa além das taxas inclusas nas transações processadas no mesmo. Assim que um bloco for resolvido e aceito pela rede descentralizada começa a corrida pelo próximo bloco.

Tem sido amplamente bem sucedido principalmente devido às suas seguintes propriedades:

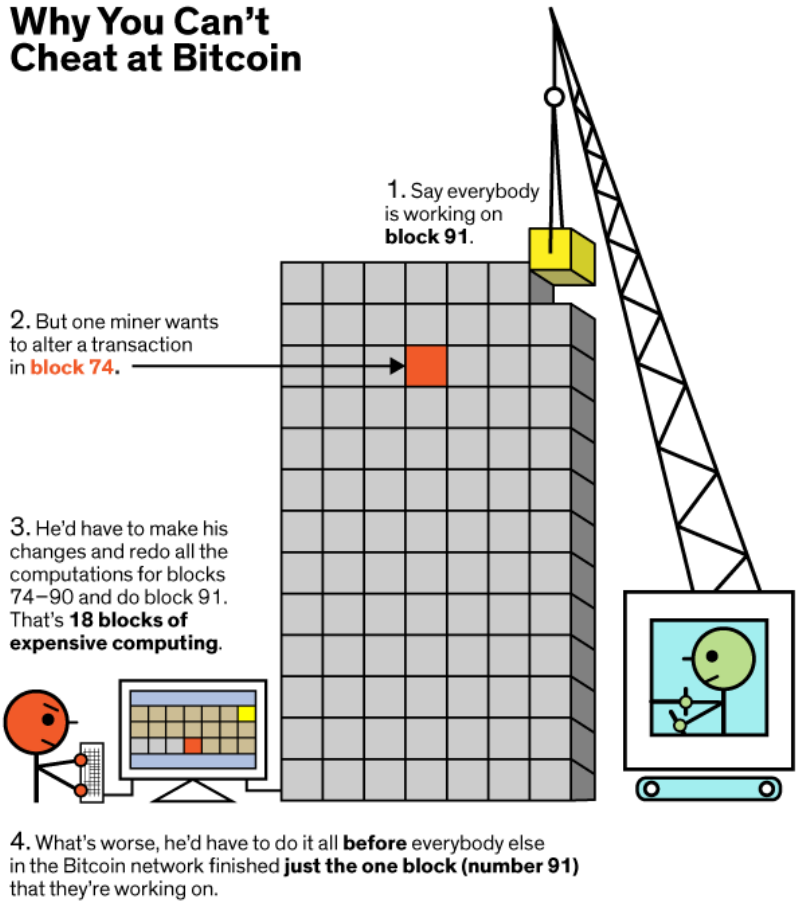
1. É difícil encontrar uma solução para esse problema

2. Quando é dada uma solução para esse problema, é fácil verificar se está correto

Sempre que um novo bloco é extraído, esse minerador é recompensado com alguma moeda (recompensa por bloco, taxas de transação) e, portanto, é incentivado a manter a mineração. Em Prova de Trabalho (PoW), outros nós verificam a validade do bloco verificando se o hash dos dados do bloco é menor que um número predefinido.

Devido à oferta limitada de poder computacional, as mineradoras também são incentivadas a não trapacear. Atacar a rede custaria muito por causa do alto custo de hardware, energia e potenciais lucros de mineração perdidos.

A figura ilustra muito bem como o Bitcoin, e qualquer outra moeda que use Prova de Trabalho, desencoraja comportamentos maliciosos.



Para os leitores que estão interessados em conhecer um pouco mais sobre a divisão de cadeias do blockchain (também conhecidas como garfos ou reorganizações em cadeia) funcionam nos casos de desacordo, sugiro este artigo (PACE, 2017).

Prova de Trabalho fornece a segurança necessária para a rede e tem provado que funciona muito bem até agora. No entanto, é uma alternativa que consome energia demais:

Figura 7 – Quase todos os países africanos (separadamente) consomem menos eletricidade do que a indústria de mineração de Bitcoin

4.7 PoS - Prova de Participação

Antes de continuar, vamos fazer uma analogia da eleição do líder (o ator/agente que selecionará o próximo bloco) como uma loteria:

Em uma loteria, probabilisticamente, se Bob tiver mais ingressos do que Alice, é mais provável que ele ganhe.

De uma maneira muito similar:

Em Prova de Trabalho, se Bob tiver mais poder computacional e energia do que Alice - e, portanto, pode gerar mais trabalho -, é mais provável que ele ganhe (para o próximo bloco).

Da mesma forma, mais uma vez:

Em Prova de Participação, se Bob tiver mais participação que Alice, é mais provável que ele ganhe (para o próximo bloco).

A forma de mineração PoS usa um sorteio aleatório para decidir quem será o criador do próximo bloco. Nesse modelo o potencial criador já deve contar com ativos na moeda específica e quem tiver mais moedas tem mais chances de ser o criador/sorteado. É necessário alocar uma quantidade de moedas para este processo e caso tente comprometer ou alterar o bloco perderá suas moedas. Isto em teoria garante a integridade dos participantes. (RAY, 2018)

No PoS este processo é chamado de bloco forjado e não minado como no caso de PoW. Esse processo elimina o requisito de energia e poder computacional do PoW e o substitui pela participação. A aposta é referida como uma quantia de moeda que um

ator está disposto a bloquear por um determinado período de tempo. Em troca, eles têm uma chance proporcional à sua aposta de ser o próximo líder e selecionar o próximo bloco. Existem várias moedas existentes que usam PoS puro, como Nxt e Blackcoin.

O principal problema com o PoS é o chamado problema de nada em jogo. Essencialmente, no caso de uma bifurcação, os stakers não são desincentivados de apostar em ambas as correntes, e o perigo de problemas com gastos duplicados aumenta.

Para evitar isso, surgiram algoritmos de consenso de híbridos, como a combinação PoW-PoS usada por Decred. Pesquisa ativa em direção a um protocolo seguro e descentralizado de Prova de Participação está sendo feita pela Fundação Ethereum com Casper The Friendly Ghost e Casper The Friendly Finality Gadget. (BUTERIN; GRIFFITH,) - (ZAMFIR, 2015)

A essência é que o PoW oferece a segurança mais comprovada até hoje, mas ao custo de consumir uma enorme quantidade de energia. PoS, a alternativa primária, elimina os requisitos de energia do PoW e substitui os mineiros por “validadores”, que têm a chance de validar (“meu”) o próximo bloco com uma probabilidade proporcional à sua participação. Comparado ao PoW, o PoS é muito mais eficiente em termos de consumo de energia, uma vez que não exige força computacional para a resolução do algoritmo.

Há diferentes moedas que usam este algoritmo de consenso e diversas formas de PoS também. Em algumas o rateio de novas moedas é feito de forma proporcional as moedas existentes, em outras todas as moedas foram pré-criadas assim cada bloco novo não dá recompensa, o criador apenas recebe as taxas das transações processadas naquele bloco.

5 CONCLUSÃO

Os algoritmos de consenso que analisamos são capazes de diferenciar todas as categorias de consenso que exista na blockchain. É a rede que movimenta informação para milhões e milhões de pessoas promovendo muitas facilidades. Então fica a dúvida, será que eles nunca se interferem? Ou existem mutuamente?

A resposta está na arquitetura da rede blockchain, que como já comentamos é uma arquitetura inteligente, projetada com os algoritmos de consenso que é o ponto crucial dessa arquitetura.

O principal problema com os bizantinos, e consequentemente em sistemas distribuídos, é chegar a um acordo. Se um único item falhar, os nós podem não chegar a um acordo.

Por outro lado, os algoritmos de consenso não enfrentarão realmente esse tipo de problema, pois seu principal objetivo é atingir um objetivo específico por qualquer meio. Os modelos de consenso da Blockchain são muito mais confiáveis e tolerantes a falhas do que os Bizantinos.

É por isso que quando pode haver resultados contraditórios em um sistema distribuído, é melhor usar algoritmos de consenso para uma tomada de decisão eficiente. É fato afirmar que não pode haver nenhum sistema descentralizado sem algoritmos comuns de consenso. Não importa se os nós confiam uns nos outros ou não, eles terão que seguir certos princípios para chegar a um acordo coletivo, e para fazer isso, você precisará verificar todos os algoritmos de consenso.

São os algoritmos de consenso que tornam a natureza das redes blockchain tão versáteis. Sim, não há um único algoritmo de consenso do blockchain que possa afirmar ser perfeito, mas essa é a beleza da tecnologia que imaginamos – a constante mudança para podermos aprimora-los.

A análise probabilística formal de blockchains pode se beneficiar dos quase quarenta anos de trabalho em sistemas distribuídos. Embora grande parte da análise de erros bizantinos em sistemas distribuídos seja determinística, grande parte dela pode ser trazida para o mundo probabilístico por meio de uma observação cuidadosa de fenômenos de concentração e de caminhadas aleatórias em gráficos.

Referências

AKKOYUNLU, E. A.; EKANADHAM, K.; HUBER, R. V. Some constraints and tradeoffs in the design of network communications. In: ACM. *ACM SIGOPS Operating Systems Review*. [S.l.], 1975. v. 9, n. 5, p. 67–74. Citado na página 49.

ANTONOPOULOS, A. M. The blockchain. *Mastering Bitcoin.—O'Reilly Media, Inc.*, p. 136, 2014. Citado 2 vezes nas páginas 29 e 30.

ANTONOPOULOS, A. M. *Mastering Bitcoin: Programming the open blockchain*. [S.l.]: O'Reilly Media, Inc., 2017. Citado na página 30.

ARROW, K. J. *Social choice and individual values*. [S.l.]: Yale university press, 2012. v. 12. Citado na página 32.

BÊRNI, D. de A. *Teoria dos jogos: jogos de estratégia, estratégia decisória, teoria da decisão*. [S.l.]: Reichmann & Affonso Editores, 2004. Citado 2 vezes nas páginas 35 e 38.

BRADBURRY, D. *Hyperledger goes to school*. 2017. Citado na página 27.

BUTERIN, V.; GRIFFITH, V. Casper the friendly finality gadget, 2016. *URL: http://arxiv.org/abs/1710.09437. White Paper*. Citado na página 60.

CASTRO, J. D.; RIBEIRO, E. Um teste empírico para a teoria dos jogos: o modelo da racionalidade egoísta. *Monografia de conclusão de graduação em Ciências Econômicas, UFRGS*, 2000. Citado na página 38.

D'AMICO, A. L. A contribuição da teoria dos jogos para a compreensão da teoria de relações públicas: uma análise da cooperação. Pontifícia Universidade Católica do Rio Grande do Sul, 2008. Citado 3 vezes nas páginas 35, 37 e 39.

ECONOMIST, T. The promise of the blockchain: The trust machine. *The Economist*, v. 31, 2015. Citado na página 27.

EDGE, J. Elc: Spacex lessons learned. *lwn. net*, 2013. Citado na página 55.

FERRARI, M. A.; FRANÇA, F.; GRUNIG, J. E. Relações públicas: teoria, contexto e relacionamentos. *São Paulo: Difusão Editora*, 2009. Citado na página 38.

FIANI, R. *Teoria dos jogos*. [S.l.]: Elsevier Brasil, 2006. Citado 2 vezes nas páginas 34 e 36.

FIANI, R. Teoria dos jogos: com aplicações em economia. *Administração e*, 2009. Citado 4 vezes nas páginas 41, 42, 44 e 45.

FIGUEIREDO, R.; SALOMÃO, S. A modelagem do conflito e a teoria dos jogos: fundamentos econômicos e desdobramentos filosóficos. *Rio de Janeiro: IEI/UFRJ*, 1993. Citado na página 32.

FRIEDMAN, J. W. *Oligopoly and the Theory of Games*. [S.l.]: North-Holland, 1977. v. 8. Citado na página 38.

KIHLSTROM, K. P.; MOSER, L. E.; MELLIAR-SMITH, P. M. Byzantine fault detectors for solving consensus. *The Computer Journal*, Oxford University Press, v. 46, n. 1, p. 16–35, 2003. Citado na página 54.

LAMPORT, L.; SHOSTAK, R.; PEASE, M. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, ACM, v. 4, n. 3, p. 382–401, 1982. Citado na página 51.

MARTIN, J. *Everything You Need to Know About Loom Network, All in One Place (Updated Regularly)*. 2018. <https://medium.com/loom-network/everything-you-need-to-know-about-loom-network-all-in-one-place-updated-regularly-64742bd839fe> Citado na página 56.

MOUGAYAR, W. *The business blockchain: promise, practice, and application of the next Internet technology*. [S.l.]: John Wiley & Sons, 2016. Citado 2 vezes nas páginas 27 e 28.

MOUGAYAR, W. *Why the Blockchain Still Lacks Mass Understanding*. [S.l.]: Retrieved September 24th, 2017. Citado na página 29.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. Working Paper, 2008. Citado 2 vezes nas páginas 27 e 55.

NASH, J. Non-cooperative games. *Annals of mathematics*, JSTOR, p. 286–295, 1951. Citado 2 vezes nas páginas 41 e 47.

NELSON, M. *The Byzantine Generals Problem*. 2007. <https://marknelson.us/posts/2007/07/23/byzantine.html>. Citado na página 53.

NEUMANN, J. V.; MORGENSTERN, O. *Theory of games and economic behavior (commemorative edition)*. [S.l.]: Princeton university press, 2007. Citado na página 31.

PACE, A. *Chain Splits and Resolutions*. 2017. <https://medium.com/@alpalpalp/chain-splits-and-resolutions-d3398bddf4ab>. Citado na página 58.

RAIFFA, H.; LUCE, R. D. *Games and décisions: introduction and critical survey*. [S.l.]: John Wiley, New York, 1957. Citado na página 33.

RAY, J. *Proof of Stake FAQs (Updated Regularly)*. 2018. <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs>. Citado na página 59.

SOUZA, Á. A. d. A teoria dos jogos e as ciências sociais. Universidade Estadual Paulista (UNESP), 2003. Citado 3 vezes nas páginas 35, 37 e 38.

STEINER, J. et al. Blockchain: the solution for transparent in product supply chains. *A white paper was written by Project Provenance Ltd*, 2016. Citado na página 28.

SWAN, M. *Blockchain: Blueprint for a new economy*. [S.l.]: O'Reilly Media, Inc., 2015. Citado na página 28.

TAPSCOTT, D.; TAPSCOTT, A. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. [S.l.]: Penguin, 2016. Citado na página 27.

VARIAN, H. R. *Microeconomia-princípios básicos*. [S.l.]: Elsevier Brasil, 2006. Citado na página 40.

ZAMFIR, V. Introducing casper “the friendly ghost”. *Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casper-friendly-ghost*, 2015. Citado na página 60.

ZHENG, Z. et al. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, v. 1, p. 1–25, 2016. Citado na página 28.