Avaliação de mecanismos de consenso para blockchains em busca de nova estratégia mais eficiente e segura

Yoshitomi Eduardo Maehara Aliaga, Victor Cerqueira Leal, Antônio Unias de Lucena, Marco Aurélio Amaral Henriques

[1]Departamento de Engenharia de Computação e Automação Industrial (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (Unicamp)
13083-852 – Campinas, SP, Brasil

{ymaehara,vcleal,alucena,marco}@dca.fee.unicamp.br

Abstract. *In this work, we detail a study of the main consensus mechanisms proposed so far for blockchains and evaluate their strong and weak points. The main objective is to show which requisites should a new consensus mechanism have in order to facilitate the participation of common users in the block construction and blockchain maintenance processes.*

Resumo. *Neste trabalho detalhamos um estudo sobre os principais mecanismos de consenso já propostos para blockchains e avaliamos seus pontos fortes e fracos O principal objetivo é mostrar que requisitos um novo mecanismo deveria possuir a fim de facilitar a participação de usuários comuns nos processos de construção de blocos e manutenção do blockchain.*

1. Introdução

Nos últimos anos o *blockchain* tem atraído muita atenção devido ao sucesso da criptomoeda Bitcoin e da rede Ethereum. Aplicações baseadas em *blockchains* tornam-se cada dia mais populares e surgem propostas interessantes e inovadoras para uso de *blockchains* em cartórios digitais, gestão de identidades, sistemas de reputação, armazenamento confiável de informação, entre outras.

Entre as novidades que o *blockchain* traz, destacam-se os mecanismos de consenso, que permitem que partes desconhecidas entre si e até mesmo concorrentes cheguem a um consenso sobre o estado atual e passado dos dados armazenados no *blockchain*, permitindo criar aplicações distribuídas descentralizadas de forma confiável.

Dentre estes mecanismos o mais conhecido é o *Proof-of-Work* (PoW), que é utilizado na criptomoeda *Bitcoin* [Bashir 2017]. Porém, apesar de dar uma solução ao problema do consenso, ele também tem gerado outros problemas como a necessidade de alto poder computacional e o elevado consumo de energia elétrica [Zheng et al. 2017a].

Por este motivo, foram propostos outros mecanismos tais como *Proof-of-Stake, Proof-of-Activity, Delegated-Proof-of-Stake,* entre outros, como uma forma de contornar as desvantagens presentes no primeiro algoritmo [Zheng et al. 2017a, Bano et al. 2017]. Apesar de contornar essas desvantagens, estes mecanismos ainda continuam apresentando alguns problemas, como será discutido mais adiante.

No presente trabalho é feita uma comparação dos principais mecanismos de consenso em uso ou propostos, com o fim de permitir uma avaliação mais precisa dos pontos fortes e fracos dos mesmos por aqueles que pretendem projetar um novo *blockchain*.

Além disso, este trabalho procura determinar as caraterísticas que seriam desejáveis para um novo mecanismo de consenso com maior equidade de condições na participação de usuários, isto é, que evitasse a concentração da capacidade de criar novos blocos em alguns poucos grupos mais bem equipados material e financeiramente.

Outros trabalhos, como os apresentados em [Greve et al. 2018, Zheng et al. 2017b, Zheng et al. 2017a, Tschorsch and Scheuermann 2016, Bano et al. 2017, Sankar et al. 2017, Lin and Liao 2017, Cachin and Vukolić 2017], também abordaram o tema de consenso em *blockchain*. Entretanto, neste trabalho toda a análise se faz no âmbito de *blockchains* públicos, onde as barreiras à participação ainda persistem e os desafios são maiores.

Este artigo está organizado da seguinte forma: na Seção 2 são apresentados os conceitos fundamentais sobre *blockchain*; a Seção 3 apresenta que são os mecanismos de consenso e quais foram estudados; a Seção 4 detalha as comparações entre estes mecanismos; a Seção 5 apresenta os requisitos desejáveis para um novo mecanismo seguro e com maior equidade de condições na participação de usuários e, finalmente, na Seção 6 são apresentadas as conclusões e os trabalhos futuros.

2. Estrutura do blockchain

O *blockchain* é uma cadeia de blocos interligados através de *hashes*. A utilização de funções de *hash,* criptografia assimétrica na forma de assinaturas digitais e mecanismos de consenso faz com que o *blockchain* seja robusto a fraudes. Os blocos mantêm a informação da lista de transações de forma semelhante a um livro razão em contabilidade [Nakamoto 2009] . Estes blocos estão armazenados em nós que são interligados através de uma rede peer-to-peer (P2P), o que resulta em uma grande redundância de armazenamento das informações pelos nós, dando ao *blockchain* um caráter distribuído. Estes nós criam, conferem, repassam e aceitam um novo bloco de forma descentralizada por meio de um mecanismo de consenso.

A Figura 1 mostra os detalhes do *blockchain* usado pela criptomoeda *Bitcoin* , mostrando as duas partes principais de cada bloco: cabeçalho e corpo. O corpo contém todas as transações financeiras assinadas e verificadas. O cabeçalho contém a raiz da árvore de Merkle montada a partir das transações, bem como o *hash* do cabeçalho do bloco anterior, um carimbo de tempo e outras informações relevantes para o processo de construção do bloco [Nakamoto 2009].

3. Mecanismos de Consenso

Um mecanismo de consenso é um conjunto de passos que são dados por todos ou pela maioria dos nós para chegarem a um acordo sobre um estado ou valor [Bashir 2017]. Um mecanismo de consenso pode ser visto também como uma solução ao clássico Problema dos Generais Bizantinos (PGB) definido por Lamport, Shostak e Pease [Lamport et al. 1982].

A seguir são apresentados os principais mecanismos de consenso usados ou propostos para *blockchains* públicos, isto é, os *blockchains* que não estão sob controle de nenhum

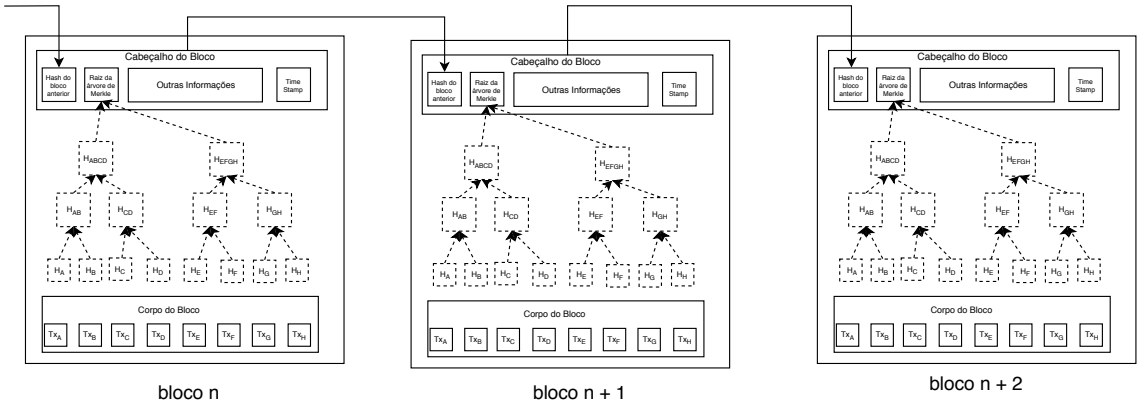

Figura 1. Estrutura da cadeia de blocos - blockchain

grupo de indivíduos ou organizações e que permitem a participação de qualquer novo usuário interessado na construção e validação de blocos.

3.1. Proof-of-Work (PoW)

O *Proof-of-Work* (PoW) é um mecanismo de consenso em que cada nó minerador busca uma solução para um desafio computacional ou matemático a fim de poder criar um novo bloco. Como geralmente a criação de um novo bloco está atrelada à criação de novas criptomoedas, este processo é também conhecido por mineração. Devido ao sucesso da moeda *Bitcoin* e outras similares, este é o mecanismo mais aceito e adotado. No caso específico do *Bitcoin* , a idéia do PoW consiste em encontrar por tentativa e erro (força bruta) um valor para o *hash* do cabeçalho do bloco de tal forma a atender um parâmetro de dificuldade pré-definido [Nakamoto 2009], como é mostrado na Figura 2.

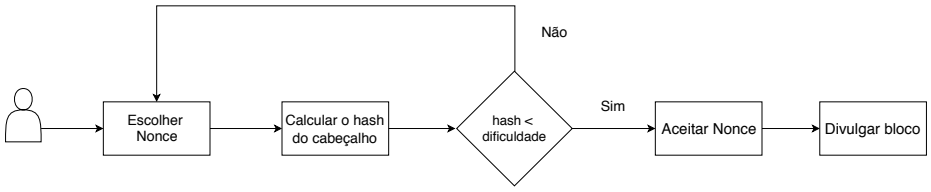

Figura 2. Proof of Work no *blockchain* do Bitcoin

Um dos problemas gerados por este mecanismo de consenso é a necessidade de um grande poder computacional, o que resulta na concentração do poder de mineração entre aqueles que detêm controle de uma grande quantidade de hardware capaz de trabalhar em paralelo. Muitas máquinas em paralelo causam um consumo excessivo de energia elétrica, especialmente considerando que todos os que tentaram simultaneamente resolver o desafio e não conseguiram, desperdiçaram todo o esforço e energia gastos no processo.

Blockchains que utilizam este mecanismo de consenso: *Bitcoin, Bitcoin Cash, Bitcoin Gold, Litecoin, Primecoin* e *Ethereum* [Bano et al. 2017] , entre outros.

3.2. Proof-of-Stake (PoS)

O *Proof-of-Stake* é um mecanismo de consenso em que o sistema faz uma escolha do nó que poderá criar um novo bloco por meio de um sorteio, cuja probabilidade de um nó

ser sorteado é baseada na quantidade de moedas atreladas a ele [King and Nadal 2012], como mostrado na Figura 3. Para a geração de um bloco é necessária uma prova de que o nó possui uma certa quantidade de moedas [Vasin 2013]. Este mecanismo diminuiu o gasto de energia em comparação com PoW já que não depende do poder computacional elevado e nem de cálculos matemáticos de vários mineradores o que faz com que tenha um baixo consumo de recursos de hardware [Tschorsch and Scheuermann 2016].

Entretanto, o PoS tem a desvantagem de poder gerar uma concentração de riquezas, já que quem possui mais moedas acaba tendo mais chances de ser escolhido para criar novos blocos e ganhar as taxas por isso, ficando ainda mais rico. *Blockchains* que utilizam este mecanismo de consenso: *NxT, BlackCoin , PeerCoin , Ethereum* [Bano et al. 2017, Zheng et al. 2017b] (futuramente com os algoritmos *Slasher* & *Casper TFG*) [Zamfir 2017] e Cardano (algoritmo *Ouroboros* [Bano et al. 2017]).

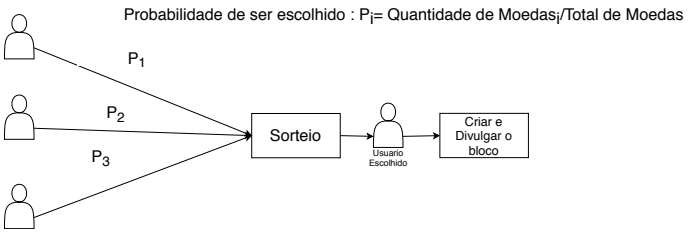

Figura 3. Processo de sorteio na criação de blocos no PoS

3.3. Delegated-Proof-of-Stake (DPoS)

O Delegated-Proof-of-Stake é um mecanismo de consenso derivado do PoS, mas com a diferença de que neste mecanismo um certo número de usuários escolhem seus representantes para gerar e validar os blocos [Zheng et al. 2017a].

Os usuários podem escolher qualquer um dos representantes disponíveis para gerar blocos. Cada nó tem direito a um voto por testemunha e este processo é chamado de *votação de aprovação* [BitshareTeam].

Blockchains que utilizam este mecanismo de consenso: *Bitshare [Zheng et al. 2017b], Steem, ARK, EOS, Lisk* .

3.4. Proof-of-Burn (PoB)

A ideia deste mecanismo consiste em cada nó investir (ou queimar) alguma quantidade de moedas para ter alguma probabilidade de ser o criador do bloco: quem queimar mais moedas tem a maior probabilidade de ganhar [P4Titan 2014]. O papel de queimar moedas é servir de prova no momento da mineração por PoB. Este conceito de queimar consiste em enviar moedas a um endereço especial chamado endereço de queima, já que não há mecanismo que permita utilizar uma moeda enviada a este endereço [Zheng et al. 2017a].

Blockchains que utilizam este mecanismo de consenso: *Slimcoin, Embercoin*.

3.5. Proof-of-Activity (PoA)

É um mecanismo de consenso híbrido que mistura PoW e PoS aproveitando seus benefícios. Determina que o bloco minerado seja assinado por N mineradores para ser

válido. Neste sentido, mesmo algum dos nós possuir mais de 50% de todas as moedas, ele não conseguirá controlar a criação de novos blocos [Zheng et al. 2017a]. O termo *activity* enfatiza o ponto que somente os usuários ativos (os que mantêm um nó online) são recompensados pelos serviços que eles proveem para a rede [Bentov et al. 2014].

Blockchain que utiliza este mecanismo de consenso: *Decred*.

3.6. Algorand

O *Algorand* é um *blockchain* com um consenso rápido baseado em um sorteio para escolha de um comitê que realiza uma votação para determinar o bloco que será inserido na cadeia. O processo é feito em várias rodadas e, em cada uma, é sorteado um usuário para propor um bloco. Este mecanismo é escalável para muitos usuários permitindo atingir o consenso com baixa latência e baixa probabilidade de ramificações [Gilad et al. 2017].

4. Comparação de Mecanismos

Como os diferentes mecanismos de consenso analisados têm várias particularidades, similaridades e diferenças, compilamos uma tabela que destaca as principais características de cada um e permite uma comparação mais direta entre seus pontos fortes e fracos. Da Tabela 1 podemos extrair algumas informações mais relevantes.

O consenso nos mecanismos DPoS, PoA e Algorand é obtido de forma similar: um grupo de usuários (ou nós) é quem decide sobre a criação de um novo bloco. Enquanto o DPoS faz uma votação direta, o PoA e o *Algorand* fazem sorteio baseado na quantidade de moedas possuídas. O *Algorand* tem uma tolerância a 1/3 de nós falhos ou maliciosos, enquanto o restante dos mecanismos têm uma tolerância de 50%.

As características que dificultam fraudes são muito variadas. Entre as mais interessantes está a tragédia dos comuns, um princípio moral que governa o mecanismo PoA, o qual tenta manter o bem comum entre os usuários: se algum usuário age mal, prejudica todos, inclusive a si mesmo.

Outro aspecto interessante é o sorteio criptográfico usado no Algorand como forma de gerar uma imprevisibilidade e sigilo durante o processo de criação de blocos. Junto com a renovação frequente de membros, este conceito torna difícil que um adversário corrompa o comitê.

Vários outros parâmetros podem ser usados na comparação dos mecanismos além dos aqui mostrados como, por exemplo, o número de transações/seg. Entretanto, neste artigo preliminar, nos manteremos só naqueles apresentados por questões de espaço.

5. Características desejáveis em um novo mecanismo de consenso

Comparando os pontos fortes e fracos dos mecanismos de consenso descritos acima, foi possível chegar a uma proposta de um conjunto de caracteristicas desejáveis para um novo mecanismo que resolvesse os principais problemas apontados e reforçasse a participação em igualdade de condições para qualquer usuário que desejasse fazer parte da rede que cria e mantém os blocos em cadeia:

1. baixo consumo energético;
2. boa capacidade de armazenamento de dados;

Tabela 1. Comparação dos mecanismos de consenso

MECANISMOS DE CONSENSO	Proof-of-Work (POW)	Proof-of-Stake (POS)	Algorand	Delegated-Proof-of-Stake (DPOS)	Proof-of-Burn (POB)	Proof-of-Activity (POA)
Tipo de mecanismo	Puro	Puro	Puro	Puro	Puro	Híbrido
Criadores e/ou precursores	1. Cynthia Dwork e Moni Naor 2. Adam Back (*Hashcash*) 3. Satoshi Nakamoto (*Bitcoin*)	1. Nick Szabo (idéia sobre o mecanismo) 2. Quantum Mechanic (primeiro que descreveu o mecanismo) 3. Sunny King e Scott Nadal (primeira moeda)	1. Silvio Micali e Jing Chen (teoria) 2. Yossi Giland, Rottem Hemo, Giorgio Vlachos e Nickolai Zeldovich (implementação)	Daniel Larimer	P4Titan	Iddo Bentov, Charles Lee, Alex Mizrahi e Meni Rosenfeld
Consenso	Verificação se algum minerador chegou a uma solução	Sorteio baseado na quantidade de moedas	• Verificação do usuário que propõe o bloco • Verificação dos membros do comitê em cada rodada • Votação para concordar com o *hash* do bloco proposto	Processo de seleção de testemunhas de criação dos blocos e delegados	Verificação da quantidade de moedas queimadas	• Verificação do cabeçalho do bloco vazio • Verificação dos usuários ganhadores do sorteio • Verificação se é uma extensão legítima do *blockchain*
Tolerância a falhas	$\leq$ 50% do poder de mineração	$\leq$ 50% da posse da quantidade de moedas	$\leq$ 33,33% da quantidade de usuários maliciosos	$\leq$ 50% da quantidade de representantes maliciosos	$\leq$ 50% da quantidade de moedas queimadas	$\leq$ 50% dos usuários maliciosos online
Estável e robusto?	Sim	Sim	Sim	Sim	Sim	Sim
Produz ramificações ?	Sim	Não	Sim	Não	Não	Sim
Recompensa por criação do bloco	Sim	Sim	Não	Não	Sim	Sim
Precisa de moedas para crescer?	Não	Sim	Sim	Sim	Sim	Sim
Poder computacional e consumo energético (relativo)	Alto	Baixo	Baixo	Baixo	Baixo	Médio
Características que dificultam a fraude	Computação Intensiva	Valorização das moedas pela demanda	• Sorteio Criptográfico • Renovação dos membros do comitê • Janela de tempo de consenso (1 min) • Consenso Tentativo	• Embaralhamento das representantes • Vigilância	Investimento Contínuo	Tragédia dos comuns (se você age mal, prejudica todos, inclusive você mesmo)
Quem cria o bloco?	Mineradores	O usuário escolhido no sorteio	O usuário escolhido pelo sorteio que propõe com a maior prioridade	Os representantes escolhidos por votos	O usuário que queima mais moedas	A última testemunha aleatória
Vantagens	• Adoção e aceitação mais difundidas • Segurança pela dificuldade de fraude	• Baixo uso de recursos de software e hardware	• Possui uma boa probabilidade de que todos os usuários concordem nas mesmas transações	• É mais rápido que POW e POS • Tem mais participação dos usuários já que eles decidem sobre os representantes	• É difícil de se fraudar já que tentar obter o controle da rede o tempo todo se torna cada vez mais caro	• Tenta ser o mais justo possível na repartição das taxas e na escolha dos usuários • Apenas participantes onlines
Desvantagens	• Consumo energético ineficiente • Concentração de mineração	• Problema de concentração de riqueza	• Originalmente sem incentivos • Pode gerar blocos vazios	• Muito dependente da participação dos votantes	• Obter um ganho ou recuperar o investimento é um processo muito lento e precisa de constância no investimento (queima)	• Consumo energético ineficiente • Concentração de mineração

3. escolha do grupo criador do bloco por sorteio (o grupo seria sorteado com maior chance para os usuários que estão há mais tempo em atividade na rede);
4. esquema de recompensa para os criadores de blocos;
5. esquema de punição para fraudadores;
6. ranqueamento dos usuários por reputação.

Em outros trabalhos [Sankar et al. 2017, Lin and Liao 2017, Cachin and Vukolić 2017] são descritos mecanismos que atendem algumas destas características. Entretanto, eles consideram *blockchains* privados para a implantação das propostas, nos quais a questão é muito simplificada por haver um controle total dos usuários e sua participação. Destacamos uma vez mais que, neste projeto, buscamos viabilizar as características acima descritas em um *blockchain* público, onde os desafios são maiores devido à inexistência de controles sobre quem entra e quem sai da rede.

6. Conclusão e Trabalhos Futuros

Da comparação entre os principais mecanismos de consenso existentes foi possível avaliar melhor os pontos fortes e fracos de cada um, o que nos trouxe algumas diretrizes sobre como estruturar um novo mecanismo de consenso que permita a criação de um novo modelo de *blockchain* que seja menos exigente em termos de recursos materiais e energéticos, mantendo os mesmos níveis de segurança existentes nos sistemas atuais.

Como resultado final deste esforço, pretendemos chegar a um *blockchain* mais distribuído, isto é, com participação mais ativa e com maior equidade de condições para todos os usuários interessados, o que certamente trará mais segurança (será mais difícil algum grupo ultrapassar os 50% do poder computacional da rede) e mais estabilidade (será preciso remover uma quantidade maior de nós da rede para interrompê-la) para as aplicações baseadas neste tipo de *blockchain*.

Como trabalhos futuros destacamos a proposta de um novo mecanismo de consenso para *blockchain* público que tenha as características desejáveis aqui elencadas, a implementação de uma prova de conceito deste mecanismo para viabilizar uma avaliação mais precisa de seu funcionamento e a execução de testes extensivos para determinar a real capacidade de o novo mecanismo atender os requisitos desejados.

7. Agradecimento

À CAPES pelo financiamento parcial desta pesquisa.

Referências

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., and Danezis, G. (2017). Sok: Consensus in the age of blockchains. *arXiv preprint arXiv:1711.03936*.

Bashir, I. (2017). *Mastering Blockchain*. Packt Publishing Ltd., 1 edition.

Bentov, I., Lee, C., Mizrahi, A., and Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake. *SIGMETRICS Perform. Eval. Rev.*, 42(3):34–37.

BitshareTeam. Delegated proof of stake. `http://docs.bitshares.org/bitshares/dpos.html`. (acessado em 26/03/2018).

Cachin, C. and Vukolić, M. (2017). Blockchain consensus protocols in the wild. *31st International Symposium on Distributed Computing (DISC 2017)*, 91:1–16.

Gilad, Y., Rotem Hemo, S. M., Vlachos, G., and Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. *SOSP '17 Proceedings of the 26th Symposium on Operating Systems Principles*, pages 51–68.

Greve, F., Sampaio, L., Abijaude, J., Coutinho, A., Ítalo Valcy, and Queiroz, S. (2018). Blockchain e a revolução do consenso sob demanda. *XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, Minicurso.

King, S. and Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. [Online]. `https://peercoin.net/assets/paper/peercoin-paper.pdf`. Whitepaper.

Lamport, L., Shostak, R., and Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401.

Lin, I.-C. and Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, vol 19(num 5):pp.653–659.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. [Online]. `https://bitcoin.org/bitcoin.pdf`. Whitepaper.

P4Titan (2014). Slimcoin a peer-to-peer crypto-currency with proof-of-burn "mining without powerful hardware". [Online]. `https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf`. Whitepaper.

Sankar, L. S., Sindhu, M., and Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. *4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 1–5.

Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123.

Vasin, P. (2013). Blackcoin's proof-of-stake protocol v2. [Online]. `https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf`. Whitepaper.

Zamfir, V. (2017). Casper the friendly ghost a "correct-by-construction" blockchain consensus protocol draft v0.1. [Online]. `https://github.com/ethereum/research/blob/master/papers/CasperTFG/CasperTFG.pdf`.

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017a). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2017b). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services (IJWGS)*.