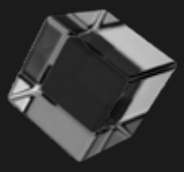


BlockDAG

BlockDAG Network

DAGpaper V2

World’s first DAG Chain, Mixing Security
of Blockchain with Speed of DAG

DAGstract

The evolution of blockchain technology has been swift since the inception of Bitcoin, marked by continual advancements and the emergence of new challenges. Among these challenges lies the blockchain trilemma, encompassing Security, Scalability, and Decentralization. Traditionally, blockchain networks have grappled with balancing these three parameters. BlockDAG represents an innovative approach aimed at addressing this trilemma.
This paper introduces a protocol tha"t diverges from the conventional linear chain of blocks, instead employing a directed acyclic graph (DAG) structure. We delve into the algorithms governing the creation and ordering of the DAG, while also elucidating how the protocol ensures both security and scalability.
Note: This technical document is an ongoing project. We will update this document to reflect the most recent development progress. Our development process is ongoing and iterative, therefore the code and implementation may alter from what is represented in this paper.

Evolution of chain: Reimagining DLT with BlockDAG

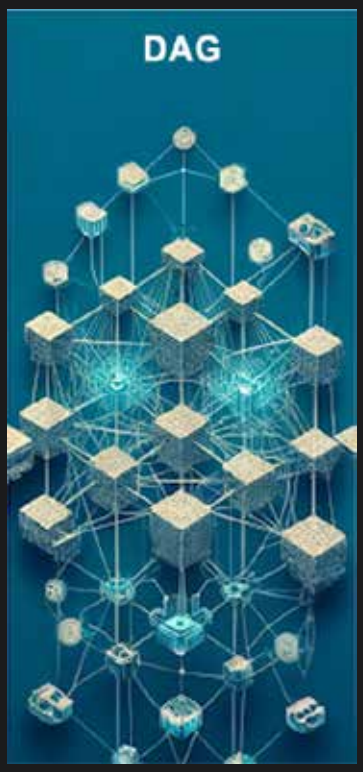
The realm of distributed ledgers has witnessed a remarkable evolution, spearheaded by blockchain technology. Blockchains have revolutionized data security and trust, offering an immutable record of transactions across a decentralized network. However, as blockchain adoption grows, limitations in scalability and transaction speed have emerged. Directed Acyclic Graphs (DAGs) have emerged as a potential solution, offering parallel processing and faster throughput. Yet, DAGs often come with trade-offs in terms of security and decentralization.

Blockchain

Blockchain is a distributed and decentralized technology that underlies cryptocurrencies like Bitcoin and Ethereum. At its core, a blockchain is a chain of blocks, where each block contains a batch of transactions. These transactions are grouped, verified, and added to the chain in chronological order. Blockchain's core strength lies in its decentralized and secure nature. It creates an immutable record maintained by a distributed network of computers. This fosters trust and transparency, eliminating the need for a central authority.
However, as blockchain adoption surges, its limitations in scalability become increasingly evident. Processing large volumes of transactions can be slow and expensive, hindering widespread application.
This paper introduces a protocol that diverges from the conventional linear chain of blocks, instead employing a directed acyclic graph (DAG) structure. We delve into the algorithms governing the creation and ordering of the DAG, while also elucidating how the protocol ensures both security and scalability.
Note: This technical document is an ongoing project. We will update this document to reflect the most recent development progress. Our development process is ongoing and iterative, therefore the code and implementation may alter from what is represented in this paper.

DAG:

Directed Acyclic Graphs (DAGs) offer a potential solution to blockchain's scalability woes. Unlike blockchains, DAGs don't rely on linear blocks. Instead, transactions reference previous validated transactions, enabling parallel processing and potentially faster transaction speeds. This makes DAGs ideal for high-throughput applications. However, achieving security and decentralization on par with blockchains remains a challenge for some DAG implementations.



BlockDAG

BlockDAG is a hybrid concept that combines features of both traditional blockchains and DAGs. It retains the benefits of DAGs, such as high scalability and faster transaction processing, while integrating the security and trust of blockchain consensus mechanisms.

BlockDAG emerges as a groundbreaking solution, meticulously merging the strengths of both blockchain and DAG architectures. It leverages the robust security and decentralization of blockchains while incorporating the efficient, scalable transaction processing of DAGs. This strategic integration allows blockDAG to handle a significantly higher volume of transactions at faster speeds compared to traditional blockchains. By overcoming the inherent limitations of both technologies, blockDAG paves the way for a future where distributed ledgers can seamlessly scale to meet the ever-growing demands of the cryptocurrency and broader digital landscape.

Introduction

Blockchain networks such as Bitcoin and Ethereum (PoW version) operate on the Proof of Work (PoW) model, where miners are responsible for creating blocks. Each block consists of new transactions submitted by users, a proof-of-work puzzle, and a reference to the previous block. These networks follow a linear chain structure, where new blocks are appended to the end of the longest chain while disregarding other blocks.

The security of these chains hinges on the assumption that honest nodes are sufficiently interconnected. When a miner extends the chain with a new block, it must propagate to all honest nodes before the next block is created. Consequently, the protocol regulates the creation of new blocks to ensure that the previous block reaches the maximum number of honest nodes in time. For instance, in Bitcoin, this interval is set to 10 minutes.

BlockDAG network introduces a novel protocol that utilises a Directed Acyclic Graph (DAG) structure to organise blocks, hence termed BlockDAG. Unlike traditional blockchain architectures, where blocks reference a single previous block, the blocks in BlockDAG reference all leaf nodes of the DAG. This approach enables the inclusion of more blocks, thereby accommodating more transactions and achieving higher throughput. However, realising this objective presents several challenges. Firstly, there is a need to mitigate the inclusion of blocks from malicious users. Secondly, a method to linearly order the DAG to determine the sequence of transactions must be established.

Illustrated by an example of a block DAG G, each block references all blocks known to its miner at the time of creation. The terminology associated with the DAG, demonstrated using block H as an example, is elucidated herein.

It is essential to emphasise that employing a Directed Acyclic Graph (DAG) as a ledger represents an approach to on-chain scaling. Furthermore, it should be acknowledged that the scalability of the blockchain can be further enhanced by leveraging existing off-chain scaling solutions.

- Past(H) = {Genesis, C, D, E} – blocks which H references directly or indirectly, and which were provably created before H;
- Future (H) = {J, K, M} – blocks which reference H directly or indirectly, and which were provably created after H;
- Anticone (H) = {B, F, I, L} – the order between these blocks and H is ambiguous. Deciding the order between H and blocks in anticone (H) is the main challenge of a DAG protocol.
- Tips(G) = {J, L, M} – leaf-blocks, namely, blocks with in-degree 0; these will be referenced in the header of the next block

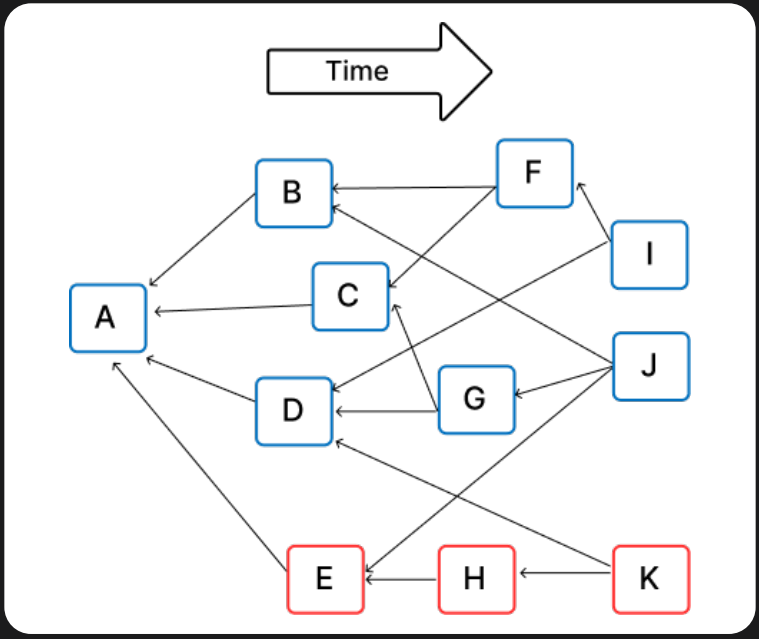
Protocol

Before delving into the protocol's description, it is prudent to establish a few foundational definitions.

Definition Given a DAG G = (C, E), a subset S C is called a k-cluster, if B S : |anticone (B) ∩ S| ≤ k.

Here, C represents blocks and E represents the hash references or edges. We will frequently write B ≣ G instead of B ≣ C. k is a parameter that is pre decided

Maximum k-cluster SubDAG (MCSk)
Input: DAG G = (C, E)
Output: A subset S * ≣ C of maximum size, s.t. |anticone (B) ≣ S * | ≤ k for all B ≣ S ≣



Consider an example of the largest 3-cluster of blocks within a given DAG, denoted as A, B, C, D, F, G, I, J (coloured blue). It can be readily verified that each of these blue blocks has at most 3 blue blocks in its anticone, and it is also evident, albeit less straightforward, that this set is the largest with this property.
By configuring PHANTOM's inter-connectivity parameter with k = 3, it is implied that a maximum of 4 blocks is assumed to be generated within each unit of delay. Consequently, typical anticone sizes are expected not to exceed 3.
Blocks located outside the largest 3-cluster, namely E, H, K (coloured red), are attributed to the attacker (with high probability). For example, block E features 6 blue blocks in its anticone (B, C, D, F, G, I), indicating that these blocks did not reference E, presumably because E was deliberately withheld from their miners. Similarly, block K accommodates 6 blue blocks in its anticone (B, C, G, F, I, J), suggesting that its malicious miner had likely received some blocks from (B, C, D, G) but violated the mining protocol by not referencing them.

Intuition

Distinguishing between honest blocks (blocks mined by cooperating nodes) and dishonest ones is crucial. In the context of the DAG mining protocol, a miner is directed to acknowledge the entire locally observed DAG in its new block by referencing the “tips” of the DAG. Consequently, if block B was mined at time t by an honest miner, any block published before time t - D was received by the miner and is thus included in B’s past set. Similarly, if B’s miner is honest, B is published immediately, and thus any honest block created after time t + D belongs to B’s future set.
This mechanism results in the set of honest blocks in B’s anticone, denoted as anticone(B), typically being small, encompassing only blocks generated within the interval [t - D, t + D]. In essence, the likelihood of an honest block B encountering a large honest anticone is minimal, indicated by Pr (|anticoneh (B)| > k) ≣ O e −C·k, for some constant C > 0 (this follows from a bound). It’s important to note that, unlike anticone(B), an attacker can easily inflate the size of anticone(B) for any block B by creating numerous blocks that do not reference B and are kept secret, preventing B from referencing them on the Poisson distribution’s tail.
Leveraging this property, we configure PHANTOM’s parameter k such that the probability mentioned above is smaller than δ, for some predefined δ > 0.

$$k(D_{max},\delta) := \min\left\{\hat{k}\in\mathbb{N}:\left(1-e^{-2\cdot D_{max}\cdot\lambda}\right)^{-1}\cdot\left(\sum_{j=\hat{k}+1}^{\infty}e^{-2\cdot D_{max}\cdot\lambda}\cdot\frac{(2\cdot D_{max}\cdot\lambda)^{j}}{j!}\right)<\delta\right\}$$

Following this intuition, the set of honest blocks (with perhaps a fraction δ exception) is ensured to constitute a k-cluster.
The parameter k is predetermined and integrated into the protocol. Its definition is as follows:
The rationale behind this parameter is to establish an upper limit on the number of blocks generated concurrently. Since block creation adheres to a Poisson process, for any block B generated at time t, it is guaranteed that at most k(D_max, δ) additional blocks were created within the time interval [t - D_max, t + D_max], with a probability of at least 1 - δ. It’s worth noting that blocks created by honest nodes in the intervals [0, t - D_max) and (t + D_max, ∞) belong to B’s past and future sets, respectively. Consequently, theoretically, |anticone(B)| ≤ k with a probability of at least 1 - δ. However, an attacker can artificially inflate B’s anticone by generating blocks that do not reference it and by withholding their blocks to prevent B from referencing them.
Now, that the discussion of intuition is complete, let us delve into describing the steps involved in the protocol.

Selection of a Well-Connected Cluster

The initial step entails selecting a cluster comprising well-connected blocks from the Directed Acyclic Graph (DAG). This cluster is pivotal as it forms the foundation for subsequent processing steps. The selection criteria prioritise blocks with robust connectivity within the DAG.

Topological Sorting of the DAG

Following the selection of the well-connected cluster, the protocol proceeds to perform a topological sort of the DAG. During this step, emphasis is placed on favouring the blocks within the chosen cluster while penalising those lying outside it. This topological sort ensures that the blocks are arranged in a logical sequence that optimises the processing efficiency of the protocol.

Ordering of Transactions

As a result of the topological sort, an order is established over the blocks within the DAG. This order, in turn, induces a corresponding order over the transactions contained within these blocks. Transactions are executed based on this order, with precedence given to those that are consistent with the established sequence. By adhering to this ordered execution, the protocol ensures the integrity and coherence of transaction processing within the DAG-based ledger system.

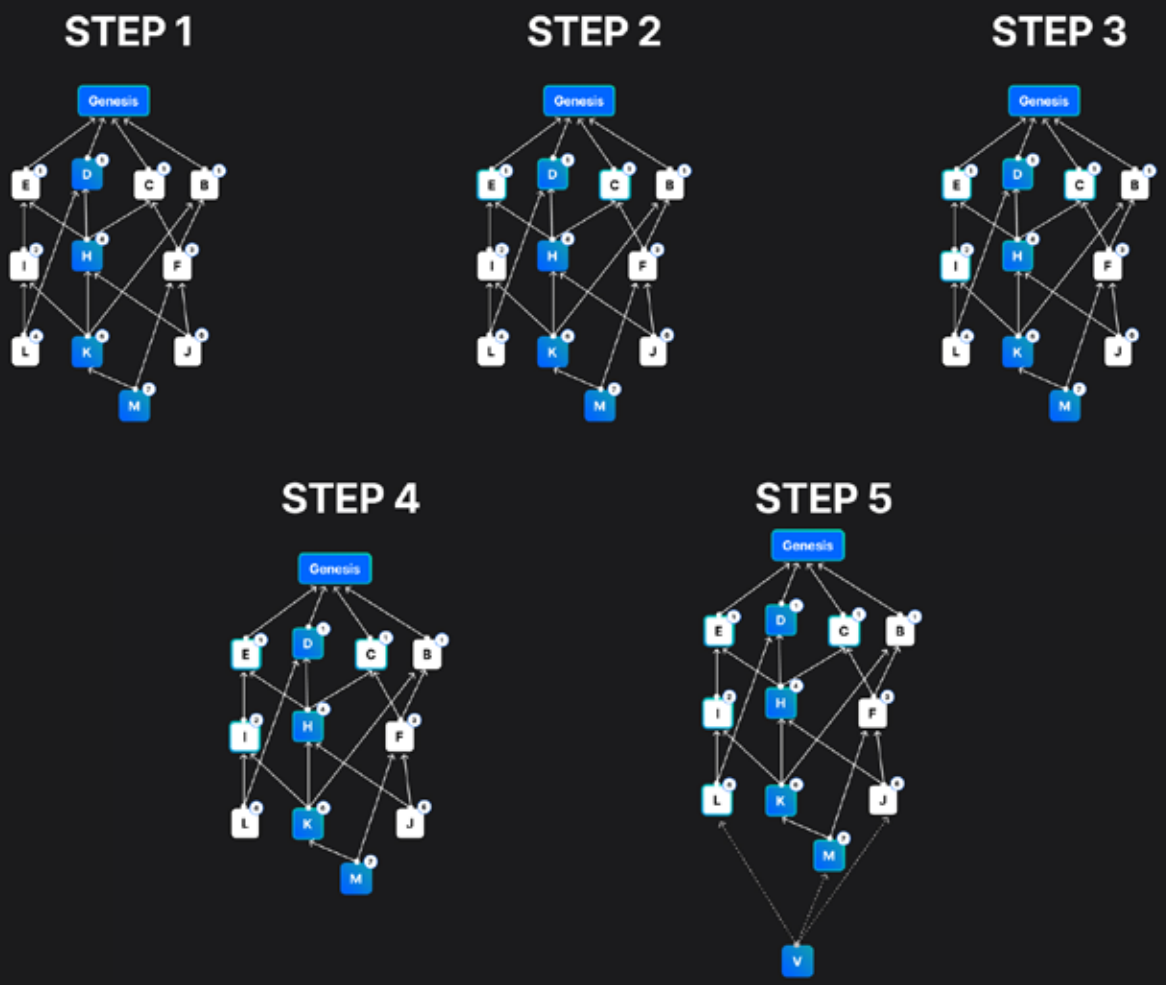
Algorithm 1 Choosing the cluster

Algorithm 1 selects a k-cluster in a greedy manner. We denote the set of blocks it returns as BLUE_k(G). The algorithm functions as follows:

- Given a Directed Acyclic Graph (DAG) G, the algorithm recursively computes the past set of each tip in G, resulting in a k-cluster for each tip.
- It then makes a greedy choice and selects the largest cluster among the output clusters.
- Finally, it attempts to expand this set by adding any block whose anticone is sufficiently small with respect to the set.

Intuitively, the DAG inherits the coloration of its highest scoring tip, denoted as B_max, where a block's score is determined by the number of blue blocks in its past: score(B) := $|BLUE_k(past(B))|$.
Blocks in the anticone of B_max are then coloured to maintain the k-cluster property, essentially creating a chain-selection rule. B_max becomes the chain tip, with the highest scoring tip in its past serving as its predecessor, and so forth, forming the chain Chn(G) = (genesis = Chn0(G), Chn1(G),..., Chn_h(G)).

This approach resembles the reasoning used in Section 1 concerning the Maximum k-cluster SubDAG problem. However, instead of seeking the maximal k-cluster directly, the aim is to maximise it by starting with the tip with the highest cluster and subsequently adding blocks from its anticone. Therefore, informally, the algorithm can be viewed as approximating the optimal solution to the Maximum k-cluster SubDAG problem.
In an example involving a blockDAG G, the greedy algorithm is employed to construct its blue set, denoted as BLUE_k(G), with a parameter k set to 3. The operation commences by selecting the chain in a sequential manner, beginning from



the highest scoring tip M. Subsequently, the algorithm proceeds to select its predecessor K, followed by H, and D (with the tie between C, D, E being arbitrarily resolved), culminating with Genesis. Additionally, to adhere to methodological requirements, a hypothetical “virtual” block V, representing a block whose past encompasses the entire current DAG, is introduced into this chain. Blocks within the chain, namely genesis, D, H, K, M, and V, are shaded with light-blue to denote their inclusion. The set BLUE_k(G) is then recursively constructed, initially empty, by traversing the blocks sequentially. During this process, blocks are added to BLUE_k(G) based on their relevance from either their past or anticone. For instance, during step 1, block D is visited, and genesis is added to the blue set as it is the only block in the past of D. This recursive procedure continues with subsequent steps, each adding blocks to BLUE_k(G) based on their association with the preceding blocks and the defined k-cluster criteria.

Algorithm 1 - Selection of a blue set

Input: G – a block DAG, k – the propagation parameter
Output: BLUEk (G) – the dense-set of G function CALC-BLUE(G, k)
if B == genesis then return {genesis}
for B tips(G) do BLUEk (B)
←CALC-BLUE(past(B), k)
Bmax ← arg max {|BLUEk (B)| : B tips(G)} (and break ties arbitrarily)
BLUEk (G) ← BLUEk (Bmax) ⋃ {Bmax}
for B anticone (Bmax) doin some topological ordering
if |anticone (B) ⋃ BLUEk (G)| ≤ k then
add B to BLUEk (G)
return BLUEk (G)
Algorithm 2 - Ordering The DAG

Algorithm 2 Ordering The DAG

PHANTOM facilitates transaction ordering within its blockDAG structure through an ingenious algorithm known as Greedy Heaviest Observed Sub-DAG (GHOSTDAG). Here's an elucidation of its functioning:

Core Concept:
Unlike traditional blockchains characterised by a single, linear chain, PHANTOM's Directed Acyclic Graph (DAG) architecture permits parallel block creation. Consequently, an algorithm is necessitated to ascertain the ultimate order in which transactions within these blocks are processed and validated. Enter the GHOSTDAG algorithm.

Process

Initialization: The algorithm commences with an empty queue and a list. It proceeds by adding the genesis block (the first block in the DAG) to the queue.

Iterative Processing: During iterative processing, the algorithm sequentially extracts a block (B) from the front of the queue and appends it to the list. Subsequently, it traverses all validated child blocks (C) of block B.

For each child block (C): For each child block (C), the algorithm evaluates all blocks (D) that exist "in the past" of child C, encompassing blocks referenced by C or its ancestors. Additionally, these blocks (D) are not part of the "anticone" of block B, signifying blocks that cannot be reached from B. Essentially, these past blocks (D) hold the potential to influence the ordering of C. Consequently, all these past blocks (D) are included in the queue. Furthermore, the child block (C) itself is subsequently re-added to the queue.

Output: Upon depletion of the queue, the list containing the ordered blocks signifies the conclusive transaction order within the DAG.

Algorithm 2 Ordering of the DAG

Input: G – a block DAG, k – the propagation parameter
Output: ord(G) – an ordered list containing all of G's blocks function ORDER(G, k)
initialise empty queue topo queue
initialise empty ordered list L
BLUEk (G) ←CALC-BLUE(G, k) topo queue.push (genesis)
while topo queue 6= ø do
B ← topo queue.pop()
L.add(B) (B is added to the end of the list)
for all C ▒ childrenB ▒ BLUEk (G) do
for all D ▒ past(C) ▒ anticone (b) \ L do
topo queue.push(D)
topo queue.push(C)
ord(G) ← L
return ord(G

Prioritising "Heaviness":

A fundamental aspect of GHOSTDAG involves the prioritisation of blocks within the queue. Blocks that receive more references from previously validated blocks are deemed "heavier." Consequently, these heavier blocks are prioritised for processing, being removed from the queue first. This incentivizes miners to construct upon the most widely accepted sections of the DAG, progressively establishing a comprehensive order for transactions.

Benefits:

GHOSTDAG provides an efficient mechanism for ordering transactions within the blockDAG structure. By prioritising "heavier" chains, it enhances security by rendering it challenging for malicious actors to disrupt the established order.

Limitations:

While GHOSTDAG offers an efficient means of ordering transactions within PHANTOM's blockDAG, it is a greedy algorithm, prioritising local optimality over identifying the absolute "best" chain in all scenarios. This trade-off between efficiency and optimality can result in limitations. Additionally, the complexity inherent in the blockDAG structure may introduce some overhead compared to simpler linear blockchains when determining the final order of transactions.
In essence, GHOSTDAG provides a robust and efficient solution for transaction ordering within PHANTOM's blockDAG, facilitating enhanced security and scalability.

Security:

The security of the PHANTOM protocol is upheld by several crucial pillars:
Honest Majority Assumption
Similar to many blockchain protocols, PHANTOM relies on the assumption that the majority of miners participating in the network are honest actors. These miners are incentivized to adhere to the protocol's rules and contribute to the network's security. However, if a malicious majority were to gain control, they could potentially disrupt the network's functionality and compromise its security.

GHOSTDAG and Chain Dominance

The GHOST DAG (Greedy Heaviest Observed Sub-DAG) algorithm serves as a cornerstone in securing the PHANTOM network. By prioritising blocks with more references from previously validated blocks, it encourages miners to build upon the most widely accepted portions of the DAG. This fosters a self-reinforcing mechanism where the chain maintained by the honest majority accumulates weight and dominance over time. While malicious actors might attempt to create "orphan branches" or engage in double-spending attacks, their efforts are likely to be futile against the superior computational power of the honest majority. Eventually, the honest chain would overtake any malicious chains due to its cumulative weight of references.

Probabilistic Security

It is essential to recognize that PHANTOM's security guarantees are probabilistic rather than absolute. While the GHOST DAG algorithm and the honest majority assumption significantly enhance security, there remains a finite chance that a well-resourced attacker controlling a substantial portion of the mining power could disrupt the network. This underscores the importance of continually monitoring the network's health and exploring additional security measures to mitigate such risks.

Limitations and Trade-offs

NP-Hardness

The computational complexity associated with identifying the optimal chain within a blockDAG structure poses a significant challenge. This problem is categorised as NP-hard, indicating that finding the guaranteed best solution becomes increasingly challenging as the DAG grows larger. While GHOSTDAG offers an efficient method for prioritising blocks, it does not guarantee the identification of the absolute optimal chain every time.

Attack Vectors

Despite the mitigation of certain security risks by the honest majority assumption, PHANTOM remains susceptible to attacks exploiting vulnerabilities in the network's design. Sybil attacks, where a single malicious actor controls multiple nodes under the guise of independent participants, have the potential to disrupt the voting process and influence block validation. Furthermore, Denial-of-Service (DoS) attacks, aimed at overwhelming the network with a surge of invalid transactions, could impede its transaction processing capabilities.

In conclusion, PHANTOM represents a promising approach to achieving scalability in blockchain technology. However, it's essential to recognize the inherent trade-offs between scalability and absolute security. The probabilistic nature of security in PHANTOM underscores the need for continuous research and development to bolster the protocol's security mechanisms and explore methods to mitigate potential vulnerabilities. By addressing these challenges, PHANTOM can further solidify its position as a viable solution for scalable blockchain networks.

Notable features Of BlockDAG network

Quick and efficient: BlockDAG facilitates rapid transaction processing with its DAG architecture. Transactions are confirmed in near real-time, eliminating the delays associated with traditioqnal block mining. This speed unlocks new use cases, especially in time-sensitive applications, streamlining user experiences.
Low transaction fees: BlockDAG puts an end to exorbitant transaction fees. Its efficient design reduces computational overhead, allowing you to enjoy the full benefits of the network without emptying your wallet. This inclusivity opens up blockchain technology to a wider audience:

- Individuals are empowered to participate with worrying about fees.
- Businesses can leverage blockchain without high fees eating into profit
- BlockDAG offers a high transaction throughput of 10000-15000 TPS.

EVM Compatibility: BlockDAG aligns seamlessly with the Ethereum Virtual Machine (EVM). Developers can effortlessly deploy existing Ethereum-based smart contracts, accelerating project development. This compatibility offers access to a rich toolkit of resources and established communities within the blockchain landscape. Several tools from Ethereum, including some web3 tools and MetaMask, are also directly compatible with the blockDAG network.

- Easily deploy existing Ethereum-based smart contracts, accelerating development
- Tap into a vast ecosystem of tools, resources, and communities
- Leverage the proven technology and security of Ethereum.

Scalability: BlockDAG's architecture promotes intrinsic scalability. Its parallel processing capability allows for greater throughput as the network grows, ensuring the platform adapts to increasing demand. This future-proof design prepares blockDAG for mainstream adoption.

- Resilience against network congestion, even during peak usage
- Long-term sustainability for a thriving blockchain ecosystem

Mircopayments made easy: BlockDAG's combination of speed and minimal fees creates an ideal environment for microtransactions. Users can confidently transact small amounts without disproportionate costs. This opens doors for new business models and facilitates frictionless interactions within decentralized applications.This unlocks new possibilities like:

- In-game economies powered by microtransactions
- Tipping and content monetization models with minimal overheads
- Frictionless machine-to-machine payments

Decentralized Innovation Engine: BlockDAG empowers developers to reimagine the world through decentralized applications. Its smart contract support fuels the creation of self-executing agreements and automated workflows, driving innovation in:

- Decentralized finance (DeFi), with new financial instruments and protocols
- Supply chain management, with enhanced transparency and traceability
- And countless other industries ripe for disruption

BlockDAG Network Ecosystem

Explorer: This platform enables the user to unleash in-depth analysis of the blockDAG network. Acting as a search engine diving into real-time data, trace transactions that provide detailed data from the start to the current state.

Users can access information about:

- Specific Transactions
- Public wallet addresses
- Contrats deployed
- Coins
- Nodes connected to the network

Low code, NO code: Turn your blockchain visions into reality, even without a deep coding background. Our Low-code/No-code platform simplifies the creation of utility tokens, meme tokens, and NFTs. Select from pre-built templates, customize to your needs, and let our intuitive interface streamline deployment.

- Empowers individuals and businesses to innovate on the blockchain
- Accelerates development timelines, reducing time-to-market
- Expands the blockDAG ecosystem with diverse new projects

BlockDAG Payment Card: Experience the future of finance with the BlockDAG Crypto Payment Card. Seamlessly bridge the gap between crypto and everyday spending, backed by rock-solid security for peace of mind. Your digital assets become your gateway to the world. Experience the future of finance where your crypto wallet opens doors worldwide.

Key Benefits:

- Streamlines the use of cryptocurrencies for daily purchases
- Provides a tangible use case for BDAG, expanding its utility
- Drives mainstream adoption by bridging crypto and traditional finance

Proof of engagement mobile application: Mine crypto as you engage with the BlockDAG ecosystem. Our mobile app transforms your smartphone into a mining tool without impacting battery life or data usage. Effortless sign-up, referral rewards, and transparent progress tracking make building your crypto portfolio fun and accessible.

Key Benefits:

- Offers an easy entry point into the world of cryptocurrency
- Encourages active ecosystem participation through rewards
- Grows the blockDAG community with a user-friendly experience

Introducing the BlockDAG Coin (BDAG)

BlockDAG Coin or BDAG serves as the foundational native coin and utility coin within the BlockDAG ecosystem, playing a pivotal role in facilitating various operations and interactions within the network. As the lifeblood of the ecosystem, BDAG empowers users, validators, and decentralized application (dApp) developers alike, fostering a vibrant and sustainable digital economy.

***DISCLAIMER: YOU SPECIFICALLY ACKNOWLEDGE AND AGREE THAT TRADING AND/OR TRANSACTION IN/WITH BDAG TOKENS MAY BE PROHIBITED IN CERTAIN JURISDICTIONS AND NO PERSON IN THE UNITED STATES OF AMERICA AND ITS TERRITORIES, CANADA, DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA), CUBA, SYRIA, IRAN, SUDAN, CRIMEA REGION OF UKRAINE, PEOPLE'S REPUBLIC OF CHINA.**

THE PROSPECTIVE PARTICIPANTS SHOULD NOT CONSTRUE THE CONTENTS OF THIS WHITEPAPER AS INVESTMENT, LEGAL, BUSINESS, ACCOUNTING, TAX, OR OTHER ADVICE. IN DECIDING TO ACQUIRE BDAG TOKENS THE PROSPECTIVE PARTICIPANTS MUST RELY ON THEIR EXAMINATION OF THE ISSUER THEREOF AND THE TERMS OF THE OFFERING, INCLUDING THE MERITS AND RISKS INVOLVED. THE PROSPECTIVE PARTICIPANTS SHOULD CONSULT THEIR ATTORNEYS, BUSINESS ADVISORS, AND/OR TAX ADVISORS AS TO THE LEGAL, BUSINESS, ACCOUNTING, TAX, AND RELATED MATTERS CONCERNING THE ACQUISITION OF BDAG TOKENS.

THIS WHITEPAPER DOES NOT CONSTITUTE A PROSPECTUS AND DOES NOT CONSTITUTE AS AN OFFER OF FINANCIAL INSTRUMENTS AND/OR SECURITIES TO THE PUBLIC OR ANY OFFER IN ANY WAY CONNECTED TO A COLLECTIVE INVESTMENT SCHEME. THE BDAG TOKEN DOES NOT POSSESS ANY OF THE NECESSARY CHARACTERISTICS REQUIRED TO BE CONSIDERED AS ELECTRONIC MONEY, AN ELECTRONIC MONEY TOKEN, AN ASSET-REFERENCED TOKEN, A TRANSFERABLE SECURITY, MONEY MARKET INSTRUMENT, UNIT IN COLLECTIVE INVESTMENT SCHEMES, COMMODITY, SECURITY, OR ANY OTHER FORM OF FINANCIAL INSTRUMENT AS DEFINED IN THE MARKETS IN FINANCIAL INSTRUMENTS DIRECTIVE II.

Transaction Fees
One of the primary functions of BDAG is to serve as the medium for transaction fees within the BlockDAG network. Users engage with the network by utilizing BDAG to cover the costs associated with processing transactions. These fees contribute to the operational expenses of maintaining the network infrastructure and incentivize validators to continue securing the DLT network.

P2P Transaction
BDAG can also be used for peer-to-peer (P2P) transactions, enabling users to transfer funds directly between wallets on the BlockDAG network. P2P transactions provide a decentralized and efficient way for individuals to exchange value without the need for intermediaries. Users can securely send and receive BDAG coins instantly, allowing for seamless transactions across the BlockDAG ecosystem.

Staking Rewards
BDAG also plays a crucial role in the staking mechanism of BlockDAG. Validators who stake their BDAG coins participate in the consensus mechanism and contribute to the security and integrity of the network. In return for their active participation, validators receive staking rewards in the form of additional BDAG coins. This incentivizes validators to uphold the network's consensus rules and maintain the decentralization of BlockDAG.

dApp Access
Furthermore, BDAG coins serve as access keys to certain decentralized applications (dApps) within the BlockDAG ecosystem. Some dApps may require users to hold BDAG coins in their wallets to access specific features or to interact with the functionalities offered by these applications. By incorporating BDAG as a means of access, dApp developers incentivize coin holders to actively engage with their platforms, driving adoption and usage.
Ultimately, BDAG embodies the essence of utility and value within the BlockDAG ecosystem, enabling seamless transactions, incentivizing network participation through staking rewards, and facilitating access to a diverse range of decentralized applications. As the backbone of the ecosystem, BDAG plays a pivotal role in driving innovation, fostering community engagement, and establishing BlockDAG as a leading force in the decentralized digital landscape.maintain the decentralization of BlockDAG.

How to Mine BDAG?

Mining BDAG on the BlockDAG network requires careful setup and configuration. Follow these steps diligently to ensure a smooth mining experience:

Step 1: Hardware Setup

- Begin by setting up your hardware for mining. For optimal performance, we recommend using ASIC miners.
- Ensure a stable power supply for your ASIC miners to prevent interruptions in operations.
- As ASIC miners do not have built-in WiFi capabilities, it is advisable to connect them directly to Ethernet cables. This ensures a stable and fast connection, essential for efficient mining operations.

Step 2: Establish Network Connection

- Once your hardware is set up, establish a robust network connection to maximize performance.
- Verify that each ASIC miner is properly recognized on the local network to enable seamless communication with other miners and the mining pool.

Step 3: Mining Pool Configuration

- Mining pools play a crucial role in distributing rewards among network participants, making it essential to connect your ASIC miners to a mining pool.
- Log in to the control panel of each ASIC miner and input the necessary information to connect to the mining pool. This includes protocols, addresses, usernames, and other relevant details.
- Before commencing mining operations, ensure that the miners' control panels are configured correctly and ready for operation. Verify the connection and configuration settings to avoid any potential issues during mining.

By following these steps meticulously, you can set up your mining hardware and configure it to mine BDAG effectively on the BlockDAG network.

Tokenomics

BlockDAG Coin (BDAG) boasts a total supply of 150 billion coins, demonstrating its rarity and dedication to preserving value. To maintain a controlled environment and prevent excessive inflation, BlockDAG Network implements a halving event every 12 months, similar to Bitcoin.

Max Supply: 150,000,000,000 (150 Billion)

BlockDAG, akin to Bitcoin, adopts a capped total coin supply model, ensuring a stable and predictable ecosystem. This proactive approach mitigates the risks associated with unchecked inflation, fostering confidence in the network's long-term sustainability.

Presale Allocation: 33% = 49,500,000,000

Out of the total supply, 50 billion coins (33%) are earmarked for the presale phase. This allocation aims to incentivize early supporters with special rates, strategically amplifying BlockDAG's visibility and engagement in the cryptocurrency market.

Community Allocation: 66% = 99,000,000,000

- **Miners:80%=79,200,000,000**

The backbone of BlockDAG's security and reliability lies in its miners. With an allocation of 78.8 billion coins, early miners are duly rewarded for their contributions, while also incentivizing future miners to actively participate in network maintenance.

- **Community Building: 15% = 14,850,000,000**

BlockDAG allocates 14.8 billion coins (15% of the community allocation) towards fostering a vibrant community ecosystem. Through educational programs, courses, hackathons, seminars, and conferences, BlockDAG seeks to empower community members and enhance the platform's environment.

- **Liquidity Pool: 5% = 4,950,000,000**

To facilitate seamless trading and minimize price volatility, BlockDAG allocates 4.9 billion coins (5% of the total supply) to its dedicated liquidity pool. This ensures an adequate supply of coins for traders and stakeholders, bolstering the overall health of the ecosystem.

- **Team: 1% = 990,000,000**

A reserve of 990,000,000 coins (1% of the total supply) is set aside for the dedicated BlockDAG team, with these funds locked. This approach underscores the alignment of the team's goals with BlockDAG's long-term success, fostering ongoing contributions and promoting fairness and transparency within the project.

Important Legal Considerations

1. Disclaimers and Limitations of Liability

To the fullest extent permissible by the applicable law, the issuer of the BDAG Token and any of their subsidiaries, affiliates, and licensors, and their respective employees, agents and contractors make no express warranties and hereby disclaim all implied warranties (including, without limitation, regarding any crypto tokens, smart contract, etc.), including the implied warranties of merchantability, fitness for a particular purpose, non-infringement, correctness, accuracy, or reliability. Nor does the issuer of the BDAG Token provide any warranties over any third-party services such as wallets, or marketplaces which you may use to access the BDAG Token.

You accept the inherent security risks of providing information and dealing online over the internet. The issuer of the BDAG Token will not be responsible or liable to You for any losses You incur as the result of your use of any blockchain network or any digital and/or electronic wallet, including but not limited to any losses, damages or claims arising from: user error, such as forgotten passwords or incorrect smart contracts or other transactions; server failure or data loss; corrupted wallet files; or unauthorised access or activities by third parties, including but not limited to the use of viruses, phishing, bruteforcing or other means of attack. Crypto tokens are intangible digital assets that exist only by virtue of the ownership record maintained on the Blockchain. All smart contracts are conducted and occur on the decentralised within the blockchain, which is early stage and/or experimental technology. The issuer of the BDAG Token makes no guarantees or promises with respect to smart contracts. The issuer of the BDAG Token is not responsible for losses due to blockchains or any features of or related to them or any electronic and/or digital wallet.

The issuer of the BDAG Token and their subsidiaries, affiliates, and licensors, and their respective employees, agents and contractors, will not be liable to You or to any third party for any indirect, incidental, special, consequential, or exemplary damages which you may incur, howsoever caused and under any theory of liability, including, without limitation, any loss of profits (whether incurred directly or indirectly), loss of goodwill or business reputation, loss of data, cost of procurement of substitute goods or services, or any other intangible loss, even if they have been advised of the possibility of such damages.

You agree that the issuer of the BDAG Token's total, aggregate liability to you for any and all claims arising out of or relating to the BDAG Token, is limited to the amounts You actually paid the issuer of the BDAG Token in the twelve (12) month period preceding the date the claim arose. The issuer of the BDAG Token sold the purchased BDAG Token in reliance upon the warranty disclaimers and limitations of liability set forth herein, which reflect a reasonable and fair allocation of risk and form an essential basis of the bargain. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, and some jurisdictions also limit disclaimers or limitations of liability for personal injury from consumer products, so the above limitations may not apply to personal injury claims.

2. Governing Law and Jurisdiction

Any action related will be governed and interpreted by the Laws of the Seychelles, and shall, in the case of any legal action, be subject to the exclusive jurisdiction of the Seychelles, and You waive any objection to this jurisdiction and venue.

3. Arbitration

You and the issuer of the BDAG Token agree that any and all disputes arising out of or in connection with the BDAG Token will be resolved exclusively by means of individual arbitration. You and the issuer of the BDAG Token agree that such disputes will be settled in accordance with the Centre for Effective Dispute Resolution ("CEDR") Model Mediation Procedures, and a mediator shall be nominated by the CEDR. You and the issuer of the BDAG Token are waiving your rights to normal recourse to the Courts of Law.

4. No Class Action

You and the issuer of the BDAG Token agree that any claims brought against each other will be brought in their own individual capacity, and not as a member of a class of claimants in any legal action.

Problem Statement

Traditional blockchains tend to suffer from a few inherent limitations that are discussed below.

Scalability Issues

Traditional blockchains, exemplified by Bitcoin and Ethereum, rely on a linear chain of blocks for data storage. So, one of the primary issues with traditional blockchains is scalability. As more transactions are added to the network, the size of the blockchain grows, leading to longer confirmation times and increased resource requirements for participating nodes. This scalability problem can hinder widespread adoption and limit the potential for mainstream applications.

Low Transaction Throughput

Traditional blockchains are able to handle only a limited number of transactions processed per second, thereby leading to network congestion and low transaction throughput.

High Transaction Fees

Traditional blockchains often suffer from high transaction fees during periods of network congestion. As the number of transactions increases, users may need to pay higher fees to prioritize their transactions for inclusion in the next block. High fees can deter users and limit the usability of blockchain applications, particularly for small-value transactions.

Delays in Confirmation Times

Transactions in traditional blockchains require multiple block confirmations for finality. This, in turn, leads to delays in confirmation times resulting in increased time for finalizing a transaction.

Compromised Privacy and Security

While blockchain technology offers transparency and immutability, ensuring privacy and security remains a challenge. Public blockchains store transaction data openly, raising concerns about the confidentiality of sensitive information. Moreover, the pseudonymous nature of blockchain transactions does not guarantee anonymity, as transactions can still be traced through sophisticated analysis techniques. Ensuring robust privacy and security measures without compromising the transparency of the blockchain is a complex issue that requires ongoing research and development efforts.

Increased Energy Consumption

While blockchain technology offers transparency and immutability, ensuring privacy and security remains a challenge. Public blockchains store transaction data openly, raising concerns about the confidentiality of sensitive information. Moreover, the pseudonymous nature of blockchain transactions does not guarantee anonymity, as transactions can still be traced through sophisticated analysis techniques. Ensuring robust privacy and security measures without compromising the transparency of the blockchain is a complex issue that requires ongoing research and development efforts.

Our Solution

BlockDAG addresses these challenges by adopting a novel approach based on DAGs and an efficient Proof of Engagement (PoE) consensus mechanism.

Enhanced Scalability

- BlockDAG breaks free from the constraints of linear blockchains by employing Directed Acyclic Graph (DAG) technology. In a DAG, transactions can be added concurrently rather than sequentially, allowing for parallel processing.
- This design innovation removes the bottleneck of block creation times. Networks built on blockDAG architectures see increased scalability as more users join, as their transactions add to the processing power rather than causing slowdown.
- The combination of Proof of Engagement (PoE) consensus and DAG transaction processing unlocks a future where high-throughput applications can thrive on the blockchain.

Increased Transaction Throughput

- With its optimized Proof-of-Engagement consensus and the scalability of the DAG structure, blockDAG networks achieve significantly higher transaction throughput. This means more transactions can be confirmed per second, streamlining processes and avoiding congestion.
- The increased throughput translates to a better user experience – applications based on blockDAG feel responsive and handle surges in activity without straining.

Almost Instantaneous Transactions Confirmation

- BlockDAG streamlines confirmations thanks to its efficient consensus mechanism. Instead of relying on large mining pools, user participation directly drives transaction validation.
- This design reduces the waiting time for confirmations, sometimes to mere seconds. Near-instant confirmations are essential for time-sensitive applications like point-of-sale payments and fast-paced decentralized exchanges.

Uncompromised Privacy and Security

- BlockDAG addresses privacy concerns through a careful design. Transactions don’t have to be broadcast to the entire network, but can instead travel directly between involved parties. This limits the potential attack surface.
- The blend of Proof-of-Engagement for securing the network’s integrity and the transactional privacy benefits of the DAG maintain transparency without sacrificing user data
- This focus on privacy opens up new use cases where sensitive information needs to be exchanged over the blockchain.
- This eliminates the vast energy expenditure associated with mining, making it an environmentally conscious blockchain solution.
- This efficiency positions blockDAG as a leader in the movement towards sustainable cryptocurrency technologies.

Technical Build Roadmap

Our roadmap delineates a path forward marked by ambition, precision, and unwavering commitment to our community. It serves not only as a plan but also as a promise to drive the future of decentralized finance.

April

- Formulate the development technical whitepaper
- Selection of DAG data structure
  - PHANTOM DAG
  - GHOST DAG
- Implementation of DAG algorithm onchain.
- Testcases of DAG
- Speed test report
- Security and load testing

May

- Deployment of DAG
  - Single cluster
  - Multi cluster
- Gossip protocol integration
- Implementation of P2P network
- Implementation of state management
- Implementation of account management

June

- Consensus protocol implementation for reaching an agreement.
- Implementation of account balances
- Implementation of the transaction manager

August

- Deployment of chain
- Alpha testnet launch
- Explorer development
- Mobile application development
- Testnet launch

BlockDAG Ecosystem: Paving the Way for Future Innovations

dApps Integration

BlockDAG's vibrant ecosystem is tailored to provide a seamless platform for building Decentralized Applications (dApps). Whether users seek to develop logistics solutions, financial dApps, or digital identity platforms, BlockDAG's architecture offers a comprehensive suite of tools and APIs in one unified platform. The interoperability of BDAG enables seamless integration with the decentralized world, empowering users to unlock new possibilities.

Efficient Transactions

BlockDAG's utilization of Directed Acyclic Graph (DAG) technology ensures simultaneous addition of blocks to the chain, eliminating bottlenecks and enhancing scalability for efficient transaction processing. With a remarkable speed of 10000 to 15000 transactions per second, BlockDAG sets the benchmark for industry-leading transaction speeds without compromising on security.

Robust Security for Transactions

BlockDAG endeavors to revolutionize industries by harnessing the power of blockchain technology. As a leading medium of exchange with rapid confirmation times, BlockDAG assumes a pivotal role in facilitating secure financial transactions within a decentralized capital market. From logistics and supply chain management to insurance platforms, digital identity services, and lending and borrowing platforms, BlockDAG aims to encompass a diverse array of solutions under one unified roof, presenting limitless possibilities for secure and efficient financial transactions.

GLOSSARY

Anticone

In a Directed Acyclic Graph (DAG), the set of blocks that are not directly or indirectly referenced by a particular block. These blocks are not part of the chain that leads to the selected block.

Cluster

A group of interconnected blocks within a DAG that are closely related or share common characteristics. Clusters may represent subsets of blocks that have a higher degree of connectivity or influence within the overall structure.

DAG (Directed Acyclic Graph):

A graph structure consisting of nodes connected by directed edges where there are no cycles. In the context of blockchain technology, a DAG is used as an alternative data structure to the traditional linear blockchain, allowing for parallel block creation and increased scalability.

GHOSTDAG (Greedy Heaviest Observed Sub-DAG):

An algorithm used in certain blockchain protocols, including Phantom, to prioritize blocks within a Directed Acyclic Graph based on their weight or influence. GHOSTDAG plays a central role in determining the order of transactions and maintaining the security of the network.

Phantom

A blockchain protocol that utilizes a Directed Acyclic Graph (DAG) structure, along with the GHOSTDAG algorithm, to achieve scalability and security in transaction processing. Phantom aims to address the limitations of traditional blockchain architectures by allowing for parallel block creation and transaction ordering.

REFERENCES

- Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert Van Renesse. Bitcoin-ng: A scalable blockchain ¨ protocol. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), pages 45–59, 2016.
- Michael R Garey and David S Johnson. Computers and intractability, volume 29. wh freeman New York, 2002.
- Aggelos Kiayias and Giorgos Panagiotakos. On trees, chains, and fast transactions in the blockchain. Cryptology ePrint Archive, Report 2016/545, 2016.
- Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing Bitcoin security and performance with strong consistency via collective signing. In 25th USENIX Security Symposium (USENIX Security 16), pages 279–296. USENIX Association, 2016.
- Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. Inclusive blockchain protocols. In International Conference on Financial Cryptography and Data Security, pages 528–547. Springer, 2015.
- Rafael Pass and Elaine Shi. Hybrid consensus: Efficient consensus in the permissionless model, 2016.
- Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. Technical Report (draft), 2015.
- Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. Spectre: A fast and scalable cryptocurrency protocol. IACR Cryptology ePrint Archive, 2016:1159, 2016.
- Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security, pages 507–527. Springer, 2015.
- David Williams. Probability with martingales. Cambridge university press, 1991.
- Yonatan Sompolinsky and Aviv Zohar. Phantom: A Scalable BlockDAG protocol, 2018.
- Yonatan Sompolinsky, Aviv Zohar and Shai Wyborski. Phantom Ghostdag. A Scalable Generalization of Nakamoto Consensus, 2021.