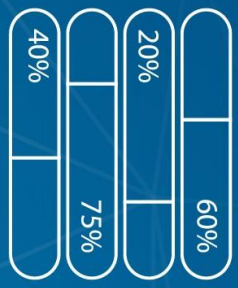
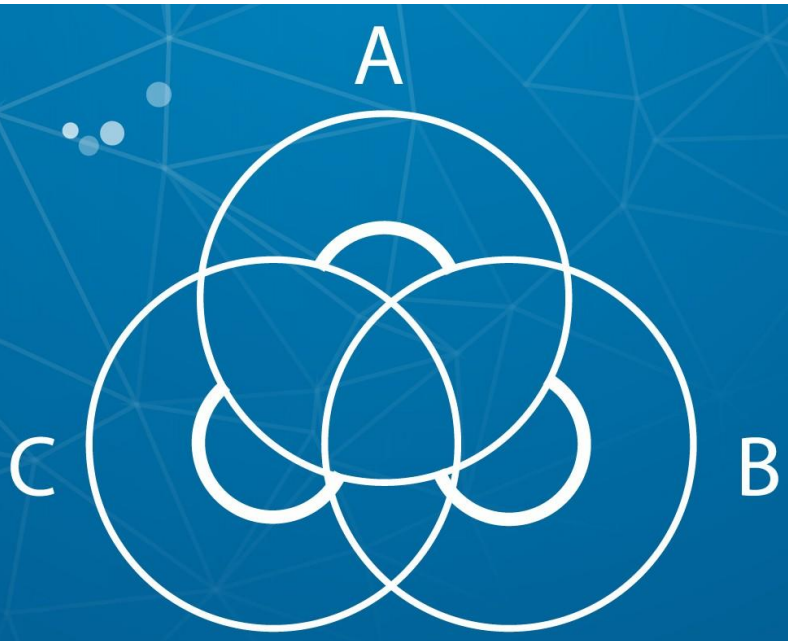


Domino Blockchain

Scalable, secure, and decentralized blockchain for mass adoption



Domino Blockchain Whitepaper

1. Abstract

It is widely recognized blockchain technology faces the trilemma of scalability, security and decentralization. Developers are forced to make trade-offs. Bitcoin network trades scalability for security and decentralization to process about 5 transactions per second (TPS). Ethereum makes a similar trade-off to process about 15 TPS. Several projects can achieve 1000-3000 TPS by reducing the degree of decentralization. In comparison a centralized network such as Visa can process over 25,000 TPS. To gain mass adoption and compete with centralized networks, blockchain needs to scale.

Many projects attempt to achieve the scalability by sharding including Ethereum 2.0. Sharding requires partitioning of network into multiple shards and each shard will achieve consensus on its own. By definition, sharding reduces the number of participating nodes and potentially increases the chances of a 51% attack.

A major reason that blockchain can not scale is transactions are received in different order by different node. It is time consuming for nodes to agree on the order. Bitcoin and Ethereum force mining nodes to use a lot of electricity to find solution to a hard computational puzzle.

Whoever solves the puzzle first gets to decide on the order of the transactions and create the next block in the blockchain.

Domino Blockchain uses the following approaches to solve the seemingly insolvable trilemma and create a blockchain that is scalable, secure, decentralized, and permissionless. Prototype shows that it can sustain 100,000 transactions per second with a block time of 0.2 seconds. The scalability is achieved without relying on any layer 2 solutions or sharding. Domino will use the super fast blockchain to build an ecosystem including a global peer-to-peer payment system, a decentralized exchange, DeFi, games and many other decentralized applications.

1)Domino creates a cryptographic hash order for all received transactions. Transaction ordering is no longer determined by the block producers. Instead it is determined by the cryptographic hash algorithm and persisted to the blockchain. We call this *Proof of Time (PoT)*. This is conceptually similar to Solana's Proof of History (PoH, Reference 1), but with important differences in architecture and implementation.

2)Domino uses a special *Proof of Stake (PoS)* algorithm called *Fast Byzantine Agreement* (FBA, Reference 2) as consensus for block production and validation to achieve transaction finality in 3.5 seconds.

3)Domino introduces a *hybrid validation model* to enhance security while maintaining unlimited participation and decentralization. We introduce a new decentralized firewall, composed of mobile devices and laptops around the world, used to

endorse transactions and surveillance block production and validation. Any device can join the network to perform these functions and get rewarded. Endorsement of transactions is done by sampling random nodes and obtaining sufficient staking. This process can greatly reduce the number of erroneous transactions. An unlimited amount of nodes can be used to perform this function (we call it surveillance nodes or decentralized firewall). Block production and validation is performed by a set of high-bandwidth and high-performance commercial-grade servers (we call them core nodes). The core nodes are distributed all over the world. Surveillance nodes are only involved with surveillance of the blockchain and endorsement of transactions. They do not produce blocks. By separating blockchain surveillance from block production/validation we enable unlimited decentralization, extensive participation, and enhanced security through surveillance. Any mobile device and computer can join the network without permission and hardware restrictions.

4)Introduce a new consensus algorithm (*Domino Consensus*) that can quickly identify fraudulent nodes from a large number of surveillance nodes.

5)Introduce a decentralized storage as part of the blockchain to offload large data or old data. This is particularly useful to store NFT image data with high resolution.

2. Background

Blockchain holds great promise to revolutionize the financial industry and other industries. But mass adoption is hindered by its

inability to scale. Many blockchains have trouble scale to 1000 TPS. Blockchain is based on distributed servers to achieve decentralization, permissionless-ness and censorship resistance. However, among the three pillars of decentralization, scalability, and security, there must be some trade-offs to be made. It is very hard to achieve all three at the same time. Bitcoin and Ethereum trade-off scalability for decentralization and security. Ripple, Stellar Lumens, and EOS trade-off decentralization for scalability and security. In this paper we describe a new blockchain that can achieve all three without trade-offs. It is decentralized such that any device can join the network. Security of the system is maintained through cryptography and decentralization. The details of the system is described in the following sections.

3. Blockchain Architecture

1. Proof of Time and Cryptographic Global Clock

Due to the decentralized nature of blockchain systems, it is very costly to have every node agree on how the transactions are ordered. This is because every node has a slightly different clock and transactions arrives at each node in different order. Not to mention certain node can misbehave and intentionally order the transactions in a way to their financial advantages. To solve this problem, Bitcoin employs a block time of about 10 minutes to impose a delay long enough to have all nodes to agree on the order of transactions. Ethereum managed to cut the block time to 15 seconds. This is probably the lowest anyone can achieve for a Proof of Work (PoW) system. For PoS systems the block time is lower. Tendermint has a timeout window of 3 seconds, Libra around 10, and Aglorand around 5. But this delay is still a significant amount of time for financial systems that handle large amount of transactions. What if we can have a way to order the transactions without relying on a consensus

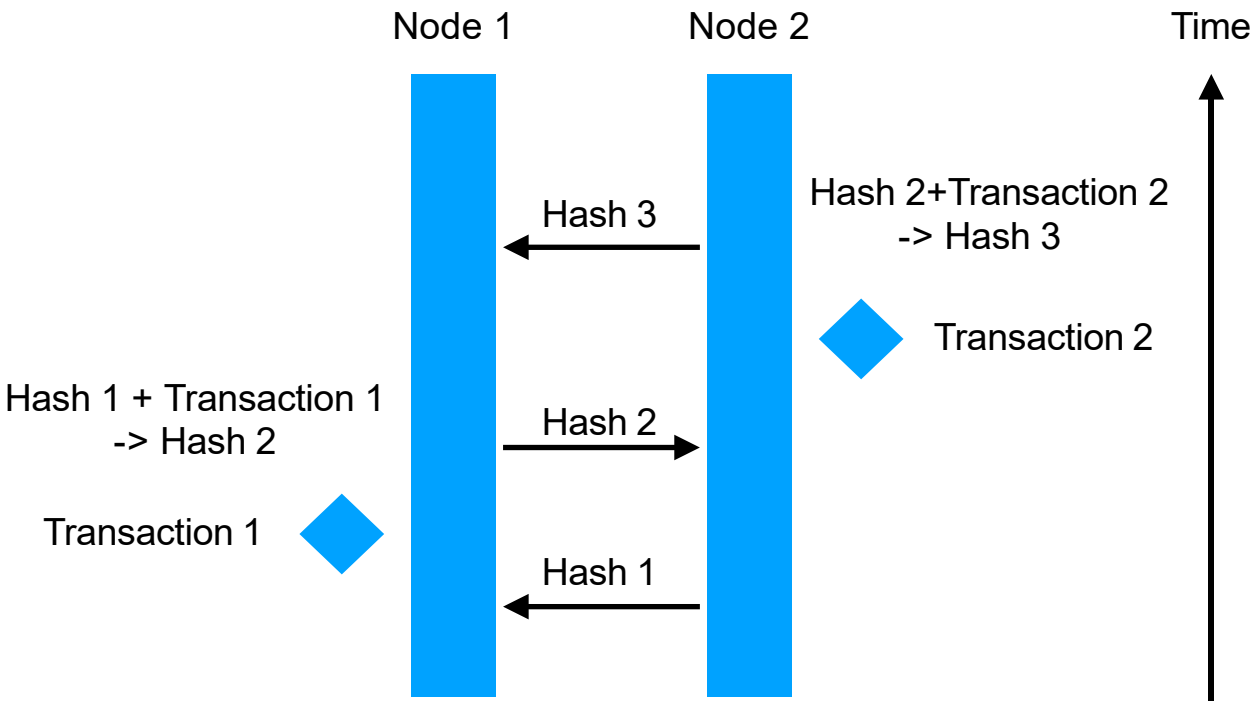
mechanism of either PoW or PoS? This should greatly reduce block time and increase blockchain throughput.

Indeed there is a way to solve this problem through cryptography namely SHA-256 Hashing. SHA-256 is a one-way hashing algorithm that can reduce any amount of data into a constant number of bytes (256 bit hash). It is also deterministic - if you apply the algorithm to the same data again, you will get the same hash value every time. It is also very quick to compute the hash. If you take the same data and change even a single bit, the hash value will be drastically different. There is no way to guess the input data from the resulted hash value. In fact Bitcoin blockchain is created using SHA-256 double hash by linking blocks together in a chain that is sequential in time by this hashing algorithm. Every block contains a hash that is calculated by the hash of the previous block and all transactions in the current block. By including the hash of the previous block, it is guaranteed the previous block is produced before the current block. If anyone tries to change the previous block, the hash of the previous block will no longer be the same. All subsequent blocks will have to be recomputed. The SHA-256 algorithm guarantees that the blocks in the Bitcoin blockchain are produced sequentially in time. No one can dispute this order.

We can use this mechanism to cryptographically order all transactions arriving on the same node. But how do we order transactions created by two nodes? The answer is to use the output hash of the first node as input to create hash output on the second node, and vice versa.

In the following diagram, Node 2 produced “Hash 1” and shared with Node 1. Node 1 takes Hash 1 and Transaction 1 to produce Hash 2. Hash 2 is shared with Node 2. Node 2 takes Hash 2 combined with

Transaction 2 to produce Hash 3. We can effectively use the hash algorithm to synchronize Transaction 1 and Transaction 2. It is indisputable that Transaction 1 happened before Transaction 2.

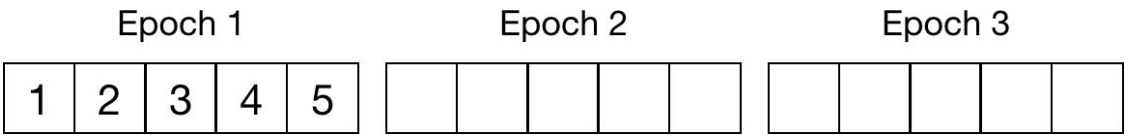


By doing this we effectively synchronized two nodes in time. In fact this process is transitional, we can use this mechanism to synchronize all nodes in the network to create a global decentralized clock (unit of time). Transactions recorded in each node can be hashed and encoded into this global decentralized clock so all nodes can agree on the order of transactions and blocks. This mechanism was first proposed by the Solana project (Reference 1). Solana was able to use this mechanism to create a blockchain network with a block time of 400 ms and sustain 50,000 transactions per second on the testnet with 200 high performance nodes. The reason of such a huge improvement over other blockchain is cryptographically ordering of transactions and reduction in the needs to

reach consensus about transaction ordering. The Solana network limits nodes to high end servers with high bandwidth. It trades some decentralization for improved scalability. Our blockchain leverage the concept of Proof of History mechanism but differs in the architecture and implementation. In addition, Domino Chain introduces some innovative approaches to reach unlimited decentralization and enhanced security without sacrificing scalability. The details of these approaches are described in the following sections.

3.2 Fast Byzantine Agreement and Leader Selection

In Solana's implementation of PoH (Reference 1), there are still a lot of chances that the blockchain will fork into multiple paths due to rotation of leaders. A consensus needs to be reached to determine which fork will be used as the final chain growth direction. We introduce a deterministic algorithm to select next block producer that can be easily verified such that only one path is valid to grow the chain. Network traffic and delay is further reduced. More throughput can be achieved.



We divide time into epochs (each epoch is 1 second). Each epoch is further divided into 5 slots. Each slot is 200 ms. In the first step a block is proposed for each slot. Second step is voting to select who would be the epoch leader with a very short message. Third step is to certify the blocks by verifying there are no double spending, overspending, and blocks are

valid. We conduct all three steps with a Verifiable Random Function (VRF) to ensure randomness and to minimize security risks.

A VRF is consisted of three algorithms Keygen, Evaluate, and Verify.

Keygen(r) $\rightarrow$ (VK, SK). The key generation algorithm randomly produces a verification key (VK) and a secret key (SK) pair.

Evaluate(SK, X) $\rightarrow$ (Y, ρ). The evaluation algorithm takes as input the secret key SK, a random seed X and produces a pseudorandom output string Y and a proof ρ.

Verify(VK, X, Y, ρ) $\rightarrow$ 0/1. The verification algorithm takes as input the verification key (VK), the seed (X), the output (Y) and the proof (ρ). It outputs 1 if and only if it verifies that Y is the output produced by the evaluation algorithm on inputs (SK, X).

The output (Y) is unique for the given input pair (SK, X), meaning it is impossible to find another output (together with a valid proof) for a given key-pair (VK, SK) and seed X.

Each account in the network holds a secret participation key SK, while the verification key VK is publicly known to everyone.

In the block proposal step, accounts are selected to propose new blocks to the network. This phase starts with every node in the network looping through each of the accounts that it manages and, for each account that is online and participating, running VRF to determine if the account is selected to propose the block.

Y / ((2^hashlen)-1) <= P (a publicly known selection probability)

The output Y of VRF is pseudorandom and evenly distributed from 0 to (2^hashlen)-1 (hashlen is the bit-length of the hash). Staked token DOMI is used to calculated a weighted priority such that the probability of selection is proportional to the number of token DOMI to prevent Sybil attacks (Reference 2).

Once an account is selected, each node propagates its proposed block along with the VRF output, which proves that the account is a valid proposer. Each node in the network will get block proposals from other nodes. Next, each node will run the VRF for every participating account it manages to see if they have been chosen to participate in the selection committee. If an account is chosen, it will have a weighted vote based on the number of DOMI it has. Each account chosen will filter the proposals down to one by voting to confirm the block. These votes will be for the lowest VRF block proposal calculated at the timeout and will be sent out to the other nodes along with the VRF proof. Each node will validate the committee membership VRF proof before adding to the vote tally. Once 2/3 of majority is reached for the leader selection, the process moves to the certification step.

A new committee is then selected to check the block proposal that was selected in the selection phase for overspending, double-spending, or any other problems. If valid, the committee votes again to certify the block. This is done in a similar manner to the selection vote where each node iterates through its managed accounts to select a committee and to send votes. These votes are collected and validated by each node until 2/3 of majority is reached, triggering an end to the round and prompting the node to create a certificate for the block and write it to the ledger. At that point, a new round is initiated and the process starts over.

What we are implementing is Fast Byzantine Agreement (FBA) protocol (Reference 2). The protocol is not performed among all user in the network. Instead, it is confined to a small randomly chosen committee of users for each round. FBA can scale to millions of core nodes because the protocol is executed to a small committee. Increasing of user base does not slow down the protocol instead it increases the robustness and security of the protocol. A large user base can also help to increase throughput as different committee would be working on certifying different blocks due to our unique implementation of the protocol. We will explain that further in the next sections. A epoch leader will produce 5 blocks sequentially, but each block will be certified by separately selected random committees to ensure security. Even if an adversary is selected as the leader of an epoch, but the proposed blocks would not pass certification by randomly selected committees if they are invalid.

The uniqueness and pseudo-randomness properties of the VRF are crucial in ensuring that no user can brute-force through multiple outputs Y until he/she finds one that falls within the desired range. Such attack is mitigated by the uniqueness property of the VRF because once the seed X is fixed, the VRF can only be used to produce a single output. Moreover, the verification key VK must have been entered into the system before the current epoch, at the time when the seed X was essentially unpredictable.

The above computation is extremely cheap. Each user only needs to perform a single Evaluate function computation to decide if they are selected to serve on the committee.

A new and independent committee is chosen for each round of the FBA. This is possible due to the unique property called player

replaceability. Briefly, different users are able to participate in different rounds of the FBA without having to pass any state to each other. This allows us to satisfy a high level of security, where a user is allowed to be dynamically corrupted after any message they send as part of the protocol.

During leader selection phase, the proposed values are hashes of blocks and are propagated in parallel with the actual blocks. The protocol allows the users to select epoch leader from the block hashes in Step 2 without seeing the full blocks. As hashes and selection-votes are short messages and propagate much faster than full blocks, by the time most honest nodes receive the actual block, they should have already received 2/3 selection-votes for the block when the leader is honest. Thus most honest nodes can certify the block the moment they receive it, and a certificate is produced in only one voting step after the block is propagated. Since each leader will produce 5 blocks in a row we only need to select a new leader every 5 blocks. But each block will be certified by a separately selected random committee to ensure security.

3.3 Separating Block Production from Block Validation

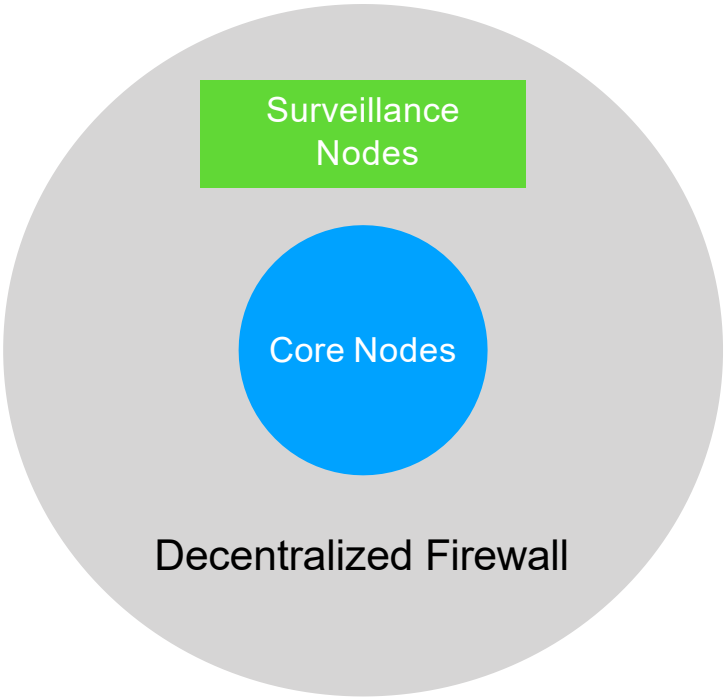
In a typical PoS network, block producer is selected and it will validate transactions and select transactions to put into a new block such that block production and validation is performed by a single node. While this is easier to implement and reduce network traffic but it opens door to adversaries to manipulate the block with invalid transactions.

In our implementation of FBA, the protocol is separated into three steps: block proposal, leader selection, and block certification. Each step is performed by independently selected random nodes as committees. This reduces the chance of block manipulation to a very small and

negligible probability when Byzantine nodes are less than 1/3 of the total stakes (Reference 2).

3.4 Surveillance Nodes and Decentralized Firewall

In the Domino network, there are two types of nodes: core nodes and surveillance nodes. Core nodes are responsible for proposing blocks, selecting block leaders, certifying blocks and replicating certified blocks to all nodes. Surveillance nodes are responsible for surveillance of the network and endorsement of transactions. In a sense, surveillance nodes act as a firewall that are decentralized and can ensure the healthiness of the network and all nodes behave honestly. If there are adversary nodes, they are discovered, exposed and eliminated quickly to limit damages to the network.



In previous sections, we described proposing blocks, selecting leaders, and certifying blocks. In this section we describe transaction endorsement and surveillance of the network.

When a transaction is submitted, it is immediately forwarded to a few surveillance nodes for endorsement before it is published to the network. These nodes are selected based on the network topology for efficiency and incentivizing social engagement. This process is very fast (less than 3 seconds) and the user should not notice any significant delay. When surveillance nodes join the network, the social relationship is recorded. The endorsing surveillance nodes are chosen according social relationship. Nodes with higher stakes are also chosen with a higher probability. The selected surveillance nodes verify the transaction by checking signature validity, account balance, and pending transactions to ensure the transaction is valid, no double spending or overspending. If everything is checked out ok each surveillance node endorse the transaction by digital signing and return to the submitter node. The submitter node collects all signed endorsements and package everything into one transaction and submit to the network via a core node that is close to the submitter. In case the submitter node does not have any socially connected surveillance nodes, the system will randomly select a few surveillance nodes to endorse the transaction. The endorsement nodes are compensated for each endorsement via a portion of the transaction fee. Usually each user (surveillance node) is located in a social tree structure. The selection process goes from the leave to the root direction. We encourage users to stake a good amount of DOMI especially when they have a large network in their social tree.

The endorser selection algorithm can be changed by a majority of 2/3 core nodes and surveillance nodes to approve.

In reality, producer/validator nodes and surveillance nodes perform different type of work and have different type of hardware requirements. Typically producers need to have high bandwidth and multi-core CPU or GPU. Depending on the type of validation that needs to be performed, some validations can be performed by lower spec computers or even mobile devices. We use SHA256 hashing algorithms in our design. Computing SHA256 hash with giving input data is super fast and can be achieved by a single core CPU or GPU. Once hash is calculated, it is compared with the previous calculated hash by block producers attached to the block header. Block producers/validators require high-performance and high-bandwidth servers while surveillance nodes can be any type of computers, laptops, or even mobile devices. This hybrid validation model greatly expands the degree of participation and decentralization to reach most people worldwide while maintaining high scalability and high throughput in the blockchain.

5. Domino Consensus Algorithm

Besides endorsement, surveillance nodes continuously monitor and surveillance the network by ensuring:

- Transactions are properly signed
- No double spending or overspending
- Blocks are structured properly with header and payload
- Next block producers are chosen according to the correct algorithm (the algorithm is deterministic).
- No misbehaving producers or validators

- No parallel chain

Whenever there is an error or adversary detected, it is broadcasted to 10 randomly selected surveillance nodes in the network to alert all nodes about the error. Each surveillance node will verify the error or violation. If it is confirmed, the surveillance node will choose 10 randomly selected nodes and alert them about the error. This process confirms the error. Once error is confirmed, the erroneous nodes will be removed from the network for a configurable period of time and stake will be slashed. We call this "*Domino Consensus*" as it is similar to Domino's Effect during the error detection process.

The design of Domino Consensus was inspired by Avalanche Consensus (Reference 3). In Avalanche Consensus, each node samples a set of randomly selected nodes. If the majority choose one color, this node will choose that color. This process is repeated a few times and the network will reach a metastable state and therefore achieve consensus. Avalanche consensus is a new class of consensus algorithm that differs from Classical consensus and Nakamoto Consensus in that it can reach consensus much faster among a large number of distributed nodes. Domino consensus is a variation from Avalanche consensus. The difference is when nodes sample randomly, it does not need to choose one color versus another. Instead it will collect all potential errors from the selected nodes. The node does not blindly tell other nodes about the errors. Instead it will verify each error and only alert another 10 random validators about the confirmed errors. This removes the potential threat of some bad node intentionally spreading false error signals to corrupt the network. This consensus mechanism allows the surveillance nodes to quickly discover and confirm errors in the network such that actions can be taken immediately to address the errors and secure the network.

In most cases, error might be detected even before it is committed to the blockchain as there are many nodes actively surveillance the network constantly. When block validators validate a block, they will check the errors and ensure none of the errors are included in the block.

Surveillance nodes will continue to monitor the producers/ validators to ensure blocks are generated properly and the right leader is producing the blocks. Any misbehavior will be marked and propagated to the whole network. Any producers identified as misbehavior node will be removed from the producer list and staked token will be slashed.

The following errors will be checked constantly by the surveillance nodes:

- double spending
- Over spending
- Dust attack
- Long range attack
- Forged signature
- Misbehaving producers and validators
- Parallel chains

Surveillance rewards are calculated based on the errors found by the surveillance nodes. First one finding an error and subsequently verified will be rewarded highest. Second node verified the error will be rewarded in half. Third node verified the error will have half of the second

reward. So on and so forth. Reward amount for each error is fixed. This incentivizes surveillance nodes to find new errors in the network and verify them as early as possible. This process exposes errors in the network as early as possible.

3.6 Domino Virtual Machine and Smart Contract

Ethereum Virtual Machine (EVM) is the first generation decentralized application platforms and runtime environment for smart contracts. However, issues with the performance and efficiency have been identified. There are also few people capable and available to expand on EVM and provide tools for it.

WebAssembly (WASM) is a standard for web browsers developed by W3C workgroup that includes Google, Mozilla, and others. It supports multitude of languages that compile to WASM. WASM is high performance as it is build to be as close to native machine code as possible while being platform independent. Small binary code can be shipped over the internet to devices with low bandwidth. WASM expands supported languages to include Rust, C/C++, C#, Typescript, Haxe, and Kotlin. WASM has been continuously developed by standards committees and major companies such Google, Apple, Microsoft, Mozilla, and Facebook.

Domino Virtual Machine (DVM) is being built to be WASM-compliant with floating point operations removed for consensus algorithms. In addition, DVM will support Solidity such that any existing Ethereum smart contract code can be migrated to Domino easily. Similarly, Polkadot, a next-generation blockchain interoperability protocol, is being built with WASM support from the ground up. The

Ethereum Foundation is also working on implementing WASM support into geth and researching the use of WASM in sharding.

In the future, we will be designing a visual programming tool that can create smart contract with drag and drop UI support that does not require programming skills. This will greatly increase adoption rate as most people do not have programming experience.

3.7 Domino Decentralized Storage

As the size of the blockchain grows, it is necessary to have a storage solution to offload blockchain data. Domino chain plans to build an integrated storage mechanism that is decentralized and censorship-resistant on the Surveillance Nodes and follows the Swarm protocol. One of the main reason to select Swarm rather than IPFS is Swarm's core storage component as an immutable content addressed chunkstore rather than a generic distributed hash table. This makes it easier to offload blockchain data to Swarm.

4. Domino Ecosystem

1. Global Peer-to-Peer Payment Network

Cross border payments and remittance with a market size of over $680 billion have always been a problem as it is slow and expensive using traditional banking system. When Bitcoin was first created it was intended to address this very issue. However due to the high mining fee and slow finality it is hard to use Bitcoin for daily payments especially when the amount is small. Domino network will have the advantage of low transaction fee and fast settlement compared with other blockchains and cryptocurrencies. Domino will support immediate settlements of cryptocurrencies including stable coins like USDT and USDC.

Domino has partnership agreement with Unbanked (unbanked.com) to offer fiat on ramp to convert fiat currency to stable coins. Stable coins can be transferred instantly for payments.

Domino will offer a non-custodial crypto wallet that holds DOMI, BTC, ETH, USDT, USDC and other cryptocurrencies. The wallet is also a validator node that can participate in securing the network while earning rewards on DOMI.

2. Crypto Debit Card

Domino's partnership with Unbanked (https://unbanked.com) offer crypto debit card to enable users to spend their crypto with a traditional debit card like Visa or MasterCard. Users only need to deposit crypto into their wallet. The linked debit card to the wallet can allow users to spend their crypto at over 50 million merchants in the Visa network or MasterCard network. Domino would be using Unbanked's settlement layer to convert crypto into fiat after user swipes their card at the merchants. All US residents are eligible to apply for a crypto debit card already. Unbanked is working on bringing the service to over 153 countries worldwide. Once this service is available to Unbanked customers, the same type of services can be made available to Domino blockchain users.

3. Decentralized Exchange

With the super fast transaction speed, a decentralized exchange would be built on top of Domino blockchain by our partners. Users of the exchange would experience similar performance like a centralized exchange. Many users realize the biggest risk of centralized exchanges is the loss of their crypto assets especially on hot wallet managed by the exchanges. The reason why many users are not using decentralized

exchange is scalability issues and usability issues. Domino would address both of these issues with the massively scalable blockchain infrastructure. Domino has a partnership agreement with BCone crypto exchange (www.bcone.vip) to build a next-generation decentralized exchange on top of the Domino blockchain.

4.4 NFT Support

A Non-Fungible Token (NFT) is a unit of data stored on a decentralized ledger, or a blockchain, that certifies a digital asset to be unique and therefore not interchangeable. NFTs can be used to represent items such as photos, videos, audio, and other types of digital files. NFTs are tracked on blockchains to provide the owner with a proof of ownership that is separate from copyright. The NFT market value tripled in 2020, reaching more than $250 million. During the first quarter of 2021, NFT sales exceeded $2 billion.

In the second phase of the implementation, Domino blockchain will add an integrated decentralized storage that can handle large amount of data stored on the blockchain seemlessly. This will facilitate NFTs with high resolution images or other types of data. Most blockchains today do not provide such capability to transact NFTs with large data sets. Domino blockchain will serve this growing market with unlimited decentralized storage, low transaction fees and instant settlements.

5. Milestones

December, 2021	Domino Testnet launch
March, 2022	Domino wallet app release on mobile devices and personal computers
June, 2022	Domino Mainnet Launch
July, 2022	Crypto debit card available on mobile app (through integration with Unbanked API)
August, 2022	Fiat on ramp in the US and other countries integrated into Domino (through integration with Unbanked API)
March, 2023	Launch decentralized storage for NFT and historic data

6. Team Members

Please visit our website at https://dominochain.com to see updated list of team members.

7. References

1. Anatoly Yakovenko, Solana whitepaper, https://solana.com/solana-whitepaper.pdf

2. Jing Chen, Sergey Gorbunov, Silvio Micali, Georgios Vlachos, Algorand Agreement, Super Fast and Partition Resilient Byzantine Agreement, https://eprint.iacr.org/2018/377.pdf

3. Team Rocket, Maofan Yin, Kevin Sekniqi, Robbert van Renesse, Emin Gün Sirer Cornell University, Scalable and Probabilistic Leaderless BFT Consensus through Metastability, https://assets.website-files.com/5d80307810123f5ffbb34d6e/6009805681b416f34dcae012_Avalanche%20Consensus%20Whitepaper.pdf