WHITEPAPER

ABSTRACT

With the advent of blockchain technology in the early 2000's the world has been watching, excited to see what becomes of it. Most notably Bitcoin has captured everyone's attention as being a currency that operates on the blockchain but other communities have sprung up in its wake. While Bitcoin serves its own purpose, the core technology of the blockchain can be extended to be more secure and advanced. That's where DigitalNote comes in.

DigitalNote is a robust **Proof-of-Work/Proof-of-Stake hybrid blockchain** with instant untraceable transactions and highly secure encrypted messaging features at its core. Innovative and forward-thinking, the network is resistant to the 51% attacks that plague other cryptocurrencies (via its VRX v3.0 technology) and it is mobile-ready with lightweight wallet functionality. DigitalNote is decentralized and competitive with a Masternode network that enhances untraceability and provides incentive for users to secure the network, while enabling instant private transactions and P2P messaging that are impossible to trace or censor. Miners and stakers are encouraged to participate via network fee payouts, causing consistent block generation and ensuring a lightning fast network overall. This document is intended to describe in detail the different systems that the DigitalNote project employs and how they operate in unison to provide the end user of any community a seamless and intuitive experience.

FEATURES & SPECIFICATIONS

Supply cap: 10,000,000,000 XDN

Consensus: Proof-of-Work + Proof-of-Stake

PoW algorithm: bmw512 (Wish) - ASIC resistant

PoS algorithm: Echo512 - ASIC resistant

Block time target: 2 minutes

Minimum enforced block spacing: 45 seconds

Maximum block spacing (soft limit): 3.17 minutes

Confirmations required to spend: 15

Masternode collateral: 2,000,000 XDN

Block reward: 300 XDN (PoW + PoS + dev allocation)

Block reward split: 250 XDN PoW + PoS see-saw, 50 XDN dev allocation

Difficulty retarget: VRX v3.0 w/ hybrid chain swing

CodeBase origins: BTC 0.11 reference source + custom XDN features (dynamic max-block sizes, MN/Network payout see-saw, dev allocation, velocity blockchain constraint system) + DASH features (Darksend, InstantTX, messaging, masternodes)

Masternode swing base: 100 XDN/block

Masternode swing peak: 200 XDN/block

Network swing base: 150 XDN/block

Network swing peak: 50 XDN/block

Emissions swing:

- *Incremental step:* 20% step
- *Interval:* 30 blocks
- *Step per interval:* 1 step
- *Steps per swing:* 5 steps (up or down)
- *Epoch (see-saw finish):* 15 intervals
- *Upswing duration:* 5 intervals
- *Downswing duration:* 5 intervals
- *Idle duration:* 5 intervals (no adjustment)

FEATURES & SPECIFICATIONS

Supply Cap: The maximum coin supply is estimated to be reached ~25 years after launch around 2044, with a variance depending on how many coins are burned after the swap period ends. Once the maximum coin supply is reached, the XDN system will only pay network fees to the participants of the blockchain's emissions ensuring an exact cap of 10 billion XDN to ever exist.

Coin Burn: Users have about 6 months to swap their XDN from the old codebase to the current one. Funds that have not been swapped from the old codebase within the swap period will be "burned", thus lowering the circulating supply of XDN.

Reserve Blocks: Initially the DigitalNote team mined what are known as "reserve blocks" in order to generate the proper amount of coins needed for the swap from the old XDN codebase to the current one (specifically 80,000,000 XDN per block for blocks 2-102). By doing so users are able to retain their balance from the previous blockchain project and move onto a more secure and stable codebase. A small portion of this was saved into a DigitalNote project fund in order to complete the XDN v2.0 upgrade successfully, ensure future exchange listings and allow for future expansions and features.

Block Reward Split: A portion of the network paid emissions (50XDN/block) is sent to a developer team address to support DigitalNote team members directly so that they may continue development and be compensated for their work.

ENCRYPTED MESSAGES

"P2P encrypted messages are completely anonymous, private and uncensorable."

Approaching the secure/private messaging system is a daunting task as there are many implementation references floating and many schools of thought on proper implementation and functionality of this sort of feature. For the DigitalNote system we went with simplicity and effectiveness by using a Dash reference private message system, which will soon reincorporate the legacy XDN self-destruct feature, allowing users to force their messages to become deleted from both the sender and recipient's history and data all together.

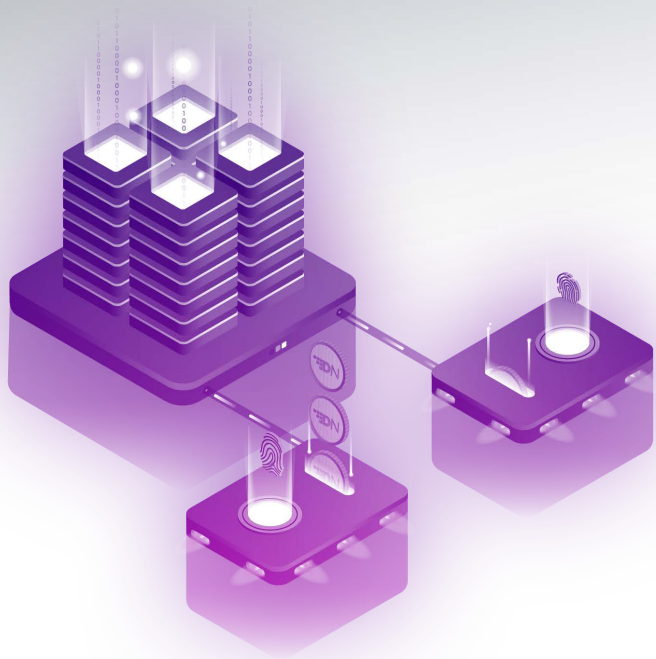
In addition to this the XDN method relays messages directly using p2p (peer-to-peer) protocol by first sending the message data through an encryption method, much like how blocks are encrypted on the blockchain itself, and then relaying them through the p2p protocol. The recipient then decrypts the message locally through the wallet/client and is able to then read and/or reply to the message. The system is very flexible and allows for further feature updates such as aliases and account registration on the network if the user so opts. There is no "middle-man" or third party at any part of the function of the private messaging so there is nothing to intercept or risk when relaying a

message to another party. Only the sender and the recipient using the proper authentication keys can access the messages and once again if they are self-destructing then in a designated period of time the message will eventually erase itself and cease to ever exist entirely.

Encryption keys used by either the sender or recipient are stored in an encrypted file just like the main wallet data file and require the wallet/client to properly load and unlock these keys using the appropriate data file. Further security such as a passcode to lock and unlock the messaging functionality in order to protect from possible equipment compromise or other emergency situations are also a reality being able to plug right into this system further improving user security and privacy with this system. If either data file goes missing from the messaging system it will be automatically recreated however the new one will be blank thus either erasing all previous normal messages (not including self-destructed messages) or even rendering that receiving address/key lost forever and inaccessible to any party. Storing and backing up this would of course be a wise decision however for utmost security and privacy this system operates in such a manner.

In general this is a powerful and adaptive system that is a great solution to many shortcomings of the way we currently communicate in the world.

INSTANT & ANONYMOUS TX



"The network combines its legacy CryptoNote ring signature obfuscation with coin mixing."

Obfuscating and overall concealing transaction source and destination has always been a big aspect of blockchain technology for quite some time now. From CryptoNote codebases which are designed solely for this type of method but execute it poorly to such projects as Dash and PIVX to name a couple that have provided attempts at creating a solution to this.

DigitalNote's execution of this type of feature is to utilize Dash's protocol and improve upon it from there similarly to the previously discussed messaging feature. The reason behind this is that overall the system is a good base point. It works by first having a "pool" of available denominated coins that users have configured using their wallets and are shuffled around in order to conceal their original source. Next when a user utilizes the feature the transaction undergoes what's known as mixing. Mixing then does as the name suggests and mixes the transaction up through the Masternode system utilizing denominated coins thus making tracking either difficult or near impossible. This method of course is not perfect as a very determined individual or entity could, using custom software and advanced systems, be able to track through the mixing process and

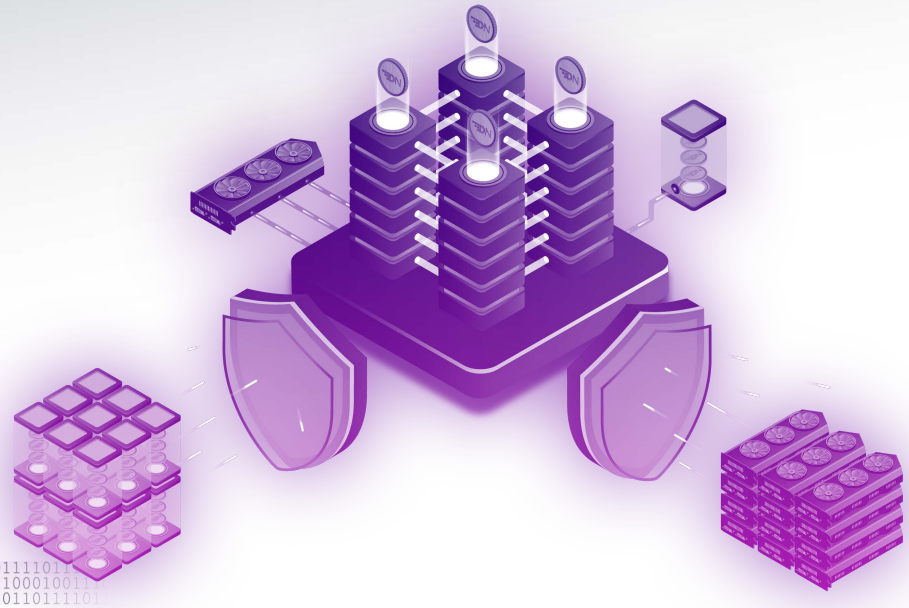
eventually find where the transaction was either sent from or to despite using this type of feature.

A solution to this is to incorporate the way that CryptoNote codebases had done utilizing ring signatures to properly obfuscate the transaction further beyond what conventional mixing and denominated coin balances can do. By putting these two systems together XDN will effectively create a "best of both worlds" scenario where the transaction cannot be tracked by any party no matter how determined they are. Both recipient and sender remain anonymous and unknown. Of course if the user so desires they may send a "clearnet" transaction in which case the transaction is not put through such a rigorous and complex process but instead simply relayed directly across the network. Legacy CryptoNote ring signatures for obfuscation will be reincorporated and combined with coin mixing soon. That being said XDN's standard method of sending is through the Dark or anonymous sending rather than clearnet as that has been the project's main aspiration since its inception.

Going beyond just security and privacy for the senders this solution also provides a hands off approach for the operators of masternodes or even the controlling party of the project as no one has the encryption keys for any user and they are never stored on any system other than the user's own. Making this secure, private, robust and simply a fantastic solution to currently lacking implementations.

RESISTANCE TO 51% ATTACKS

"DigitalNote takes a proactive approach to 51% attacks, eliminating them"



A 51% attack refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hashrate. The attackers could then prevent new transactions from confirming and reverse transactions that were completed during the attack, allowing them to halt payments on the network and attempt double-spends. In the past a 51% attack was considered more of a hypothetical attack, but the popularity and wealth of cryptocurrencies has made this type of attack a serious reality for all cryptocurrencies that do not actively develop systems to fend them off. There are various ways to combat 51% attacks and the DigitalNote network deploys multiple strategies together to help ensure the security of the protocol.

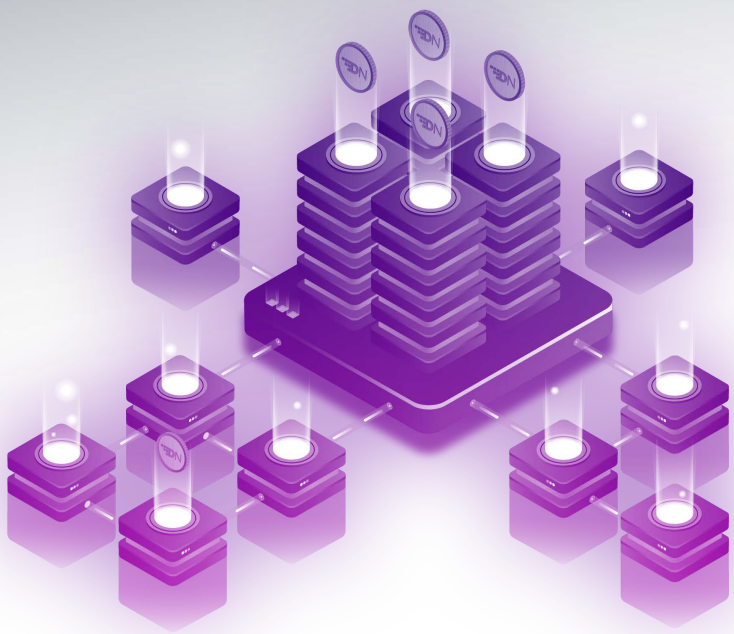
The first quality of the network that protects it from 51% attacks is the fact that DigitalNote is secured by Proof-of-Work and also Proof-of-Stake. That means that by the very nature of this setup, not only must an attacker have 51% of the hashrate but they must also have 51% of the total amount of coins to be able to attempt such an attack. While that is highly unlikely in itself, there is also another set of systems that adds an additional layer of security verses 51% attacks.

RESISTANCE TO 51% ATTACKS

Terminal Velocity RateX (VRX v3.0) balances the difficulty levels of the network so that neither Proof-of-Work miners nor Proof-of-Stake users have an advantage over the other. This system ensures that neither block type can overpower the other and both miners and stakers can benefit the blockchain equally, eliminating either as a potential 51% attack vector. VRX also ensures a narrow window around the desired block target (while still allowing for some variance) via it's velocity blockchain constraint system, essentially eliminating timestamp attacks. To learn more about the DigitalNote VRX v3.0 difficulty retargeting algorithm please read the detailed technical section dedicated to it.

Many other coins (including Bitcoin & Ethereum) are open to 51% attacks. DigitalNote takes a proactive approach, eliminating them. The wallet also verifies the entire incoming block before ever storing it to your disk, checking the stake difficulty and other parameters to make sure that a 51% attack is impossible.

MASTERNODES



"Masternodes enhance untraceability and provide incentive for users to secure the network."

Masternodes are essentially service handlers that process additional feature data for the blockchain without compromising security by forcing a verified collateral lock of a specific amount of XDN coins to run/operate. The lock is verified by the masternode launching protocol and then the Masternode is registered to the network and begins relaying data. This system ensures that the security and flexibility of the DigitalNote project and blockchains in general is not lost once again strengthening the overall network.

The way a Masternode functions is by having a participant register themselves on the network as an additional data processor allowing them to store/relay additional data that is then used to provide additional chain features such as InstanTX and Darksend. Similarly to the standard transaction protocol, a Masternode requires a persistent internet connection and penalizes any participant that consistently disconnects to avoid inconsistent connections or any possible hang-ups in service provided to end users. The longer that a user participates in the system the higher their chance become of being part of the compensated Masternodes which are automatically voted on by the network

depending on reliability and data processed. A participating user must then also lock the specific collateral amount, as mentioned previously in the Rewards and Consensus section, which will effectively become frozen as the participant will no longer be able to use them in any way until they are unlocked from the Masternode and in doing so have the balance act as a held collateral while the Masternode owner is compensated periodically for the data processed by their Masternode. Of course the payouts are not consistent and users should not expect a reward every block as the network will not always be selecting the same Masternode as a winner. Users may also force unlock their locked collateral amount instantly unregistering their activated Masternode from the network. A more proper method would be for the user to simply, using the system interface or RPC commands, first turn off their Masternode and then wait a short while for the network to unregister it normally and then unlock their coins.

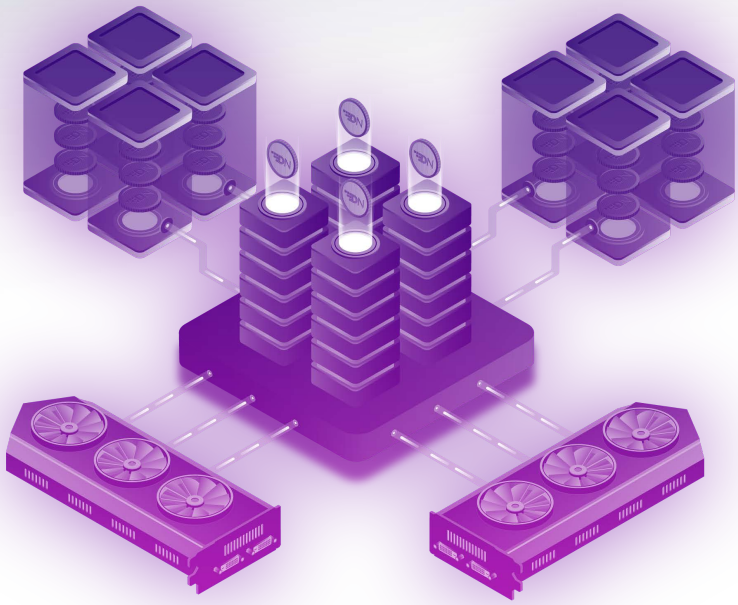
A locked balance will not be able to find the next block in the chain however any coins generated by the network is then taken and a portion of it is sent to the winning Masternode vote. Winning is determined by many factors that the chain automatically votes on such as network latency, time online, data processed, and so on. Voting on the network in this manner is crucial to ensuring the most helpful and critical Masternodes are rewarded first and more often than ones that do not provide a good, reliable service. The network payout split of the miner/staker and the winning Masternode swings between which is dominantly receiving rewards by using a mathematical seesaw which calculates a swinging curve both up and then back down in what's called a cycle. Two cycles are then called an epoch which counts a completed seesaw between dominant network payout. Epochs then infinitely repeat in predefined intervals allowing the chain to forever have this smooth fluctuating payout scheme.

MASTERNODES

This “SeeSaw” is designed to generate both holder and mining/staking interest as the network swings between which is being compensated more and overall keeping things interesting as opposed to a static reward system. The system also prevents possible abuse of payout types leveling the field between the two receiving parties. By aiming to be more dynamic not only can further user interest be stimulated but also a level of security is added and sense of balance between network participants

PROOF OF WORK + PROOF OF STAKE

"The XDN PoW/PoS hybrid system makes the network 2x as secure."



DigitalNote uses a Proof-Of-Work/Proof-Of-Stake (PoW/PoS) hybrid blockchain which directly affects how the system handles block production and stimulates interest in doing so while bolstering security and the protection from a 51% attack which still haunts many current projects.

Proof-Of-Work or (PoW) as it's often referred to, is the most notable consensus method as it's also the most common among blockchain projects since its use in Bitcoin. PoW functions by having participants contribute computing power in a form known as "hash" or "hashing" in reference to the process of creating a block of the blockchain. Participants are rewarded for correctly submitted blocks that are accepted by the blockchain/network and then confirmed as the block ages ensuring subsequent generation (mining) of future blocks by keeping participants interested. Furthermore multiple participants typically pool together their resources by using a "mining pool", as opposed to normally competing against each other, service allowing even those with little computing power to be able to receive compensation for what they do provide rather than attempting to beat an entity with considerably more hashing power. This

distribution method falls short of perfect though as it is possible to attack the blockchain by controlling what information is in the blocks being mined and submitted. These are known as "bad blocks" which are blocks with invalid information that would normally not be accepted even possibly splitting the blockchain into two versions of itself (forking) that then compete for network validity and acceptance when an entity has the ability to compute with massive amounts of power that the majority do not have access to.

Proof-Of-Stake or (PoS) for short is a newer method of block generation, however arguably one of the more secure methods of distribution though not as readily available to newcomers just climbing on board a community/project. This is because PoS uses the coins that a participant owns and is holding to generate a block, thus owning more coins and staking them provides the participant with a higher possibility of generating the next block. Staking is the act of allowing one's wallet/client to remain online in order to support the network by having randomly selected coins become temporarily unavailable while the wallet/client forges a block and then compensates the participant with an earned interest on the coins used. The longer one has owned their coins the more "weight" they accumulate and the higher their chances of forging the next block, once the block is found the coin's weight is reset to allow for other participants a chance of also mining a block. This method is considered more secure as if properly distributed the participants will invalidate most any form of attack that abuses hashing power in order to gain control of a blockchain, however one must first obtain coins in order to stake which depending on their worth can be costly and overall a deterrent to the project if this is the only method available.

PROOF OF WORK + PROOF OF STAKE

PoW/PoS Hybrid, known typically as just a "hybrid" distribution method, shuffles both PoW and PoS together onto a singular blockchain. Hybrid systems are still relatively new, as few blockchains employ a robust enough difficulty algorithm which adjusts the time span between generated blocks for either PoW or PoS and in this case both in unison. A custom difficulty retarget algorithm known as "VRX" was created for DigitalNote in order to allow for proper shuffling of generated block types within a full hybrid blockchain. By doing so the security of DigitalNote is substantially increased as PoW and PoS complement each other's shortcomings, allowing the blockchain significant edge over one operating singularly on a particular method, almost completely negating the possibility of a 51% attack.

TERMINAL VELOCITY RATEX (VRX)

"VRX v3.0 balances PoW and PoS while also securing the network against attacks."

VRX or Terminal Velocity RateX is a blockchain difficulty retarget system that, using a several block depth scan, quickly adapts the implemented blockchain/altcoin's mining or staking difficulty levels to ensure a narrow window around the desired block time. Allowing of course for some inconsistencies in block spacing due to significant increases or decreases in hashrate/staking depending on whether the blockchain is Proof-Of-Work based, Proof-Of-Stake or Hybrid, the VRX system ensures that blocks are generated at a consistently even pace. Furthermore for Hybrid blockchains the blocks are properly shuffled in a 50/50 ratio allowing both consensus types an even chance.

Simply put VRX indexes a previous set amount of blocks (typical reference implementations are set to the previous six blocks) and then compares each of them against one another in relation to their block times thus determining a set spacing between those blocks. The system then takes the determined block spacing and compares it against desired block spacing in what is called "Check Round". This check round is similar to the other retarget systems available but adjusts on a different curve

which adapts quickly to large changes in the hashrate of the blockchain, also making sure to not adjust too much so as not to "stall" the blockchain. There is one check round per pair of blocks indexed so using a six block count index depth VRX will yield five check rounds. After VRX runs through its checks it then determines whether it should change the difficulty either up or down depending whether the desired block time was overshot or rushed, the severity of which is limited to a maximum of doubling the previous block difficulty or halving it. Finally an average is calculated between the different pair of difficulty changes so that the most logical change in difficulty occurs that best suits the blockchain and is then logged by the DigitalNote system.

Late versions of the VRX systems (such as the one used) feature a unique PoW/PoS difficulty swing in which hybrid systems skew the difficulty on a curve in favor of the less often found block type. Doing so ensures that neither one block type can win out over the other one and both miners and stakers can benefit the blockchain equally. VRX was designed to directly interact with DigitalNote' Velocity block constraint system, which is discussed at greater length in the next section. This is because no other difficulty retarget method was compatible with it since the block difficulty plays an important role within the Velocity system itself.

Overall this document's intention is provide a general understanding of what VRX is and what it does. This VRX system will continue to evolve to become more robust and overall an effective solution to the blockchain difficulty retarget problem.

VELOCITY BLOCKCHAIN CONSTRAINT SYSTEM

Velocity is a tertiary blockchain constraint system designed to ensure stringent block checks and parameter enforcement. This system was designed as a modular/scalable framework and over the years of its use has been expanded to include other check types along with being planned for considerate new check implementation. Showing its usefulness now in several different blockchain implementations Velocity is looking to be a promising blockchain feature.

The key importance of Velocity is to constrain the chain with the parameters already defined within the code as opposed to having aspects such as block spacing and other properties act almost as a suggestion to the chain's operation rather than rule and law so to speak. This is very important in the sense that sudden increase in hashrate or possible attacks are still a vulnerability despite the best retarget systems out there being implemented to control block spacing along with network fees, possible invalid balance issues while sending transactions and other portions of the blockchain that are enforced with a double check but still susceptible to an attack whether it be temporary or a double spend that is confirmed and causes users of the network grief and loss which is unacceptable.

This is done by the Velocity system being a "triple check", even after a block during generation has seemingly met all requirements and is then produced it is now no longer immediately accepted. Instead it is checked again for inconsistencies and possible other exploits. Most notably users will see rejected blocks during the mining or minting phase (or both depending on coin properties), despite the tendency to assume that

there is something wrong with the chain as it is rejecting blocks this is in fact a completely normal and a welcomed operation.

Reasoning is that rapid block times, incorrect fees, insufficient balance, faked/altered timestamps, altered inputs/outputs and other issues can be manipulated by a talented programmer with malicious intent. To guard from these kinds of situations Velocity checks the generated block against the chain parameters, first it Velocity checks the block for proper spacing, if the block was generated too quickly it thus has not met one of the main parameters for the chain and is promptly rejected, staving off possible attacks and any kind of sudden increase in hashrate. Additionally to verifying block spacing Velocity also checks both block timestamp and block transaction timestamp against previously indexed values in order to verify the legitimacy of the timestamp within a block. This is done at least a couple blocks or more deep to ensure timestamp attacks are negated.

Next the system verifies that previously the client that sent a transaction (if it sent one in the previous block) was in fact a valid transaction by comparing previous balance vs current balance along with fees paid vs minimum fee required to pay. If any of these parameters are not met (mind you these are standard chain parameters and nothing outlandish) then the block is again rejected despite being generated successfully. Thus this system secures the chain, making it more stable, predictable, and overall reliable, instilling confidence that the blocks that are accepted are indeed blocks that are proper.

Currently the biggest shortcoming is that this feature is still a prototype system and as such doesn't intuitively integrate into every blockchain flawlessly. Some can experience issues such as minimum spaced blocks with either min-diff or near min-diff being used which is not an optimal operation of any sort. Next the transaction verification and previous balance checks are currently turned off until such a time as the checks become flawless, the implementation for these specific checks are still being developed to properly assertain those sections of chain parameters. Hybrid blockchains require a more intuitive difficulty retarget approach to reduce rejected blocks and cause the system to properly generate blocks so that Velocity becomes not a life support system but merely a security check to a stable and properly operating chain. Users of a Velocity implemented chains may also note that several blockchains have now been implemented with this feature, however the potential issues will not be apparent in them because they are implemented with VRX difficulty retargeting which pairs with Velocity's constraints and thus will not have the same issues listed above, in this case they will see only the benefits of Velocity running as a security check merely stabilizing the blockchain further and making it more robust.

Security Analysis

Miners may also be able to create automated cutoffs for the system so as to not waste power while blocks are simply not accepted by the chain creating two possible exploits. First that users with advanced mining systems may be able to effectively premine a block during the time that the chain is not accepting blocks and withhold it from submission until the minimum time has elapsed. If the system were to then employ a security check that verifies the block's timestamp to see if a miner had withheld a block for submission another exploit would be to set a withheld block to be created with a

valid timestamp as long as the miner knew each valid time window. These two exploits are resolved first by having the previously stated method of the system ensure the block timestamp does not come from outside the allowed block window. This discourages attacks by creating more steps for the attacker to go through before having a chance of success. Next the VRX implementation penalizes minimum block time, making the power required to maintain a possible attack (even with injecting a valid timestamp) increase exponentially until after just a few generated blocks the difficulty is so great that minimum time can no longer be achieved and another miner/staker can simply find the next block. This quickly negates any possible progress in the attack. Of course the Velocity system requires all parameters to be met and not simply just block time in order to accept what appears to be a validly generated block.

The system can be expanded to include more verification and an even more stringent implementation that may adapt to any kind of features that are added or removed. This makes the DigitalNote system very adaptable and less of a hassle to work with as it can grow with the coin and as it becomes more refined and mature so will this new security feature called Velocity.

LIGHTWEIGHT/MOBILE CHAIN

As a blockchain grows it becomes "heavier" in the sense that it continuously stores information without regard to possible hardware or service limitations to the end user. In order to circumvent such a concern for possible mobile users or users who simply cannot store the entire chain either at that moment/ indefinitely it is important to offer an alternative to what's known as a "full" client. Standard or "full" clients by general practice store and verify the entire blockchain which allows for significant redundancy and support as community members/users use the system while a "Lightweight" or "Mobile Blockchain" acts as an access portal, querying the blockchain and pulling data from it more like a block browser rather than actually storing the system locally.

By not storing the majority of files locally the DigitalNote system can more readily be used in full scale on a mobile device or by a user with limited network/storage capacities. Though much of what makes this system lightweight is simply crawling the blockchain it also of course has the capability to submit data to the blockchain to be processed in the upcoming block with or without synchronizing the blockchain. Every system should allow for customization by the user that is using it and as such the Lightweight/Mobile Blockchain is also capable of synchronizing either partially or wholly. If the option is selected, the system will synchronize from the last checkpoint and "assume" that previous transactions reported by the chains hosted by nodes are valid. Another option is to have a "quiet" full sync to run where after the semi-sync is completed from the last checkpoint the client then begins synchronizing the rest of the blockchain silently in the background allowing the user to still support the network completely at their discretion.

ADAPTIVE BLOCK SIZES

Another common shortcoming that many groups have attempted to overcome is block size limitations. Either too small or too large can be problematic as one renders the chain incapable of processing large batches of transactions within any kind of reasonable time as the network effectively "queues" up and users are stuck waiting unknown amounts of time to receive or send their coins while the other causes the chain to be possibly bloated by having overly large block sizes available when there is no need for it. This can even lead to such issues as stalled blockchains.

Employing what's known as "Adaptive Block Sizes" the XDN blockchain itself automatically calculates, within a size threshold, how large the maximum allowed block size that it should be adjusted to and then sets this as the next allowed size for the network to utilize. This is based off of network usage, the more the network is utilized the more space is made available to the block size, while the less it is utilized the lower amount of space is available to the block for generation size allowing for seamless adaptability of the blockchain system to handle any kind of network load and environment.

CONCLUSION

This whitepaper (document) is for informational purposes only, and not a binding commitment. Do not rely on this information when interacting with DigitalNote coins as ultimately the development and timing remains at the sole discretion of the DigitalNote team.

We, the DigitalNote team, intend in no way harm of any kind to anyone in any shape or form. There has never been a crowdsale of coins, presale or any other crowd funding method used for the DigitalNote project or its developers. Please understand the risks involved with cryptographic blockchain technology and their respective coins. The DigitalNote team cannot be held responsible for any lost, stolen, or otherwise missing funds of any kind. If you are unsure or have any doubt about this project we urge you to NOT invest or become involved as this is a prototype technology system as stated in numerous areas and to be used at your own risk.

CREDITS

Big thank you to all who helped make this project a reality, special thanks goes out to the following community members (usernames) who have contributed to this document's creation and revisions:

AuCHRI

Coke Zero

CryptoCoderz

Kou