The CyberMiles DPoS Protocol

Disclaimer

This article contains forward-looking statements that are based on the beliefs of Cybermiles Foundation Limited ("CyberMiles"), a company limited by guarantee incorporated in Hong Kong, as well as certain assumptions made by and information available to CyberMiles. No representation or warranty is given as to the achievement or reasonableness of any plans, future projections or prospects. If and when the CyberMiles platform is completed, it may differ significantly from the one set out in this document.

Furthermore, no representations or warranties are made as to the accuracy or completeness of the information, statements, opinions or other matters described in this document or otherwise communicated. Nothing in this document is or should be relied upon as a promise or representation as to the future or investment advice. To the fullest extent permitted under applicable law, all liability for any loss or damage whatsoever (whether foreseeable or not) arising from or in connection with any person acting on this document, or any aspect of it, notwithstanding any negligence, default or lack of care, is disclaimed. To the extent liability may be restricted but not fully disclaimed, it is restricted to the maximum extent permitted by applicable law.

The views and opinions expressed in this paper are those of the CyberMiles only. They are not advice, nor an offer or solicitation of any kind, nor may they be relied upon for any purpose. CMT and the CyberMiles platform are not intended to constitute securities or any other regulated products in any jurisdiction. Please obtain any necessary professional advice.

I. What is the mission of CyberMiles?

CyberMiles aims to build a smart contract platform that is similar to Ethereum but heavily optimized to facilitate e-commerce transactions. Our blockchain enables people to construct and execute business contracts enforced by computer code. Our goal is to build an e-commerce ecosystem that is native to the network era:

- no rent-seeking centralized monopoly;
- more fair allocation of network rewards; and
- stronger network effects through economic incentives.

The result will be a new generation of e-commerce network that is more affordable to buyers (both in merchandise prices and financing options) and more revenue streams for the sellers (such as monetizing data, supply chain financing, and consumer loans).

II. What is PoS?

When Satoshi Nakamoto invented the Bitcoin, a key insight was an economic system that is more profitable to join the network than to attack it. In the Bitcoin system, the barrier to attack the system is called Proof-of-Work, or ***PoW***, consensus. However, over the years, it has also become apparent that the PoW consensus is too slow and wastes too much energy.

To solve PoW's problems, a new consensus mechanism called Proof-of-Stake, or ***PoS***, was proposed. A PoS system allows a vote for each new block by the network's token holders. The proposer of a new block is randomly chosen. Each account's voting power is proportional to the tokens held in it. The idea is that token holders, especially large token holders, are incentivized to vote to ensure the network's security. With voting, the blockchain can validate blocks with minimal amount of computation. The proposer of an accepted new block receives award in the blockchain's cryptocurrency. This process is called "***minting***" new cryptocurrency as opposed to PoW's "***mining***". A PoS system is typically much more performant than a PoW system.

However, a traditional PoS system also suffers from two significant problems: the first problem is still performance. All token holders can run a blockchain node to propose and vote on blocks, but most token holders have no expertise or budget to run computer hardware and software required for a high-performance node. Therefore, blockchain

network is as slow as its slowest node. The second problem is the "nothing at stake" problem, where a token holder can cheat by simultaneously voting on two competing proposed blocks.

III. What is DPoS?

Delegated Proof-of-Stake (DPoS) is an improvement to the PoS mechanism. It is similar to a representative democracy with land suffrage in human society. In DPoS, the token holders vote for a small number of representatives (we call those elected representatives **"validators"** throughout this article) to represent all token holders to run network operations. The validators run ***super nodes***, which are professionally run network servers to ensure the performance and security of the blockchain network. This solves PoS's performance problem.

The votes are casted in the form of staking one's tokens. The staked tokens are locked by the network as collaterals and can be slashed when the validators misbehave. The staked tokens are never transferred to the validators who they voted for. They are simply used as a proof of voting power and incentive for the token holders to choose responsible and capable validators to maintain the blockchain. The potential punishment solves the "nothing at stake" problem.

At CyberMiles, we believe DPoS is the future of high performance and secure blockchain consensus.

IV. How CyberMiles DPoS works

Delegated Proof of Stake is a crucial economic mechanism in the CyberMiles blockchain network to reward token holders who help to maintain the security and integrity of the network protocols. There are two roles in the CyberMiles DPoS protocol: ***delegators*** and ***validators***.

A. Delegators and validators

CMT holders who choose to be delegators lock up, or ***stake***, their CMTs to participate in the blockchain network's governance through a voting mechanism. The staked CMTs are held by the network and cannot be traded or transferred because they can be slashed when governance errors occur. In exchange, the delegators receive CMTs minted through systematic inflation and transaction fees in every new block created by the network. These CMTs are called ***block award***.

The delegators themselves typically cannot or will not run the computer servers that actually power the blockchain network. Instead, delegators hire, or ***elect***, other CMT holders, or ***validators***, for this task by staking their CMTs to specific validator candidates. Validators are responsible for maintaining crucial network infrastructure, and making rule changes and governance decisions on behalf of its delegators. Since there are only 19 validators in the CyberMiles system, validators must compete for delegators' votes (staked CMTs) in order to be hired by providing secure servers running up-to-date

software, sufficient computing power and network bandwidth to power the global blockchain network.

Delegators pay validators with a portion of their block awards. Each validator's share of the block award is called the ***validator's compensation***. A validator must declare a default compensation rate at the time of candidacy declaration. The default serves as the maximum compensation rate all delegators must pay this validator. However, once a delegator stakes the validator, the validator has the option to voluntarily reduce her compensation rate for this delegator. This allows the validator to recognize delegators who make significant contributions to the community.

If a validator misbehaves and tries to harm the network, the network might slash its staked CMTs causing a loss for its delegators. So, the delegators are incentivized to only stake for reputable and trustworthy validators, therefore improving the security of the whole network.

In the CyberMiles protocol, 10% of a validator's stake must come from this validator's own CMT holding. This ensures that each validator has skin in the game because its own CMTs are also at risk for being slashed. Hence, a validator is always also a delegator for itself.

Besides the 19 validators, the CyberMiles blockchain has 5 **backup validators** in case a

validator resigns, is hacked, or otherwise drops off after being slashed. The backup validators are also paid by delegators who elected them. The concepts of validator's compensation and self-staking both apply here. The CyberMiles DPoS protocol divides the total block award pool into two parts: validators and their delegators collectively receive 90% of the total block awards; and backup validators and their delegators collectively receive 10%. The delegators will find the equilibrium point in terms of staked CMT distributions between validators and backup validators. We expect the combined staking amount for backup validators will be somewhat higher than 10% the total staking amount, resulting in less income per staked CMT for backup validators and their delegators. That is because the backup validators take less risk of slashing.

The following table shows the responsibilities, risks and rewards for validators and delegators to participate in the network governance through the DPoS mechanism.

	Rewards	Responsibilities and Risks
Delegator	Receive block awards for the CMTs it stakes in the network.	Have to give up trading for staked CMTs. Small risk of being slashed if its staked validator misbehaves (up to 1.2% of stake).
Validator	Receive validator's compensation from delegators' block awards and block awards from self-staked CMTs, by validating blocks. Participate in network governance.	Have to give up trading for self-staked CMTs. Responsible for sophisticated IT system operations with risks of hacking and being slashed.
Backup validator	Receive validator's compensation from delegators' block awards and block awards from self-staked CMTs.	Responsible for sophisticated IT system operations as a backup for validators.

A1. Voting power

The block award is distributed to the delegators and then validators based on voting power. Each stake from a delegator has a certain amount of voting power. Each validator's voting power is the sum of all its current stake's voting power, and the entire system's voting power is the sum of all validators' voting power.

Definitions Set 1:

- S_{ij} is the amount CMTs staked to validator i by delegator j. There are n delegators for validator i including the validator itself.
- V_{ij} is the adjusted amount CMTs staked to validator i by delegator j. The current voting power for delegator j at validator i is expressed as V_{ij}. In general, the voting power grows with the staked amount of CMTs at the current time.
- S is the total amount of CMTs staked to all validators. It can also be expressed as $\sum_{i=1}^{m}\sum_{j=1}^{n} S_{ij}$.

The CyberMiles protocol disincentivizes any validator from growing too big. If a single validator's stake grows above 12% of total stake of the network, this validator could cause instability in the network. So, the network protocol adjusts S_{ij} downward for this validator. This threshold incentivizes large CMT holders to diversify and stake in multiple validators, and it incentives validators to limit their max accepted stake.

$$V_{ij} = \min\left(S_{ij},\ S_{ij} \cdot \frac{12\%}{\sum_{j=1}^{n} S_{ij}/S}\right)$$

A2. Block award shares

The block award share for any delegator and validator depends on the current total voting power, award pools reserved for regular and backup validators, and the validator's compensation rate for each of its delegators. The next set of equations specify the portion of block awards distributed to delegators and validators.

Definitions Set 2:

- C_{ij} is the validator's compensation rate for delegator j at validator i. As we had mentioned, the validator can adjust compensation rate for individual delegators in its stake pool.
- $R_r(i)$ is the portion of the block award pool reserved for validator i's type. For example, it is 0.9 for validators, and 0.1 for backup validators.

In each block, the portion of block award each validator and delegator gets are as follows.

$$\textbf{Block award share for validator } i = \frac{\sum_{j=1}^{n}(V_{ij} \cdot C_{ij})}{\sum_{i=1}^{m}\sum_{j=1}^{n} V_{ij}} \cdot R_r(i)$$

$$\textbf{Block award share for delegator } j \textbf{ at validator } i = \frac{V_{ij} \cdot (1 - C_{ij})}{\sum_{i=1}^{m}\sum_{j=1}^{n} V_{ij}} \cdot R_r(i)$$

The source of the block awards is a combination of the systemic inflation determined by the validators (up to 8% per year) and the gas fees collected from transactions in the

block. In our implementation, we might choose to compute and distribute aggregated block awards every hour or even every day.

A3. Corollary

The formula to compute voting power leads to an important corollary on the potential compensations for validators and delegators.

Corollary: The more stakes a validator can attract outside of her self-stake, the more compensation the validator can receive.

Based on the engineering design of the staking mechanism, the validator can encourage and incentivize certain delegator behaviors by changing individual delegator's validator compensation rate.

A4. Examples of validator and delegator compensation

The detailed computation of validator and delegator compensation is complicated and depends on many external factors such as the staking behavior of others. In this section, however, we will look into simplified scenarios to illustrate potential ROIs. Our assumptions include the following.

- The system has reached equilibrium.
    - There is no new stake growth for all validators.
- Each validator has the same numbers of delegators.
- All delegator and validator pairs have the same validator compensation rate.
- The transaction fees are negligible in transactions.

Definitions Set 3:

- $\boldsymbol{Total(t)}$ is the total number of CMTs at time t. $\boldsymbol{Total(0)}$ is the current total number of CMTs.
- $\boldsymbol{I}$ is the system inflation rate, per year.
- $\boldsymbol{C}$ is the validator compensation rate across the system.
- $\boldsymbol{SSR}$ is the self-staking ratio of the validator.
- $\boldsymbol{R_s(i)}$ is the percentage of staked CMTs that are staked for validator i's type. It is needed as the block awards are only distributed to staked CMTs.

The following formula compute the annual incomes for validators and delegators respectively, for each CMT staked from one's own account.

$$\boldsymbol{Validator\ income/CMT = \frac{I \cdot Total(0)}{S(0)} \cdot \left(1 + \left(\frac{1}{SSR} - 1\right) \cdot C\right) \cdot \frac{R_r(i)}{R_s(i)}}$$

$$\boldsymbol{Delegator\ income/CMT = \frac{I \cdot Total(0)}{S(0)} \cdot (1 - C) \cdot \frac{R_r(i)}{R_s(i)}}$$

The following table shows how to apply the above formula to compute the block award for delegators, and validator's compensation, in different scenarios. The validator and delegator incomes listed in the table are per 100 staked CMTs per year. For simplicity, the table assumes $\frac{R_r}{R_s} = 1$, meaning the backup validators receive 10% of the total staked CMTs, making their income identical to regular validators.

Validator's compensation as a percentage of block awards (C)		If 50%		If 20%	
Stake ratio (Total/S)	Validator's self-staking ratio (SSR)	Validator (CMT)	Delegator (CMT)	Validator (CMT)	Delegator (CMT)
25%	10%	176	16	90	26
25%	20%	96	16	58	26
25%	40%	56	16	42	26
50%	10%	88	8	45	13
50%	20%	48	8	29	13
50%	40%	28	8	21	13
75%	10%	59	5	30	9
75%	20%	32	5	19	9
75%	40%	19	5	14	9

Note:

1. The "stake ratio" column is the percentage of total CMT supply that is staked for DPoS. For example, initially there were a total supply of 1 billion CMTs, so a 25% means overall 250M CMTs are staked by their holders to participate in the DPoS mechanism.
2. We are assuming a system wide inflation rate of 8% per year, which is the source of block award.
3. Validator income = validator compensation + block award from self-staked CMTs
4. Delegator income = block award from staked CMTs – validator compensation
5. The validator does not stake more than 12% of the "total CMTs staked". The income drops for if the validator exceeds that threshold. See B4 for why this threshold exists.

Incomes for both validators and delegators go up when fewer people stake their CMTs, as the 8% inflation is divided up amongst fewer parties. The validator's per-staked-CMT income goes up when it stakes less of its own tokens and gets compensation from other delegators' stakes. However, as we discussed, each validator must self-stake at least 10% of its total stake.

Next, let's compute incomes when validators receive a risk premium over backup validators. In the following table, we assume that the validator's compensation (C) is 20%, and the 30% of total staked CMTs are staked to backup validators (R_s). Recall that backup validators and their delegators collectively receive 20% of the total block awards (R_r). The

30% staking ratio means that each CMT staked to backup validators will generate less income than each CMT staked to regular validators. Delegators do that because the backup validators have less risk of slashing.

Stake ratio (Total/S)	Validator's self-staking ratio (SSR)	Validator (CMT)	Delegator (CMT)	Backup Validator (CMT)	Backup Delegator (CMT)
25%	10%	103	30	60	17
25%	20%	66	30	39	17
25%	40%	48	30	28	17
50%	10%	51	15	30	9
50%	20%	33	15	19	9
50%	40%	24	15	14	9
75%	10%	34	10	20	6
75%	20%	22	10	13	6
75%	40%	16	10	9	6

B. Ongoing validator election

Once the network is up and running, validators can be voted in and out at real time. At all times, the top 19 validator candidates that have the most "voting power" (as measured by staked CMTs) are "hired" as validators by the delegators. Validator candidates ranked between 19th and 24th are elected as backup validators.

B1. Declaration of candidacy

A validator candidate declares its candidacy to the network. It will give out 3 pieces of information in the declaration:

1. Details of its operation and credentials, including jurisdiction, data center location, security setup, and technical setup. The CyberMiles Foundation will evaluate all validator candidates, and publicly indicate the candidates that meet the Foundation's standards (i.e., information accuracy, technical competency, and hardware / network setup). However, the token holders are free to stake for any candidate regardless whether it meets the Foundation standard or not.
2. The maximum amount of CMTs it is willing to accept as stakes. In order to prevent any single validator from growing too big and therefore risking monopoly, the network protocol punishes very large validators and their delegators. (see the "B4. Block award and validator's compensation" section for details)

3. The validator's compensation rate it requires from delegators. For example, a 40% rate means that 40% of the block awards earned by delegators who staked this validator, will be paid to this validator as compensation.

B2. Acceptance of candidacy

Upon a new candidate declaration, the network immediately takes 10% of the declared maximum amount of stake from the candidate's own account, and keep it as stake. If the candidate does not have 10% of the max, the declaration will fail. The validator can, of course, stake itself with additional CMTs later.

The CyberMiles Foundation will review the candidate's information. If the foundation can verify the accuracy of the information, it will denote on-chain that the candidate is "verified". CMT holders can stake any validator candidate they like, including the unverified ones, but verified candidates from the foundation give CMT holders more confidence to stake.

B3. Staking and unstaking

The validator candidate campaigns in the community and asks people to stake it (i.e., to hire it for the job of the validator).

CMT holders (delegators) stake their CMTs to the validator candidate. It is important to note that staked CMTs cannot be traded, and once staked, a delegator must request unstaking and then wait a week before he can trade them again. You keep getting award during the waiting period.

The waiting period of unstaking is to guard against something called "long range double spend attack".

Note:

During the initial stage of the network, all delegators must stake their CMTs through a specialty hardware device known as the CMT Cube. That is to ensure network stability and fund safety during the crucial period of network startup. The CMT Cube will be free and the blockchain staking protocol will be open to all after the network became stable. See more details in the last two sections herein.

B4. Block award and validator's compensation

Once the validator candidate receives enough stake to make the top 19, it becomes a validator, and all its delegators start to receive block award (about every 10 seconds). The block award includes two parts.

1. The system has an annual inflation rate of 8%. This inflation is distributed as newly minted CMTs to delegators.
2. The delegators also receive transaction fees paid by heavy users of the blockchain.

The total block award from the system is first assigned to the delegators proportional to each delegator's voting power. The system then automatically distributes the block award to the validators and delegators based on the validator's compensation rates. The awards are added to the stake by default. For delegators and validators to withdraw the CMTs for trading, they need to request unstaking and wait for a week.

A validator can withdraw its candidacy at any time. Once a validator withdraws, the next candidate with the most staked CMTs in line will become a validator. When a validator withdraws, all its staked CMTs will be automatically unlocked after the one-week unstake waiting period. **During the whole staking period, there is no transfer of ownership of the delegators' CMTs.**

B5. Slashing and punishment

When a validator becomes unavailable or produces results that are different from the rest of the validators, the system will slash and burn 0.1% of its total stake (i.e., the validator itself and all its delegators will lose CMTs) every block (every 10s). After 12 consecutive slashes, the system removes the validator and promotes the next validator candidate as a validator. That is, delegators can be punished for up to 1.2% of their stake in a misbehaving validator.

The removed validator will no longer suffer slashing loss, but none of its delegators will earn any block awards either. Its delegator can request to unstake from it, and then re-stake their CMTs after the one-week unstake waiting period.

C. Genesis validators election

When the CyberMiles main net goes online, it needs to start with 19 validators, known as genesis validators. However, the chicken and egg problem is that there is no way to stake before the main net goes online.

To solve this problem, prior to the main net launch, the CyberMiles Foundation will work with the community to elect genesis validators based on each validator candidate's projected voting power, as well as its contributions to the community. The election process will be transparent with a public scoring mechanism. The genesis validators are the top candidates with the highest score. The scoring criteria include:

- The initial amount of CMTs the candidate is willing to stake (at least 10% of its declared max – see below)
- Validator's compensation rate it requires from delegators
- Soft commitment of CMT stake from its community.
- The reputation of the operation entity
    - An official website
    - Company information (brief introduction of the team and list of key staff, photos, and relevant background qualifications)
- Size and activities of its community (i.e., Twitter, Telegram, Medium, etc. followers and interactions)

- Geopolitical diversity of the validators (i.e., candidates from under-represented countries will have higher weight)
- Commitment to run the validator nodes according to the technical standards set by the Foundation (total expenditure and technical plan; scaling plan for hardware)
- Community development plan (validator candidate roadmap on values, community project timeline, finances, transparency, or any other topics the candidate deems important.)
- Operational nodes on the testnet for community testnet participation

To participate in the genesis validator election, each candidate must

- Declare its maximum accepted staking CMTs
- Fund its own account with 10% of the max to be staked at genesis by the network
- Declare its validator's compensation rate
- Disclose detailed information about the organization or individual

Once the CMT Cube devices are distributed to CMT holders, the continuous validator election starts. CMT holders will use the CMT Cube to vote (stake) for validators they want to hire.

D. About the CMT Cube

The CMT Cube is a home-based device specifically designed to facilitate validator election during the initial stage of CyberMiles network operation. It is a hardware device that acts both a CMT wallet (i.e., stores and manages a CMT account), and an easy-to-use user interface, or UI, for staking the CMTs in the wallet to elect validators. Its UI also displays the up-to-date earnings (delegator's block award) the account receives over time. The hardware wallet at home is much safer than web-based or phone-based software wallets, and hence is ideal for holding and staking significant amounts of CMTs.

The CMT Cube hardware consists of an LED touch screen for managing CMTs in the associated account, a secure chip for storing private key information, and a mobile computer running a customized version of Android. It uses very little electricity, and only need to be turned on when the user needs to make changes to the account (e.g., to check account balance, to deposit or withdraw CMTs, to stake or unstake a validator etc.)

In the long run, any CMT holder will be able to stake his or her CMTs via an open software API provided by the network. However, during the crucial period of network startup period, the network is vulnerable to attacks and the CyberMiles Foundation must take an active role in making sure that the validator elections are free from attacks and frauds. The requirement for a hardware device creates additional safeguards for the validator election process. For example, as the device has an upfront cost (it will be reimbursed

over the year and eventually it is free) and has an upper limit for CMTs it can hold (100,000 CMTs), it is very hard for a large stake holder to split into hundreds of CMT accounts to secretly manipulate the election. The device also has a lower limit of 1000 CMTs it must hold and stake to prevent DDoS attacks or Sybil attacks that use small amounts of stakes to abuse the system.

The block award distributed to the delegators will automatically show up on the CMT Cube UI. Since the CMT Cube is the only way to participate in validator staking, it is currently the only way for CMT holders to earn delegator awards at the initial stage.

As shown in the "validator and delegator compensation" table, the expected income of each CMT Cube (delegator's income) is proportional to the amount of CMTs staked, and is related to factors such as the network-wide total staked CMTs, validator's compensation rate. We generally expect the delegator's income will be higher than the system inflation rate (currently at 8% per year).

The CMT Cube device will be sold exclusively on the cybermiles.io web site, and it will be priced in CMTs.

A second type of the CMT Cube is called the "CMT Enterprise Cube". It is a general computing device specifically designed for large stakeholders to stake. It has a minimum stake of 1 million CMTs for each delegator account, and can stake to multiple validators.

E. About CyberMiles App

CyberMiles App is a free mobile App can be used to stake CMTs and manage CMT asset, including but not limited to store, transfer, receive, and other functions.

Now CMT holders can stake CMT to Validators with CyberMiles App to get block awards.

V. Key parameters

Term	Value	Description
Annual inflation	Up to 8%	The amount of new CMTs "minted" by the system as block award for delegators and validators. The actual inflation rate is determined by a vote by validators, but should never exceed 8% per year.
Minimum self-staking ratio	10%	The amount of CMTs in a validator's stake that must come from its own funds.
Validator's size threshold	12%	The threshold (soft cap) a single validator can take in total network stake before the system diminishes the block award for this validator and its delegators.
Number of validators	19	The top 19 candidates with the most stake become validators. Their delegators will earn block awards.
Number of backup validators	5	The candidates with stake amounts ranked between 20th and 24th in the network. Their delegators earn block awards

Block award pool split between validators and backup validators	9:1	Validators and their delegators collectively receive 90% of total block awards; backup validators and their delegators collectively receive 10% of total block wards.
Block time	10s	Time for a new block to be created. Once a block is created, all the transactions in the block are confirmed and finalized.
Slashing	0.1% of stake every block for 12 blocks (up to 1.2% stake)	The system slashes and burns a validator's stake (including all the delegators who stake in it) when a validator misbehaves.

Unstake waiting period	7 days	The amount of time a delegator must wait to reclaim its funds when it unstakes a validator.
CMT Cube max	100,000 CMTs	The maximum amount of CMTs a single CMT Cube device can hold and stake.
CMT Cube min	1,000 CMTs	The minimum amount of CMTs a single CMT Cube device must hold and stake.
CMT Enterprise Cube max	None	The maximum amount of CMTs a single CMT Enterprise Cube account can hold and stake.
CMT Enterprise Cube min	1,000,000 CMTs	The minimum amount of CMTs a single CMT Enterprise Cube account must hold and stake.
CyberMiles App Max	100,000 CMTs	The maximum amount of CMTs a single CyberMiles App address can stake.
CyberMiles App Min	1,000 CMTs	The minimum amount of CMTs a single CyberMiles App address can stake.