FCAM

Decentralised Digital Investing

Ethereum - The Merge is Base Camp, not The Peak.

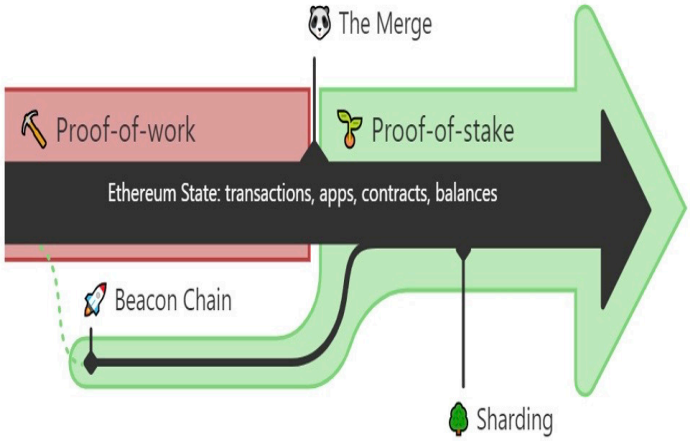
August 2022

The Merge. The first stage of the Ethereum scaling roadmap.

For anyone with even a passing interest in crypto currencies and particularly Ethereum, you will have noticed a lot of chatter recently about the upcoming Merge. In this note we will explain what the Merge is and why it's significant for the Ethereum blockchain now and for its future development.

Most simply, The Merge is the transition of the Ethereum blockchain from Proof-of-Work (PoW) consensus to Proof-of-Stake (PoS) consensus. It has been a years-in-the-making upgrade for Ethereum. In preparation for the final transition, Ethereum developers have run many tests on various test nets culminating in the last and most significant Goerli test net which was declared a success by the Ethereum core developers on the 12th of August 2022.

"The Merge represents the joining of the existing execution layer of Ethereum (the Mainnet we use today) with its new proof-of-stake consensus layer, the Beacon Chain. It eliminates the need for energy-intensive mining and instead secures the network using staked ETH. A truly exciting step in realizing the Ethereum vision – more scalability, security, and sustainability."



Source:

Since the beginning of the Ethereum project back in July 2015, proof-of-work has secured Mainnet. This is the Ethereum blockchain we know and use now —it contains every transaction, smart contract, and balance since it began.

Throughout Ethereum's history, developers have been hard at work preparing for an eventual transition away from proof-of-work to proof-of-stake. On December 1, 2020, the Beacon Chain was created, which has since existed as a separate blockchain to Mainnet, running in parallel.

The Beacon Chain has not been processing Mainnet transactions. Instead, it has been reaching consensus on its own state by agreeing on active validators and their account balances. And now, after extensive testing, we have an approximate date of 15th September 2022 for when the Merge will take place and the Beacon Chain will then be the consensus engine for all network data, including execution layer transactions and account balances.

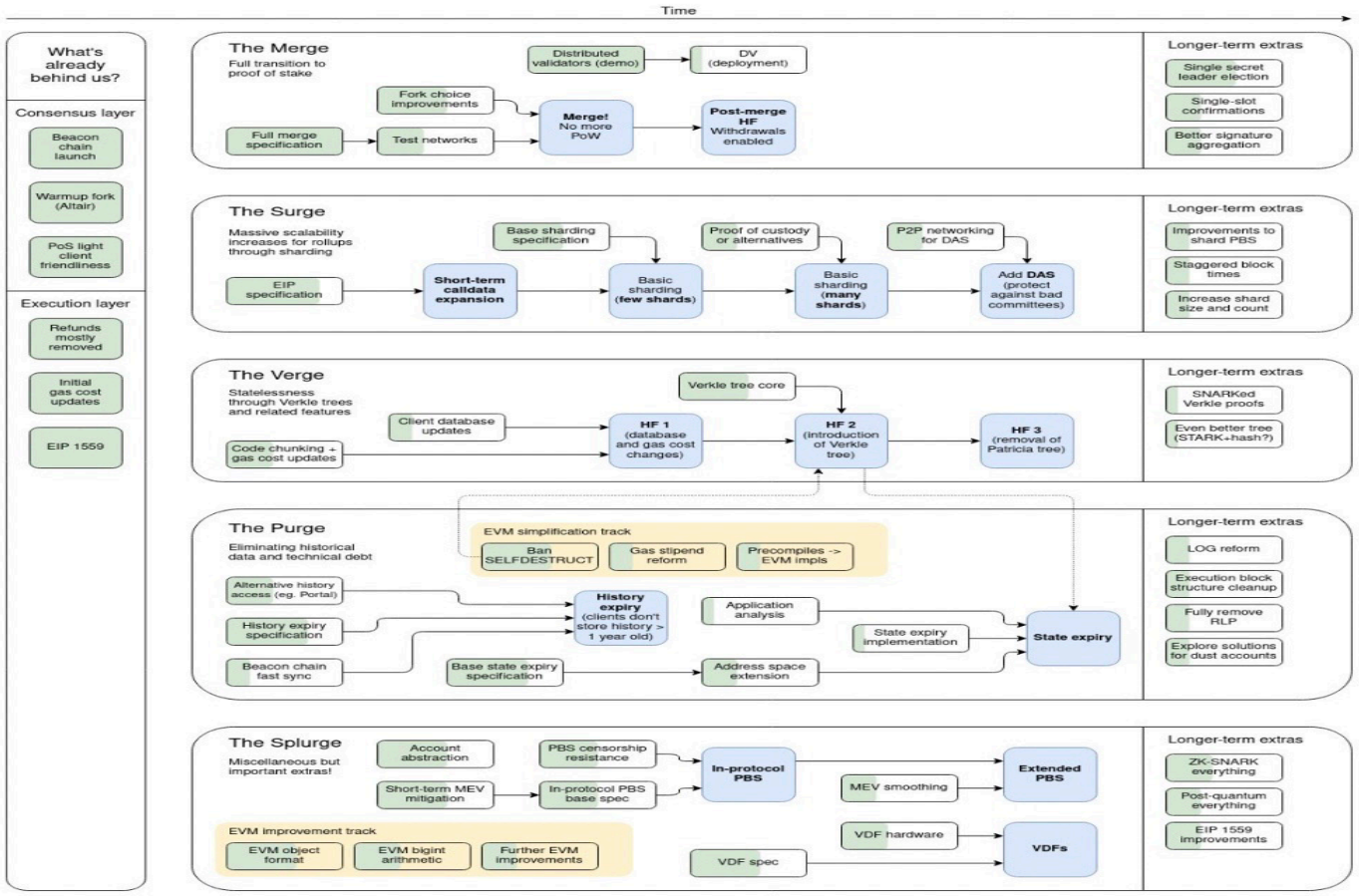
WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

The Merge represents the official switch to using the Beacon Chain as the engine of block production. Mining will no longer be the means of producing valid blocks. Instead, the proof-of-stake validators assume this role and will be responsible for processing the validity of all transactions and proposing blocks.

No history is lost. As Mainnet gets merged with the Beacon Chain, it will also merge the entire transactional history of Ethereum. For any users and or holders of assets on Ethereum this will (hopefully) happen seamlessly and we don't need to do anything.

Make no mistake, this is an incredibly ambitious technical feat to attempt. It has been likened to "replacing a plane's propellers with jet engines - in flight, with no turbulence."
Source: BowTiedBull

So now we know what the Merge is and when it's happening, it's important to know that the Merge is just the first step on the Ethereum roadmap. The roadmap to implement these features is broadly separated into five sequential initiatives. the Merge, the Surge, the Verge, the Purge, and the Splurge.



WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Merge - transition to Proof of Stake

- Surge - implement sharding
- Verge - statelessness via Verkle trees
- Purge - dealing with accumulating historical state and technical debt
- Splurge - "nice-to-have" features or "the fun stuff" as Vitalik Buterin calls it.

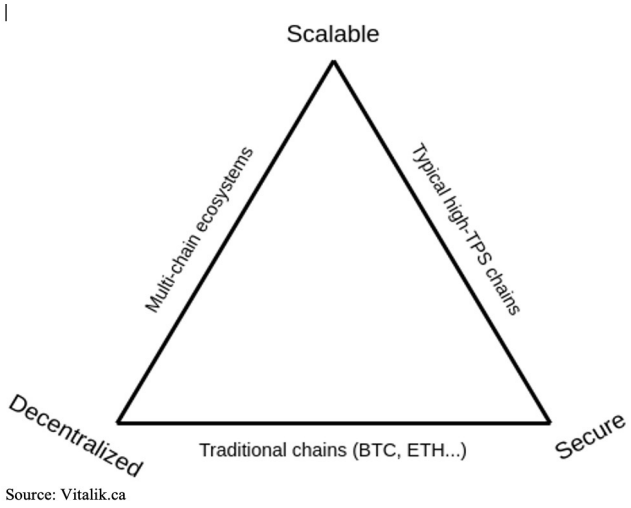
The ultimate goal for Ethereum is to be the settlement and data availability layer for anything and everything that needs to be trust less. This is a lofty goal and far more significant than trading tokens, badly drawn cartoon-like NFTs and even the more serious business of DeFi.

If Ethereum hopes to achieve its ultimate goal, it needs to remain secure and decentralized, but also improve its performance substantially. In its current state, it is architecturally bound in ways that prevent it from scaling to the necessary level.

For a blockchain to handle any substantial fraction of the world's transaction needs, it will require a transaction throughput capacity at least equal to a large credit card processor. Visa reportedly handles 65,000 transactions/second (TPS), a far cry from Ethereum's current cap of ~30 TPS.

A chain's TPS is fixed by how fast blocks are mined, and how many transactions can fit in a block. Blocks per second * transactions per block = transactions per second. It follows that the naive approach to increasing TPS is to make blocks come faster or allow more transactions per block. This is referred to as "tuning" since you're simply optimizing the blockchain's parameters to suit your goals.

The current generation of alternative Layer 1 chains which try to tune for speed run afoul of the blockchain trilemma. If you optimize for scalability by simple means (increasing block size, increasing block rate), you lose decentralization (nodes/miners have higher minimum software and hardware specifications and become less accessible due to the higher costs associated with running a node).



Source: Vitalik.ca

An example of this trade-off can be seen with the Solana blockchain. While it is very fast (has a high tps) the entire blockchain is controlled by just a few validators. These centralized parties can easily collude, be corrupted, or be shut down by governance authorities. Thus, the goal of being trust less can't be achieved.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Getting around the blockchain trilemma requires improving the underlying technology. There are many smart developers working on each aspect of the trilemma in the following manner:

- Decentralization - Shift from PoW to PoS, which reduces hardware requirements to participate in the network and removes supply chain risk from a reliance on powerful chips.
- Security - An extremely redundant and fault tolerant consensus mechanism under PoS
- Scalability - Rollups, sharding, and handling the storage problem

In addition to unveiling the Merge, Surge, Verge, Purge and Splurge at the annual Ethereum Community Conference (EthCC) in Paris on July 21, Ethereum co-founder Vitalik Buterin said that the Ethereum blockchain should be capable of handling 100,000 TPS at completion of this five-stage roadmap. The core technique to be used for achieving this goal is what is known as a rollup. A rollup is a Layer 2 chain which performs many transactions, bundles them together, and posts a corresponding single receipt to the Ethereum Mainnet. The proof itself is cryptographically verifiable so the L2 chain can't lie about what happened, and by posting the proof to Ethereum the rollup inherits the security properties of Ethereum (proof against history modification, data availability, high cost to attack, etc).

Hundreds of transactions can be rolled up into a single mainnet transaction, decoupling the rollup chain from Ethereum's own blockchain space constraints.

You can read more about rollups here.

By way of example: if Ethereum mainnet remains at 30 TPS, but all those 30 transactions are 100 TPS rollup chains posting their proofs, then the Ethereum ecosystem has suddenly become capable of 30 * 100 = 3000 TPS.

The next way of expanding TPS is via a process known as sharding. You can read a detailed article about sharding from Vitalik here:

In non-technical terms, sharding splits the entire load of a blockchain across multiple "shard" chains coordinated by a backbone or "beacon" chain. It's like the difference between a single lane road and a multi lane highway.

The key goal of sharding is to come as close as possible to replicating the most important security properties of traditional (non-sharded) blockchains but without the need for each node to personally verify each transaction.

Sharding uses some neat techniques to decouple the throughput of the blockchain from the validator workload. Without sharding, doubling the TPS means doubling the amount of validation work. With sharding, doubling the TPS increases the workload, but by a lesser amount.

That also means that the existing validator power can manage more TPS under a sharded scheme than a nonsharded scheme.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

The proposed sharding scheme has evolved significantly since the first proposals. Currently the implementation is focused on Danksharding, named after Ethereum researcher Dankrad Feist, who pioneered the design. This design focuses on shards as data availability engines, versus separate execution environments. Execution shards may come later if further throughput is needed but they are more technically complex.

The need for sharding implies the need for Proof of Stake. Proof of Work consensus can't maintain the desired security properties in a sharded system.

So now the number of TPS have been increased by expanding the base layer via sharding and using rollups to handle all the end user transactions. The next bottleneck is storage.

"Currently, running an Ethereum full node requires you to download and store the entire historical blockchain state. At present that state is over 500 GB, and speed requires you to use an SSD. A 1 TB SSD is around $100-$150 currently, which is still manageable.

But, as we increase TPS, we increase the rate we generate new things to store. It won't be long at all before you need 4 TB SSD or NVME drives to store the state, and at that point you're spending hundreds of dollars just on the storage portion of your hardware. Users in poor countries will be priced out. New nodes will take an unreasonable amount of time to sync". Source:

Participating in the network will become prohibitive for many users.

The solution to this limitation is described in the Verge stage of the Ethereum roadmap.

The verge will implement what Buterin calls "Verkle trees" (a type of mathematical proof) and "stateless clients." These technical upgrades will allow users to become network validators without having to store extensive amounts of data on their machines. In a proof-of-stake network, validators with locked-up or "staked" ETH confirm and verify transactions. In Buterin's view, the verge will be "great for decentralization."

Statelessness allows for a class of nodes that verify the chain without maintaining permanent storage. State expiry pushes out state that has not been recently accessed, forcing users to manually provide proofs to renew it.

These initiatives will allow regular users to run nodes, vs. requiring them to be power users with powerful hardware.

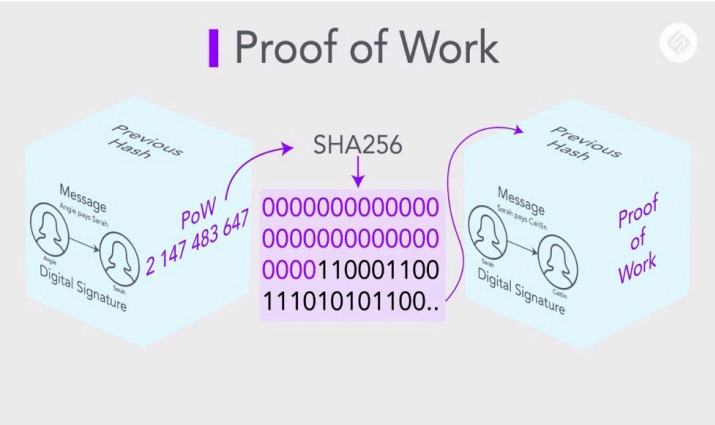
The above outline should give some understanding as to why these substantial technical upgrades are necessary to scale the Ethereum blockchain. Ethereum needs to scale to increase adoption. Rollups are key to scaling, and scaling rollups requires more base chain TPS. This TPS will be obtained via sharding, which necessitates the switch to Proof of Stake. The increase in TPS drives the need for statelessness and state expiry to manage the storage needs of the new chain.

Let's now look at The Merge itself and what's going to happen. For this next section we have sourced the excellent work of BowTiedBull's substack piece.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

"Recall that The Merge is the transition of the main Ethereum blockchain from a Proof of Work to Proof of Stake consensus model.

As reminder, in a Proof of Work blockchain, miners collect pending transactions into bundles and calculate the blockchain state that will occur when those transactions are processed. They then set about generating random numbers and hashing them with the block they have just produced, until they find a number with a hash result that has a certain number of leading zeroes.



Hash functions have mathematical properties which prevent shortcuts - the fastest way to solve them is to just keep trying numbers until you find one that works. This computational labour, costing both computational effort and electricity, is the "work" conducted under a PoW system.

The real-world cost of these inputs makes it economically unfeasible for malicious actors to produce blocks which do not adhere to the rules defined by the system. In this way all the miners in a chain can achieve consensus - an agreement on the state of the blockchain**.**

In a Proof of Stake blockchain, none of these costs are present. Instead of miners, you have validators. Security is achieved by requiring each validator to lock up a sum of money. If they behave in ways that are counter to the interests of the network (not responding, producing faulty blocks), their stake is slashed, and a portion is given to honest actors.

Proof of Stake blockchains by themselves are nothing new. Solana, Avalanche, Terra (RIP), and basically any "fast and cheap" Layer 1 alt-chain all use PoS consensus. The Merge has attracted so much attention because it's attempting to switch the consensus mechanism of the chain in-flight without disruption. This has not been done before and is a very ambitious technical goal.

The other primary innovation of Ethereum's PoS model is the new consensus algorithm, Gasper. A consensus algorithm is a set of rules each node uses to determine what the canonical blockchain state is. If two conflicting blocks are proposed, the consensus algorithm decides between them according to a particular set of pre-defined rules.

The consensus algorithm is defined at the blockchain protocol level. Barring bugs, all honest nodes should agree on the canonical state of the blockchain at any given time.

Without getting into the weeds of the new mechanism (which is a long article by itself), it combines two rulesets to simultaneously provide quick finality (once a block is included, very low chance it gets unincluded) and very strong fault tolerance (resistant to consensus loss, malicious validators, or validators going offline).

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

This combined set of properties is much stronger than competitor PoS algorithms like Tendermint.

Now for the fun part - the Merge itself.

The Beacon Chain, Ethereum's proof of stake chain, has been running in parallel to the PoW mainnet chain since Dec. 1st, 2020. During this time, it has been achieving consensus on its own state, and working out the kinks in the system.

When the Merge occurs, the Beacon Chain validators will be responsible for producing new blocks, replacing the current proof of work consensus system.

(At a technical level, there is a distinction between the execution layer (bundling and executing pending transactions to change the blockchain state) and the consensus layer (reaching agreement on which block is the current head of the blockchain). Ethereum clients are designed such that the consensus layer can be easily swapped out. For example, some Ethereum testnets use(d) Proof of Authority, and other testnets have already conducted their own Merge to Proof of Stake).

*The Ethereum chain (execution layer) will merge with the Beacon chain (consensus layer). To be a full node after the Merge, operators will have to run two separate clients - the execution client, and the consensus client. Normal users do not have to be aware of this distinction to use the chain. More here, here, and here.

All of Ethereum's testnets have successfully undergone the Merge already on their chain with the Goerli testnet successfully completing on August 12th. Mainnet "shadow forks", simulated merges based on a copy of the mainnet, have also been performed successfully. While there's obviously still a lot of things that can happen when the real deal Merge occurs, everything so far points to it working as designed.

Now, how will the Merge be executed? Is Vitalik going to ceremoniously hit "Enter" like a 2000's hackerman? Well, no.

First a little background. Each block in Proof of Work Ethereum has a "difficulty" associated with it. This difficulty is the number of leading zeroes on the proof hash needed for the block to be accepted. Higher number of leading zeroes → longer to mine the block, and vice versa. The difficulty is used to manage the time between blocks under varying network conditions. The chain also tracks the total difficulty - the cumulative sum of the difficulties of all the blocks that have come before a given block.

To kick off the Merge, the teams maintaining Ethereum clients (Geth, Nethermind, etc.) will release client versions which support the Merge. These clients will listen for an agreed-upon total difficulty value, called the Terminal Total Difficulty (TTD). Once a block which exceeds the TTD is mined, all Merge-supporting clients will automatically swap over to PoS. This ensures everyone switches at exactly the same time. More here.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

That said, it's important to realize that the Merge is almost guaranteed to cause a fork. Any miner happening to run outdated software, or who does not philosophically agree with the Merge and chooses to remain with PoW, will reject the PoS fork and continue to produce blocks on the old chain. We may end up with ETH Classic 2: Electric Boogaloo.

To combat this, we have the idea of the ice age and the difficulty bomb.

The difficulty bomb is a feature already implemented in the Ethereum protocol - after a particular block, the bomb will go off, and the difficulty of mining a new block will start becoming exponentially harder. Eventually, the difficulty will become so high that mining new blocks becomes unfeasible, and block production will grind to a halt - the ice age.

The bomb ensures that either the old PoW chain will die off, or an active sub-community will form around it similar to Ethereum Classic (ETC). PoW miners can decide to hard fork the bomb out of their clients and continue the PoW chain, but to do that they will have to coordinate a hard fork at the social layer and do the development work to disable the bomb.

Either way, the goal will be achieved. The PoW chain will not meander on as a headless, zombified entity. It will either die decisively or be reborn as a new entity.

Clearing up some misconceptions about The Merge

It's worth highlighting two commonly held expectations of The Merge which won't happen.

The first is that The Merge will reduce gas fees. The Merge is a change of consensus mechanism, not an expansion of network capacity, and will not result in lower gas fees.

"Gas fees are a product of network demand relative to the capacity of the network. The Merge deprecates the use of proof-of-work, transitioning to proof-of-stake for consensus, but does not significantly change any parameters that directly influence network capacity or throughput.

With a rollup-centric roadmap, efforts are being focused on scaling user activity at layer 2, while enabling layer 1 Main net as a secure decentralized settlement layer optimized for rollup data storage to help make rollup transactions exponentially cheaper. The transition to proof-of-stake is a critical precursor to realizing this."

Source: here

The second misconception is that transaction speed will be faster on Ethereum after The Merge. "Though some slight changes exist, transaction speed will mostly remain the same on layer 1."

Source: here

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

A Taste of the Future

Let's tie it all back to the vision.

At the end of the Ethereum upgrade roadmap, it will stand as the central chain in a constellation of application rollups, powering more transactions than a major credit card provider. You will likely never send a transaction on the mainnet except maybe to interact with legacy protocols, as that space will be predominantly used for rollups and other backend infrastructure.

You will be able to run a node and participate in securing the network from a regular consumer laptop. Fees will be low, and transactions will be fast. The increased data storage capacity of the blockchain will unlock additional use cases which are currently unfeasible.

That's assuming, of course, that everything goes as planned. There's still a lot of hard engineering work to be done, but if the Merge goes successfully that will be a very bullish indicator for the success of the rest of the roadmap."

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

DISCLAIMER

Disclaimer

Fort Canning Asset Management Pty Ltd (CAR) is a corporate authorised representative of Boutique Capital Pty Ltd (BCPL) AFSL 508011, CAR Number 1284461. CAR is an investment manager of the fund(s) described elsewhere in this document, or in other documentation (Fund).

To the extent to which this document contains advice it is general advice only and has been prepared by the CAR for individuals identified as wholesale investors for the purposes of providing a financial product or financial service, under Section 761G or Section 761GA of the Corporations Act 2001 (Cth).

The information herein is presented in summary form and is therefore subject to qualification and further explanation. The information in this document is not intended to be relied upon as advice to investors or potential investors and has been prepared without taking into account personal investment objectives, financial circumstances or particular needs. Recipients of this document are advised to consult their own professional advisers about legal, tax, financial or other matters relevant to the suitability of this information.

The investment summarised in this document is subject to known and unknown risks, some of which are beyond the control of CAR and their directors, employees, advisers or agents. CAR does not guarantee any particular rate of return or the performance of the Fund, nor does CAR and its directors personally guarantee the repayment of capital or any particular tax treatment. Past performance is not indicative of future performance.

The materials contained herein represent a general summary of CAR's current portfolio construction approach. CAR is not constrained with respect to any investment decision making methodologies and may vary from them materially at its sole discretion and without prior notice to investors. Depending on market conditions and trends , CAR may pursue other objectives or strategies considered appropriate and in the best interest of portfolio performance.

There are risks involved in investing in the CAR's strategy. All investments carry some level of risk, and there is typically a direct relationship between risk and return. We describe what steps we take to mitigate risk (where possible) in the Fund's Information Memorandum. It is important to note that despite taking such steps, the CAR cannot mitigate risk completely.

This document was prepared as a private communication to clients and is not intended for public circulation or publication or for the use of any third party, without the approval of CAR. Whilst this report is based on information from sources which CAR considers reliable, its accuracy and completeness cannot be guaranteed. Data is not necessarily audited or independently verified. Any opinions reflect CAR's judgment at this date and are subject to change. CAR has no obligation to provide revised assessments in the event of changed circumstances. To the extent permitted by law, BCPL, CAR and their directors and employees do not accept any liability for the results of any actions taken or not taken on the basis of information in this report, or for any negligent misstatements, errors or omissions.

This Document is informational purposes only and is not a solicitation for units in the Fund. Application for units in the Fund can only be made via the Fund's Information Memorandum and Application Form.