# AweCoin

## The Whitepaper

# Important Notice

PLEASE READ THIS SECTION CAREFULLY

None of the information in this whitepaper (“Whitepaper”) has been filed with, reviewed by, or approved by any regulatory authority. This Whitepaper and any part thereof may not be distributed or otherwise disseminated in any jurisdiction where the distribution or dissemination may be prohibited. No part of this Whitepaper is to be reproduced, distributed or disseminated without including this section titled “Important Notice”. If you are in doubt as to the action you should take, please consult your financial, legal, tax, technical or other professional advisors.

# General Information

This Whitepaper describes the token sale (“Token Sale”) for the sale of “AweCoin” (“AWE”) and the functionality of AWE. This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for an investment in securities in any jurisdiction. This Whitepaper also does not constitute any form of advice (whether financial, legal, tax or otherwise) and should not be relied upon in connection with any decision to purchase AWE. This Whitepaper is prepared based on the views and plans of AweCoin as of the date set out on the cover page of this Whitepaper. AweCoin reserves the sole and absolute discretion to revise any part of this Whitepaper from time to time by posting the revised Whitepaper on https://awecoin.me/ (“Website”). Such updated Whitepaper shall become effective immediately from the time of posting.

# Token Sale

The purpose of the Token Sale is to raise funds to develop, market and operate AweCoin, as generally described in this Whitepaper.

Unless otherwise agreed by AweCoin in writing, the sale of all Tokens by AweCoin during the Token Sale shall be governed exclusively by the Token Sale Terms and Conditions on the Website. No person is bound to purchase any AWE, and no purchase or payment would be accepted, on the basis of this Whitepaper. In the event of any conflict or inconsistency between the Token Sale Terms and Conditions, this Whitepaper and any other document, the Token Sale Terms and Conditions shall prevail to the extent of the conflict or inconsistency unless otherwise specified in writing by AweCoin.

As detailed in the Token Sale Terms and Conditions, the Tokens carry no rights other than a limited right of use within the ecosystem of AWE.

# Risks

Participation in the Token Sale and purchase of AWE carry with it significant risks. If any such risk materialises, it could have a severe negative impact on the Token Sale, AweCoin, AWE, and AweCoin. Accordingly, please carefully review and assess the terms applicable to the Tokens and the Token Sale, as well as the risks involved (including those listed in the Token Sale Terms and Conditions) before deciding whether or not to participate in the Token Sale.

# Disclaimer

The contents of this Whitepaper is of a descriptive nature for information only, and is not binding. Such information has been compiled by AweCoin from sources believed to be reliable. Some of this information may be forward looking in nature and based on certain assumptions. All statements other than statements of historical facts included in this Whitepaper, including, without limitation, statements regarding business strategy and plans, estimates of returns or performance, and objectives for future operations, are forward looking statements. In addition, forward looking statements can generally be identified by the use of forward looking terminology such as “may”, “will”, “should”, “expect”, “anticipate”, “estimate”, “intend”, or “believe”, their respective negatives and other comparable terminology.

Nothing in this Whitepaper is a representation, warranty or undertaking of the accuracy or fulfilment of any particular matter stated in the Whitepaper at any given point in the future, and AweCoin specifically disclaims any representation or warranty that it will execute any action or guarantee specific results regarding any matters described herein this Whitepaper. The information presented in this Whitepaper is for reference only and is not legally binding on AweCoin or any other parties.

1

# AweCoin

## Executive Summary

# Executive Summary

## What is AWE?

The intent of AweCoin is to create a protocol for building decentralized applications, providing a different set of trade-offs that we believe will be very useful for a large class of decentralized applications, with particular emphasis on situations where rapid development time, security for small and rarely used applications, and the ability of different applications to very efficiently interact, are important.

AweCoin does this by building on top of the Ethereum network, which is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions.

Smart contracts, cryptographic "boxes" that contain value and only unlock it if certain conditions are met, can also be built on top of the platform, with vastly more power than that offered by Bitcoin scripting because of the added powers of Turing-completeness, value-awareness, blockchain-awareness and state.

## Design Philosophy

### Simplicity

AweCoin is as simple as possible. An average programmer should ideally be able to follow and implement the entire specification, so as to fully realize the unprecedented democratizing potential tha cryptocurrency brings and further the vision of AweCoin as a protocol that is open to all. Any optimization which adds complexity should not be included unless that optimization provides very substantial benefit.

## Censorship-resistance

The protocol discourages attempts to actively restrict or prevent specific categories of usage. All regulatory mechanisms in the protocol are designed to directly regulate the harm and not attempt to oppose specific undesirable applications. A programmer can even run an infinite loop script with AweCoin for as long as they are willing to keep paying the per-computational-step transaction fee.

## Modularity

The parts of the AweCoin protocol are designed to be as modular and separable as possible. Over the course of development, our goal is to create a program where if one was to make a small protocol modification in one place, the application stack would continue to function without any further modification. This is so that if a desirable feature is thought of in the future, it can be included as a separate smart contract for AweCoin. AweCoin’s development aims to benefit the entire cryptocurrency ecosystem, not just itself.

## Universality

A fundamental part of AweCoin’s design philosophy is that has the potential for unlimited features. AweCoin uses Ethereum’s internal Turing-complete scripting language, which a programmer can use to construct any smart contract or transaction type that can be mathematically defined. Want to invent your own financial derivative? With AweCoin, you can. Want to set up a full-scale Daemon? Nothing is stopping you with AweCoin at your fingertips.

2

# AweCoin

## Applications

# Use Cases and Applications

## Replace Finance

There’s more to finance than currency. AweCoin’s main use case is for financial applications, providing users with more powerful ways of managing and entering into contracts using their money. This includes sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and ultimately even some classes of full-scale employment contracts.

## Pay Ethereum Transaction Fees in AWE

AweCoin essentially features an implementation of the "banking system" state transition function. Theoretically, AweCoin can potentially include another important feature that on-chain Bitcoin-based meta-currencies lack: the ability to pay transaction fees directly in AWE. The way this would be implemented is that the contract would maintain an ether balance with which it would refund ether used to pay fees to the sender, and it would refill this balance by collecting the internal currency units that it takes in fees and reselling them in a constant running auction. Users would thus need to "activate" their accounts with ether, but once the ether is there it would be reusable because the contract would refund it each time.

## Financial Derivatives

Financial derivatives are the most common application of a "smart contract", and one of the simplest to implement in code. The main challenge in implementing financial contracts is that the majority of them require reference to an external price ticker; for example, a very desirable application is a smart contract that hedges against the volatility of AweCoin (or another cryptocurrency) with respect to the US dollar, but doing this requires the contract to know what the value of AWE/USD is. The simplest way to do this is through a "data feed" contract maintained by a specific party (eg. NASDAQ) designed so that that party has the ability to update the contract as needed, and providing an interface that

allows other contracts to send a message to that contract and get back a response that provides the price. In this example, NASDAQ would be the Oracle that provides the data feed.

In practice, however, oracles are not always trustworthy, and in some cases the banking infrastructure is too weak, or too hostile, for such services to exist. Financial derivatives provide an alternative. Here, instead of a single issuer providing the funds to back up an asset, a decentralized market of speculators, betting that the price of a cryptographic reference asset (eg. AWE) will go up, plays that role. Unlike issuers, speculators have no option to default on their side of the bargain because the hedging contract holds their funds in escrow. Note that this approach is not fully decentralized, because a trusted source is still needed to provide the price ticker, although arguably even still this is a massive improvement in terms of reducing infrastructure requirements (unlike being an issuer, issuing a price feed requires no licenses and can likely be categorized as free speech) and reducing the potential for fraud.

## Identity / Reputation Systems

The earliest alternative cryptocurrency of all, Namecoin, attempted to use a Bitcoin-like blockchain to provide a name registration system, where users can register their names in a public database alongside other data. The major cited use case is for a DNS system, mapping domain names like "awecoin.me" to an IP address. Other use cases include email authentication and potentially more advanced reputation systems.

All that’s required is a database inside the Ethereum network that can be added to, but not modified or removed from. Anyone can register a name with some value, and that registration then sticks forever. A more sophisticated name registration contract will also have a "function clause" allowing other contracts to query it, as well as a mechanism for the "owner" (ie. the first registerer) of a name to change the data or transfer ownership. One can even add reputation and web-of-trust functionality on top.

## Decentralized File Storage

The key underpinning piece of decentralized file storage would be a "Decentralized Cloud Contract". This contract works as follows: First, one splits the desired data up into blocks, encrypting each block for privacy, and builds a Merkle tree out of it. One then makes a contract with the rule that, every N blocks, the contract would pick a random index in the Merkle tree (using the previous block hash, accessible from contract code, as a source of entropy), and give X ether to the first entity to supply a transaction with a simplified payment verification-like proof of ownership of the block at that particular index in the tree. When a user wants to re-download their file, they can use a micropayment channel protocol to recover the file; the most fee-efficient approach is for the payer not to publish the transaction until the end, instead replacing the transaction with a slightly more lucrative one with the same nonce after every x kilobytes.

An important feature of the protocol is that, although it may seem like one is trusting many random nodes not to decide to forget the file, one can reduce that risk down to near-zero by splitting the file into many pieces via secret sharing, and watching the contracts to see each piece is still in some node's possession. If a contract is still paying out money, that provides a cryptographic proof that someone out there is still storing the file.

## Cloud Computing

The EVM technology can also be used to create a verifiable computing environment, allowing users to ask others to carry out computations and then optionally ask for proofs that computations at certain randomly selected checkpoints were done correctly. This allows for the creation of a cloud computing market where any user can participate with their desktop, laptop or specialized server, and spot-checking together with security deposits can be used to ensure that the system is trustworthy (ie. nodes cannot profitably cheat). Although such a system may not be suitable for all tasks; tasks that require a high level of inter-process communication, for example, cannot easily be done on a large cloud of nodes. Other tasks, however, are much easier to parallelize; projects like SETI@home, folding@home and genetic algorithms can easily be implemented on top of such a platform.

## Decentralized Autonomous Organizations (DAOs)

The general concept of a "decentralized autonomous organization" is that of a virtual entity that has a certain set of members or shareholders which, with maybe a 2/3 majority, have the right to spend the entity's funds and modify its code. The members would collectively decide on how the organization should allocate its funds. Methods for allocating a DAO's funds could range from bounties, salaries to even more exotic mechanisms such as an internal currency to reward work. This essentially replicates the legal trappings of a traditional company or nonprofit but using only cryptographic blockchain technology for enforcement. So far much of the talk around DAOs has been around the "capitalist" model of a "decentralized autonomous corporation" (DAC) with dividend-receiving shareholders and tradable shares; an alternative, perhaps described as a "decentralized autonomous community", would have all members have an equal share in the decision making and require over 2/3 of existing members to agree to add or remove a member. The requirement that one person can only have one membership would then need to be enforced collectively by the group.

An alternative model is for a decentralized corporation, where any account can have zero or more shares, and two thirds of the shares are required to make a decision. A complete skeleton would involve asset management functionality, the ability to make an offer to buy or sell shares, and the ability to accept offers. Delegation would also exist Liquid Democracy-style, generalizing the concept of a "board of directors".

## Savings Wallets

Suppose that Alice wants to keep her funds safe, but is worried that she will lose or someone will hack her private key. She puts AWE into a contract with Bob, who acts as a bank.

- Alice alone can withdraw a maximum of 1% of the funds per day.
- Bob alone can withdraw a maximum of 1% of the funds per day, but Alice has the ability to make a transaction with her key shutting off this ability.
- Alice and Bob together can withdraw anything.

Normally, 1% per day is enough for Alice, and if Alice wants to withdraw more she can contact Bob for help. If Alice's key gets hacked, she runs to Bob to move the funds to a new contract. If she loses her

key, Bob will get the funds out eventually. If Bob turns out to be malicious, then she can turn off his ability to withdraw.

## Smarter Multi-signature Escrow

Bitcoin allows multi-signature transaction contracts where, for example, three out of a given five keys can spend the funds. AweCoin allows for more granularity than bitcoin; for example, four out of five can spend everything, three out of five can spend up to 10% per day, and two out of five can spend up to 0.5% per day. Additionally, AweCoin multi-signature is asynchronous - two parties can register their signatures on the blockchain at different times and the last signature will automatically send the transaction.

## Prediction Markets

Prediction markets are exchange-traded markets created for the purpose of trading the outcome of events. The market prices can indicate what the crowd thinks the probability of the event is. A prediction market contract trades between 0 and 100%. It is a binary option that will expire at the price of 0 or 100%.

Provided an oracle or SchellingCoin, prediction markets are also easy to make, and prediction markets together with SchellingCoin may prove to be the first mainstream application of “Futarchy” as a governance protocol for decentralized organizations.

## Peer-to-Peer Gambling / Lottery

Any number of peer-to-peer gambling protocols, such as Frank Stajano and Richard Clayton's Cyberdice, can be implemented on the Ethereum blockchain. The simplest gambling protocol is simply a contract for difference on the next block hash, and more advanced protocols can be built up from there, creating gambling services with near-zero fees that have no ability to cheat.

It is also possible to create a lottery where players contribute to a prize pool and the winner is randomly chosen using a future block hash as the entropy source.

3

# AweCoin

## Base Layer

# Ethereum as a Base-Layer

## Why Ethereum?

We chose Ethereum as AweCoin’s base layer for several reasons:

- It does transactions at a lower cost than bitcoin.
- It prevents inflation bugs as the code is hard-written into the immutable contract.
- It has a higher throughput than bitcoin.

## Scalability Concerns with Ethereum aren’t a Problem!

One common concern about Ethereum is the issue of scalability. Like Bitcoin, Ethereum suffers from the flaw that every transaction needs to be processed by every node in the network. With Bitcoin, the size of the current blockchain rests at about 15 GB, growing by about 1 MB per hour. If the Bitcoin network were to process Visa's 2000 transactions per second, it would grow by 1 MB per three seconds (1 GB per hour, 8 TB per year). Ethereum is likely to suffer a similar growth pattern, worsened by the fact that there will be many applications on top of the Ethereum blockchain instead of just a currency as is the case with Bitcoin, but ameliorated by the fact that Ethereum full nodes need to store just the state instead of the entire blockchain history.

Thanks to the modularity of AweCoin’s smart contract, it is possible to migrate the token, along with a snapshot of all the existing token holders. This allows the entire AweCoin system to be rebuilt easily on top of another blockchain virtual machine, should Ethereum ever be displaced in the market.

This makes the scalability of Ethereum’s network less of a problem as AweCoin can survive independently from Ethereum, should the worst ever happen.

4

# AweCoin

# Conclusion

# Conclusion

AweCoin was originally conceived as an upgraded version of a cryptocurrency, providing advanced features such as on-blockchain escrow, withdrawal limits, financial contracts, gambling markets and the like via a highly generalized programming language. The existence of a Turing-complete programming language means that arbitrary contracts can theoretically be created for any transaction type or application. What is more interesting about AweCoin, however, is that it moves far beyond just currency. Protocols around decentralized file storage, decentralized computation and decentralized prediction markets, among dozens of other such concepts, have the potential to substantially increase the efficiency of the computational industry, and provide a massive boost to other peer-to-peer protocols by adding for the first time an economic layer. Finally, there is also a substantial array of applications that have nothing to do with money at all.

The concept of an arbitrary state transition function as implemented by AweCoin provides for a platform with unique potential; rather than being a closed-ended, single-purpose protocol intended for a specific array of applications in data storage, gambling or finance, AweCoin is open-ended by design, and we believe that it is extremely well-suited to serving as a foundational layer for a very large number of both financial and non-financial protocols in the years to come.

Bitcoin was just designed to replace currency. AweCoin targets the whole of finance which gives it orders of magnitude more potential value.

## It truly is a Next Generation, General-Purpose Cryptocurrency!