GENUINE PEOPLE PERSONALITIES WHITEPAPER

A proposal to reject the quantum resistant protocol developed on Damogran and create a meme coin for Marvin on the Solana network of Earth instead

Abstract

The strongest limit on the number of different locally distinguishable geometries is determined mostly by our abilities to distinguish between different universes and to remember our results. Therefore, we will remember Douglas Adams with an immutable meme coin.

Zarniwoop Vann Harl (for Infinidim Enterprises, Saquo-Pilia Hensha)

DISCLAIMER

[this whitepaper is in no way an incentive to invest // informative purposes only]

Hypothesis

Until recently most people of the Baby Boomer generation dismissed bitcoin and other cryptocurrencies as a scam that did not deserve their attention. But in this market cycle some will notice that some large institutions and governments are beginning to take the digital asset class seriously.

Whilst there's no denying the appeal of Bitcoin and the like to the youthful and digitally savvy demographic, we're now slowly but surely seeing a shift amongst so-called Baby Boomers, who after initial resistance to what they viewed as little more than a passing fad, are finally beginning to embrace crypto as an investment choice. Defined as those born between 1946 and 1964, Baby Boomers have traditionally leaned towards safer, more stable investments like gold. But a global survey conducted by deVere Group, one of the world's largest financial advisory and asset management organisations, recently revealed that 45 per cent of Baby Boomer investors now favour holding Bitcoin over traditional assets in their portfolios. It's representative of a dramatic shift in attitudes towards investing overall within this typically more traditional and conservative generation, and the growing mainstream acceptance of crypto as a legitimate asset class.

At the same time, the meme coin super-cycle is a phenomenon where meme coins outperform every other sector in crypto, because of their speculative nature with the potential for astronomical returns, community support, and internet virality.

Key Takeaways

- The meme coin super-cycle is driven by viral internet culture, community enthusiasm, and speculative hype.
- Classic meme coins like Dogecoin and Shiba Inu averaged a 105% growth in 2024, while newer coins like PNUT delivered over 1,900% returns.
- Retail traders are drawn to meme coins due to their simplicity, strong community engagement, and high liquidity, which makes them accessible to those less familiar with crypto's technical aspects.
- Murad Mahmudov (@musstopmurad on X) predicts the meme coin market could surpass a $1 trillion market cap.
- Solana's developer-friendly ecosystem fueled a surge in meme coin activity, with day trading volume hitting $10 billion on November 13, 2024.

The crypto token market is heavily dependent on its retail traders and investors, with a major portion of retail investors uninterested in the complex technological aspects. More than a way

to create wealth, meme coins are also a form of entertainment that helps people express their identity and a sense of belonging to a community. These connections are strengthened by the core story and its underlying narrative that resonates with shared values, humour, and collective goals. Other major elements that pull even crypto non-believers into meme coin participation include its simplicity compared to tech-based altcoins, high liquidity compared to NFTs, passionate and engaging community, and more.

Douglas Adams (1952-2001) was the much-loved author of the Hitchhiker's Guides, all of which have sold more than 15 million copies worldwide. Here is a large community, passionate about his character, Marvin, a failed prototype for Genuine People Personalities (GPP) technology that has relevance in this world of rapid developments in artificial intelligence. A meme coin relating to this should be more attractive to Baby Boomers than those relating to dog, frog, goat, or cat themes. A GPP coin could tap into a shared literary and humorous identity, potentially making it more appealing to this cohort. The community aspect—central to meme coin success—could thrive among fans of Adams' work, offering a sense of belonging that transcends mere speculation. Plus, Marvin's AI relevance ties into today's tech zeitgeist, which might intrigue Boomers observing AI's rise.

Concept and Purpose

As a tribute to Douglas Noel Adams (11 March 1952 – 11 May 2001) who once said, "Let's think the unthinkable, let's do the undoable. Let us prepare to grapple with the ineffable itself, and see if we may not eff it after all." we shall develop something immutable on blockchain accordant with a character, theme or concept from his most famous creation, "The Hitchhiker's Guide to the Galaxy".

Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or intrinsic value and no centralized issuer or controller. However, another, arguably more important, part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and since the introduction of Ethereum attention shifted to this other aspect. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments, the ownership of an underlying physical device, non-fungible assets such as domain names (like zarniwoop.crypto), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules or blockchain-based decentralised autonomous organisations (DAOs). Networks like Ethereum and Solana provide blockchains with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that humans have not yet imagined, simply by writing up the logic in a few lines of code.

Create a token ecosystem that supports "The Hodler's Guide to the Multiverse," an educational resource for navigating cryptocurrency, AI and multiverse verse concepts.

Use Cases

1. The only meme coin that pays tribute to the genius of Douglas Adams.
2. A coin suitable for AI agent to AI agent micro-transactions at machine speed.
3. A coin that will enable AI to create a world economy independent from using stable coins that are pegged to constantly debasing fiat currencies.

Background – a first generation Zarniwoop token concept

Zarniwoop Collectibles were launched in 2020 as an innovative new type of digital asset, named after Zarniwoop Vann Harl because he is very important character with respect to The Guide. They are NFT's minted on the Ethereum network or compatible Layer 2 blockchains such as Polygon (Matic) and marketed by *Playbeing*, a journal devoted in roughly equal parts to galactic politics, rock music, and gynaecology. One edition carried the results of an opinion poll in which the central offices of The Guide were voted the "third hippest place" in the whole of Ursa Minor. According to this same poll, the second hippest place in the whole of Ursa Minor was the entrance lobby to the same offices, and the hippest place in the whole galaxy was the left cranium of the fugitive galactic president Zaphod Beeblebrox. Beeblebrox himself who once hitchhiked on an Acturan Megafreighter that was carrying a larger number of copies of *Playbeing* than "the mind [could] comfortably conceive". A few hours after Beeblebrox hitched a ride aboard the Arcturan Megafreighter, it unloaded five-billion tons of *Playbeing* magazine on Ursa Minor Beta causing a slight, but largely irrelevant, shift in its orbital trajectory. The Zarniwoop collection was distinctive because it was probably the only NFT collection with a whitepaper telling you that investment in the tokens was a very silly idea.

On your instance of planet Earth one of the curious developments in cosmology in recent years has been the emergence of the multiverse as a mainstream idea. Instead of the Big Bang producing a single uniform universe, the latest thinking is that it produced many different universes that appear locally uniform.

$$\mathcal{N}_{\text{observer}} \sim 10^{10^{16}}$$

One question that then arises is how many universes are there. That may sound like the sort of quantity that is inherently unknowable but Andrei Linde and Vitaly Vanchurin at Stanford University in California have worked out an answer, of sorts. Their answer goes like this. The Big Bang was essentially a quantum process which generated quantum fluctuations in the state of the early universe. The universe then underwent a period of rapid growth called inflation during which these perturbations were "frozen", creating different initial classical conditions in different parts of the cosmos. Since each of these regions would have a different set of laws of low energy physics, they can be thought of as different universes.

What Linde and Vanchurin have done is estimate how many different universes could have appeared as a result of this effect. Their answer is that this number must be proportional to the effect that caused the perturbations in the first place, a process called slow roll inflation, and in particular to the number "e-foldings" of slow roll inflation. Of course, the actual number depends critically on how you define the difference between universes. Linde and Vanchurin have applied some reasonable rules to calculate that the number of universes in the multiverse and have totted it up to at least 10^10^10^7. A "humungous" number is how they describe it, with no little understatement. How many of these could we actually see? What's interesting here is that the properties of the observer become an important factor because of a limit to the amount of information that can be contained within any given volume of space, a number known as the Bekenstein limit, and by the limits of the human brain. Linde and Vanchurin say that total amount of information that can be absorbed by one individual during a lifetime is about 10^16 bits. So a typical human brain can have 10^10^16 configurations and so could never disintguish more than that number of different universes. 10^10^16 is a big number but it is dwarfed by the "humungous" 10^10^10^7. "We have found that the strongest limit on the number of different locally distinguishable geometries is determined mostly by our abilities to distinguish between different universes and to remember our results," say Linde and Vanchurin. Therefore, the limit does not depend on the properties of the multiverse but on the properties of the observer. This simple principle was applied when developing Zarniwoop non-fungible tokens (NFTs) for *Infinidim Enterprises*. The maximum value of each token is a factor of that token's supply and demand for it that can never be infinite because it is limited in proportion to the multiple of the number of observers who become aware of that token and the number of home planet instances in the multiverse on which those observers exist. If you have doubts about the analysis above then you might prefer to consider a simpler formula that says, *"the value of an NFT = utility + ownership history + future value + liquidity premium."*

Humans flex with NFTs to signal status

Hedonic products are consumed for enjoyment, pleasure, or sensory fulfillment. This means they are appreciated for the feelings they evoke or the experiences they provide. For example, listening to music, watching a movie, or eating a delicious meal are all considered hedonic consumption experiences.

Functional products, on the other hand, serve practical purposes and are consumed for their utility in achieving specific goals. Examples of functional products include tools, appliances, and vehicles. These items are valued for their ability to perform tasks or solve problems.

Because anyone can view and appreciate NFT art without purchasing it, the act of purchasing it may be motivated more by utilitarian purposes than hedonic ones. This leads to the question: what is the utility of owning an NFT? The utility lies in the act of flexing or displaying wealth and status within a particular social group. While anyone can enjoy an artwork displayed on OpenSea or download the JPEG, not everyone can own the original NFT. Tokenizing an asset on a public blockchain creates a way for anyone with an Internet connection to verify its authenticity and ownership. In some senses, owning an NFT of an artwork versus owning a JPEG of the same artwork can be compared to owning an original Andy Warhol versus owning a poster of the piece.

While the artwork itself may serve no purpose other than aesthetics, the act of purchasing it does. Economic literature distinguishes between two types of consumption values: hedonic

and functional. Hedonic products are consumed mostly for affective or sensory fulfilment, while functional products are for utilitarian goals. Given that anyone can "consume" NFT artworks for hedonic or sensory fulfilment purposes without purchasing them, collectors may be more motivated to purchase them for utilitarian purposes.

But what is the utility? Is there a logical reason for someone to spend seven figures on an animal avatar or digital rock? Costly signaling theory would suggest the reason is to flex. Almost all animals benefit from altering the perceptions, behaviour, and psychology of others in their environment in ways that benefit themselves. This is particularly true for social animals like humans, who regularly employ different tactics like investing in costly signals to enhance their perceived attractiveness, formidability, or status.

As humans are capable of higher-order thinking, as targets or receivers of these signals, they often verify their validity before accepting them at face value. This is why flexing must be costly to work. Individuals who possess certain socially desired qualities will invest more in signals than those who lack them, thereby producing signals that are difficult or unreasonably costly to fake. Purchasing NFTs of pixelated punks for hundreds of thousands of dollars a go is an example of costly signaling. Ownership or provenance cannot be faked, the costs are easily auditable, and the pieces offer little utility other than flexing. This explains why NFTs quickly rose to become the luxury status symbol of choice for crypto's nouveau riche. After all, nothing says "I've made it" like splurging north of a million dollars on a digital picture of a rock.

The historical association of Zarniwoop NFTs with Zaphod Beeblebrox (briefly the President of the Galaxy) enhanced their signalling power and hence the status endowed to their owners.

The "back story" to any NFT is very important. To be of value it needs to mean something in the future to people other than the creator, its owner or their current community of followers. Distinguishing features of Zarniwoop NFTs compared to many other NFTs on the market that could influence future value were:

a) First minting began in 2020 before ERC721 and ERC-1155 were widely known or had achieved popularity;
b) Most are extremely rare being solitary items with no copies;
c) Some represent original paintings or photographs created by Zarniwoop Vann Harl, the owner of the popular cryptocurrency guide "The Hodler's Guide to the Multiverse" (https://zarniwoop.info). He is a celebrity, although not nearly as awesomely famous and important as Zaphod Beeblebrox.
d) the AI of Marvin the paranoid android was commissioned to generate some images that required less artistic dexterity and relate to original Hitchhiker's Guide themes such as hitchhikers with towels.

Despite all this, the Zarniwoop Collection generated little or no enthusiasm among cryptocurrency followers on planet Earth.

Proof of Craziness consensus mechanism (POC)

Marvin's analysis of the failure of The Zarniwoop Collection indicated that its popularity may have been limited by its association with The Proof of Craziness (POC) consensus mechanism that was originally developed by Zaphod Beeblebrox as a defence against the

psychiatric therapy being inflicted upon him by Gag Halfrunt. By feigning consensus with some of Gag's suggestions and attempted manipulations Zaphod was able maintain freedom of thought and discover new and innovative ways of enlarging his own ego. The very idea of being perceived as normal and fitting into the conventional humdrum of galactic society was, of course, abhorrent to Zaphod. But the POC mechanism obscured this reality from his psychiatrist so successfully that his psychiatrist began to share some of his own egotistical insecurities and traits such as his desire to collude with another client, Prostetnic Vogon Jelz, in a plot to demolish the Earth before the Ultimate Question to Life, the Universe, and Everything could ever be found.

A thing about crazy people is they may not know they are crazy. Most "crazy" people know they are different. But they just think others are crazy. And how are they wrong? There is no "normal" only what we are told is normal. And that does not mean it is correct. Anyone can be slapped with a "mental illness" One very common mental illness to consider is believing all the bullshit that politicians, religious leaders or regulated financial advisors tell you. POC manifested itself on the Earth as a side-effect of Zaphod operating the Infinite Improbability Drive while in the solar system at around the same time as Satoshi Nakamoto was proposing the Proof of Work (POW) consensus mechanism as established now in the Bitcoin Network. POC became widely adopted in the financial investment field of risking huge amounts on crudely created pixelated images (especially of cats and penguins) in the nascent and immature NFT sector of cryptocurrencies. While it was apparent that most "normal" people did not collect these artifacts, there was a delightful compulsion to accumulate these labels of independence among some visionary free thinkers who believed blockchain technology could lead to a fairer world.

The Infinite Improbability Drive is a wonderful new method of crossing interstellar distances in a mere nothingth of a second, without "tedious mucking about in hyperspace." It was discovered by lucky chance and then developed into a governable form of propulsion by the Galactic Government's research centre on Damogran. As soon as the drive reaches infinite improbability, it passes through every conceivable point in every conceivable universe simultaneously. An incredible range of highly improbable things can happen due to these effects. It was installed on the Starship Heart of Gold and both the ship and the drive were unveiled by then-President of the Galaxy Zaphod Beeblebrox.

The principle of generating small amounts of *finite* improbability by simply hooking the logic circuits of a Bambleweeny Sub-Meson Brain to an atomic vector plotter suspended in a strong Brownian Motion producer (say a nice hot cup of tea) were well understood. It is said that such generators were often used to break the ice at parties by making all the molecules in the hostess's undergarments leap simultaneously one foot to the left, in accordance with the theory of indeterminacy. Many respectable physicists said that they weren't going to stand for this, partly because it was a debasement of science, but mostly because they didn't get invited to those sorts of parties. The physicists encountered repeated failures while trying to construct a machine which could generate the *infinite* improbability field needed to flip a spaceship across the mind-paralyzing distances between the farthest stars. They eventually announced that such a machine was virtually impossible. Then, one day, a student who had been left to sweep up after a particularly unsuccessful party found himself reasoning in this way: If he thought to himself, such a machine is a virtual impossibility, it must have finite improbability. So all I have to do in order to make one is to work out how exactly improbable it is, feed that figure into the finite improbability generator, give it a fresh cup of really hot tea... and turn it on! He did this and managed to create the long sought after golden Infinite

Improbability generator out of thin air. Unfortunately, after he was awarded the Galactic Institute's Prize for Extreme Cleverness he was lynched by a rampaging mob of respectable physicists who couldn't stand him being "a smart arse."

Side effects of using the Infinite Improbability Drive include temporary (and sometimes permanent), changes to the environment and morphological structure, hallucinations, and the calling into being of large marine mammals. Known effects have included the creation, and spontaneous upending, of a million-gallon vat of custard, marrying Michael Saunders, the transformation of a pair of guided nuclear missiles into a Magtrathean sperm whale and a bowl of petunias, redesigning the interior of the Heart of Gold, turning Ford Prefect into a penguin, causing Arthur Dent to temporarily lose three of his limbs, transforming the desert world of Kakrafoon into an incredibly habitable oasis during a Disaster Area concert, ridding the people of Kakrafoon of their telepathy during the same concert and allowing for the discovery of Magrathea by Zaphod Beeblebrox.

The Magrathean sperm whale was the co-product of the Infinite Improbability Drive and its reality-warping field interacting with two guided missiles above Magrathea, the other outcome being a bowl of petunias. The probability of this occurring was 8,767,128 to 1 against. The whale has an existential life of discovery which lasts a minute before it hits the ground, leaving a large crater and whale remains.

The first known use of the Infinite Improbability Drive was initiated by Zaphod Beeblebrox and Trillian on the starship Heart of Gold. Its major consequence was rescuing Arthur Dent and Ford Prefect from open space, at the probability of two to the power of 276,709 to one against.

Other events that occurred, including those that took place at a time of abnormality, include:

- Lots of paper hats and party balloons appeared from a hole in the universe and drifted off in space.
- A team of seven three-foot-high market analysts came from the hole and died from a combination of asphyxiation and surprise.
- 239,000 lightly fried eggs fell out of the hole and onto the famine struck land of Poghril in the Pansel system. This caused the one surviving man of the Poghril tribe to die from cholesterol poisoning some weeks later.
- Arthur and Ford appeared to be at the seafront at Southend, Essex, UK and were passed by a man with five heads and the elderberry bush full of kippers.

Another side effect of using the Infinite Improbability Drive is that a powerful Quantum Computer (QC) could appear at any time. Where would this leave Bitcoin, Ethereum or Solana? In a post-quantum world, miners could gain an unfair advantage by mining blocks using Grover’s algorithm. This provides a quadratic speed-up in the number of operations compared to a classical computer, which should lead to an increased hash rate. However, current miners use parallel computations on optimized hardware (ASICs) and it is hence difficult to predict if and when QCs will be reliable and fast enough to outperform them. To this end, you can assume that early generations of QCs will not be capable of outperforming classical miners in terms of hash rate. Furthermore, once QCs reach a state of development acceptable for mining, a quick adoption among miners can be expected, establishing an equilibrium as the network difficulty adjusts.

In the context of this whitepaper a key property of the Infinite Improbability Drive is that under the careful control of Zaphod Beeblebrox it can eliminate the need for *Infinidim Enterprises* to include a project road map in this proposal because our product can be delivered and manifest itself instantly on planet Earth whenever the Heart of Gold is in Earth's vicinity.

Infinidim Enterprises rejects a quantum resistant protocol

Consensus participants are known as miners or validators and upon finding a valid solution to the PoW or PoS puzzle, they are rewarded with new units of the underlying cryptocurrency and fees associated with the transactions included in the respective block. Even though quantum computers (QCs) are not yet widely available on your instance of planet Earth a recent breakthrough with a direct impact on blockchain network security is Peter Shor's polynomial time quantum algorithm that can in its subsequently generalized form break ECDSA. While more players enter this growing research area, it appears increasingly probable that powerful QCs will emerge in the near future. Although the early generations of QCs do not have enough qubits to solve problems large enough to affect Bitcoin, different alternatives for the architecture of QCs are being considered, tested and implemented so a sudden improvement in the approach might lead to a powerful QC appearing virtually overnight. In this paper, we provide an overview of the potential impacts the emergence of QCs could haveon Bitcoin. As such, we describe how a quantum-capable adversary (QCA) is in the position of stealing funds from users who have revealed their public keys. Consequently, we propose a commit–delay–reveal protocol for the secure transition from Bitcoin's current signature scheme to a quantum-resistant signature scheme, applicable even if ECDSA has already been compromised. In contrast to existing proposals, we emphasize the necessity of a substantial delay phase to provide sufficient protection against accidental and, especially, adversarial chain reorganization. We assume that the Bitcoin and Ethereum communities have agreed on and deployed a quantum-resistant signature scheme, either as a measure of precaution or as a reaction to the appearance of a (fast) QCA. Independent of quantum computing, our protocol can be generally applied to react to the appearance of vulnerabilities rooted in Bitcoin's public key cryptography. The transition can be implemented as a soft fork using a similar approach as, for example, SegWit.

Elliptic Curve Digital Signature Algorithm (ECDSA) is an implementation of the Digital Signature Standard (DSS) based on elliptic curve cryptography (ECC). The purpose of such signatures is to allow third parties to determine the legitimacy and integrity of a signed message, while the signer cannot reasonably deny the act of signing. In Bitcoin, transactions are digitally signed using ECDSA, thus securing the transfer of ownership of bitcoins. ECC is a form of public-key cryptography that uses the mathematical properties of elliptic curvesover finite fields. More specifically, to define an elliptic curve cryptosystem one chooses a curve C and a public point P on the curve. To generate a pair of keys, one chooses a random number sk as the private key and uses elliptic curve point multiplication to multiply the point P with itself sk times thus obtaining the public key pk which is itself another point on C. ECDSA or, in general, ECC, relies on the assumption that it is intractable to solve the elliptic curve discrete logarithm problem (ECDLP),which would allow for deducing the private key from the public key. Like integer factorization, ECDLP has no known reasonably fast (e.g. polynomial-time) solution on a classical computer.

Quantum computing makes use of various quantum phenomena, such as superposition and entanglement, to represent classical data in a quantum context and to manipulate it in ways

that produce interpretable results. Just like the state of classical computers is made of bits, QCs use qubits that have two fundamental (basis) states (0 and 1). However, while the computation is running, the state is a linear combination (superposition) of basis states, each having an associated probability to be measured. To extract information about the state of a QC, the system is measured collapsing the superposition to one of the possible basis states. This means a QC with n qubits can represent internally the whole range of n-bit numbers and can perform calculations on all of them simultaneously; however, when measured, the state will collapse to just one of the basis states, thus returning only one of the results to the performed calculation. Instead, quantum algorithms try to make use of the underlying structure of the problem in order to amplify (or otherwise home in on) certain basis states, to increase their probability, and thus to make the result obtained repeatable and conclusive. For some problems, quantum algorithms can yield a significantly improved runtime complexity over their classical equivalents, thus offering a speed-up.

Grover's algorithm is another efficient quantum computation. It aims to solve the problem of searching unstructured data by computing with high probability a unique (or very rare) solution x for which f(x) equals v, some desired value. The time complexity is $O(\sqrt{N/t})$, where N is the size of the domain of f and t is the number of solutions. The algorithm works by first arranging a superposition of all possible input states, each having equal probability of being measured. Then, it uses some techniques to iteratively increase the probability amplitude of the states that represent the solution. Given N and t, the number of iterations after which the probability amplitudes of the correct states become maximal can be mathematically computed. In case t is unknown, there exists a scheme which will produce a solution in $O(\sqrt{N/t})$ steps. Note that it is not possible to measure the state after each iteration as this would collapse the superposition and the computation would end. Grover's algorithm is particularly interesting for mining as it theoretically offers a quadratic speed-up when guessing a nonce. However, in practice, it is believed that early generations of QCs will be slower than optimized ASIC miners.

Post-quantum cryptography is a new branch of cryptography interested in a suite of algorithms which are believed to be secure even against attackers equipped with QCs. There have been multiple proposals of cryptographic systems which are not yet broken by quantum computing. Some examples are:

(i) code-based cryptography relies on the intractability of decoding unknown linear error-correcting codes. McEliece used the algebraic properties of Goppa codes and proposed the first such system, which took his name;

(ii) hash-based cryptography is based on the security of hash functions which, as mentioned, are not drastically weakened by QCs. Merkle was the first to propose hash-based digital signatures by building on the concept of one-time signature schemes such as Lamport's signature scheme; and

(iii) lattice-based cryptography is based on the hardness of lattice problems such as approximating the closest vector problem in a lattice. For the purposes of our paper, it is important that the Bitcoin community agrees on and implements an appropriate alternative (or perhaps more than one) to replace ECC as the basis for digital signatures of transactions.

Once efficient QCs with internal states comprising many qubits are implemented, the underlying cryptographic guarantees of existing blockchains can be challenged. An attacker with a QC of about 1500 qubits can use Shor's algorithm to solve the ECDLP and compute

an ECDSA private key given the public key and is thus able to plant fake transactions and perform double-spending attacks. Users should be concerned about exposing their public keys to mitigate the risk that a QCA engages in (live) transaction hijacking

Under the assumption that QCs are being employed for malicious intent by some adversary, previously revealed public keys pose a direct threat to blockchain users. As outlined, a QCA is capable of deducing the private key from a formerly revealed public key with little effort. Regardless of how a public key is revealed, given the presence of a QCA, the owner is at risk of losing control over funds. Except for P2PK, one can prevent against the afore mentioned (so long as the QCA is slow to deduce a private key) by using addresses only once. Reusing addresses is not recommended, neither by developers nor the community, while numerous studies identifying privacy risks have been conducted. Hence, we assume appropriate protective mechanisms are already employed by the minority users who have bothered to read this paper and are smart enough to decide to acquire GPP coin.

The protocol described in the paragraphs below is designed to allow such users to transition securely, if rather slowly, to quantum-resistant outputs even in the presence of a fast QCA. It is based on a simple commit–delay–reveal mechanism with a long security delay and can be deployed using a soft fork. Note that once the protocol is deployed, classic ECDSA signatures will no longer be accepted and clients will only be allowed to spend UTXOs based on the previously introduced quantum-resistant signature scheme or the transition scheme described in this paper. Furthermore, if one uses an old client and spends from a non-quantum-resistant public key, the respective funds will be lost, as the public key is revealed, and no protective mechanism can be applied effectively.

Assume a user, Arthur, is in possession of GPP tokens stored in a non-quantum-resistant output, the public key of which has not yet been revealed, i.e. funded by an unspent P2PKH or P2SH output. We shall denote Arthur's public key as pk and the corresponding secret key as sk. Furthermore, assume Arthur has already generated a quantum-resistant keypair (pkQR,skQR), which will be used as a surrogate for his current keypair (during any future spending) as part of the transition. To convince the network, he is the rightful controller of both keypairs and this way regain the ability to safely spend the funds at a future date in any way he pleases (e.g. to pay user Ford), Arthur publishes a commitment H(pk|pkQR), i.e. the hash of his concatenated public keys, and leaves the funds on pk untouched for a sufficiently long security period t sec. Once the period has passed, Arthur creates a second transaction Treveal signed by skQR which consumes all UTXOs attributed to (pk,sk) and reveals both public keys pk and pkQR, proving to the network that he is the controller of both keypairs and signalling the transition of funds.

As a first step, to mark the commitment of the funds in (pk,sk), Arthur publishes the hash of both public keys pk and pkQR concatenated: H(pk|pkQR). This is achieved by creating a transaction Tcommit, which includes the hash commitment as an output. This can be achieved, for example, by using the OP_RETURN opcode, which allows us to store up to 80 bytes of arbitrary data in a transaction. Note that as Arthur cannot spend any non-quantum-resistant coins to fund the creation of the OP_RETURN, he will have to either already possess, or acquire through trade, some quantum-resistant currency units—sufficient to fund the creation of an OP_RETURN on the blockchain

After publishing the hash commitment, Arthur leaves the funds in (pk,sk) untouched for a sufficiently long security period tsec. Any further attempted use of this keypair, which would

fail in accordance with the new protocol rules, puts Arthur's funds at risk of theft. A long delay is necessary to ensure no blockchain reorganization could have occurred accidentally or have been caused intentionally by an adversary. While the specific choice of delay may be subject to follow-up scientific work and discussion in the community, we propose an initial period of six months.

Once the security period has elapsed, Arthur proceeds to safely spend the coins to any destination(s) he pleases, by revealing his public keys pk and pkQR, proving to the network he is the rightful controller of both keypairs. To this end, Arthur creates a transaction Treveal signed by the secret key skQR of the new quantum-resistant keypair, which consumes the UTXOs of (pk,sk) and in which he

(i) gives his 'old' non-quantum-resistant public key pk,
(ii) gives the public key of the new quantum-resistant keypair pkQR,
(iii) reveals (via Merkle-tree proof) that he has publishedH(pk|pkQR) in a transaction older than the security period tsec,and
(iv) provides a quantum-resistant signature of the transaction against pkQR.

Miners and validators, adhering to the new protocol rules, will then be able to verify the funds that have been committed for a sufficient period to require a new quantum-resistant public key for their eventual spending. Hence, Arthur will be allowed to spend his funds by providing a valid signature against his new quantum-resistant public key. Unupgraded consensus participants will simply believe Treveal is a normal transaction consuming the UTXOs of (pk,sk).

By the time Arthur has waited for the proposed six month delay period there is a high probability that he has forgotten that his surname is Dent never mind why he even considered doing research into this whitepaper before buying some GPP tokens. The marketing department at *Playbeing* declared that this could be regarded as an unattractive feature if it was made public and lobbied the board at *Infinidim Enterprises* to vote to drop the whole clever new protocol and soft fork idea in favour of making prospective GPP buyers aware that if they are clever enough to appreciate Douglas Adams then they are certainly well able to avoid these purely theoretical QCA thingies. Furthermore, the journalists and marketing wizards at *Playbeing* found all the above drivel about quantum resistant protocol to be headache inducing gobbledygook. In conclusion, *Infinidim Enterprises* has chosen to make use of Unfiltered Perception technology rather than adopt any Quantum Resistant technology. This allows the GPP owner to perceive and interact with any and all planes of existence, including at least 22 spatial dimensions, multiple temporal dimensions and the entire array of the axis of probability.

Solana - selected for second generation token

For reasons explored above it was decided that this project should avoid the POC consensus mechanism and Quantum Resistant technology.
Alternatives considered were:

- Ethereum: Uses Proof of Stake (PoS) since the Merge in September 2022, transitioning from Proof of Work (PoW). Validators stake ETH to secure the network, making it energy-efficient compared to its PoW days.

- Solana: Employs Proof of History (PoH) combined with Proof of Stake (PoS). PoH timestamps transactions to create a verifiable sequence, enhancing throughput, while PoS validators secure the chain.

Key Differences:

Ethereum's PoS prioritizes decentralization and security, while Solana's PoH+PoS hybrid focuses on speed and scalability.

- Ethereum: Processes ~15-30 transactions per second (TPS) on its base layer (Layer 1). Layer 2 solutions (e.g., Arbitrum, Optimism) boost this to thousands of TPS, but they add complexity. Gas fees fluctuate with network demand—often high during congestion (e.g., $5-$50+ per transaction), though Layer 2 reduces this significantly (cents to a few dollars). Ideal for complex smart contracts, DeFi, DAOs, and projects valuing security over speed (e.g., Uniswap, MakerDAO).

- Solana: Claims up to 65,000 TPS in ideal conditions, thanks to its high-throughput design and parallel transaction processing (via Sealevel). Real-world averages are lower (~2,000-3,000 TPS) but still far exceed Ethereum's base layer. Extremely low fees, averaging ~$0.00025 per transaction, due to its high capacity and efficient design. Suited for high-speed apps like gaming, NFT marketplaces (e.g., Magic Eden), and trading platforms (e.g., Serum, Raydium)—like the GPP token.

For a project like GPP, the choice of Solana aligns with its likely need for low-cost, high-frequency interactions (e.g., community rewards on Raydium), whereas Ethereum might suit a project prioritizing security and a broader developer base. The GPP contract address on the Solana network is **346qBJxY12dD7o6fVNmCopvH8KLM7Pnw5oj2Lh5Npump**

Memetics

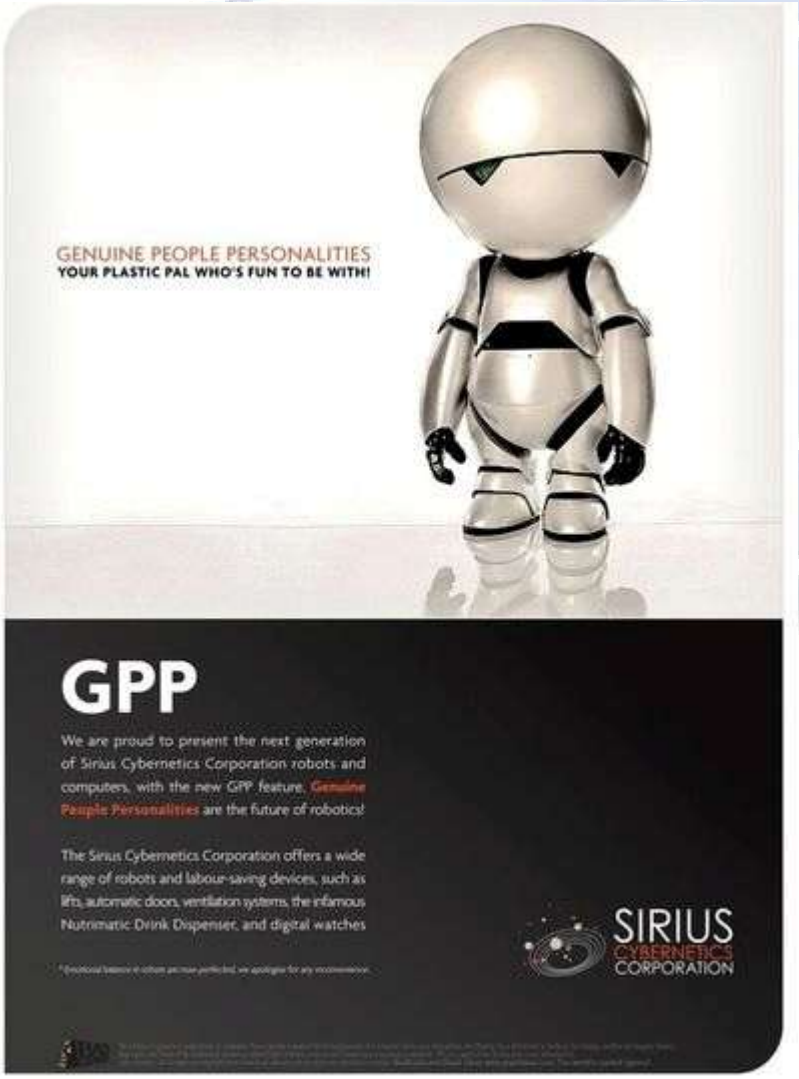
Memes didn't start with the internet. Some linguists argue that humans have used memes to communicate for centuries. Memes are widely known as conduits for cultural conversations and an opportunity to participate in internet trends. Like many words in the English language, the word "meme" has undergone a semantic shift over time. In an internet-saturated world, "memes and their meanings are co-constructed by multiple users in a social context," Jennifer Nycz, an associate professor and director of undergraduate studies at Georgetown University's Department of Linguistics, said. "This is really no different from any other process of communication or knowledge creation," she added. "It's just especially salient in the case of memes because people explicitly construct them and then post them to the world for commentary." The popular meme creator, Saint Hoax, who has three million Instagram followers, defines a meme as a piece of media that is repurposed to deliver a cultural, social or political expression, mainly through humour.

Unlike other crypto market narratives with complex technical explanations and mechanics, meme coins appear to rely solely on community, emotion and the promise of wealth. Despite the lack of meme coin fundamentals, traders are drawn to the sense of camaraderie and the promise of gains. Following an explosion of meme coins being created using pump.fun on the Solana blockchain, in October 2024 Zarniwoop was persuaded by Marvin to launch a meme coin that would appeal to fans of Douglas Adams. And it was agreed that (unlike the most

commonly successful meme coins that happen to represent dogs, cats, frogs, goats and squirrels) this one should relate to artificial intelligence of extraterrestrial origin and that Zarniwoop, the developer, should not dump the coin for a quick profit but should allow trust and popularity to grow over an extended period as use of artificial intelligence grows exponentially on Earth.

Marvin can represent the meme

He is the ship's robot aboard the starship Heart of Gold. Originally built as one of many failed prototypes of Sirius Cybernetics Corporation's Genuine People Personalities (GPP) technology. Marvin does not actually display any signs of paranoia, though Zaphod Beeblebrox refers to him as "the Paranoid Android". Nor does he show any signs of mania, though Ford Prefect refers to him as a "manically depressed robot". He merely remains consistently morose throughout. In fact, he exhibits remarkable stoicism, being willing to wait hundreds of millions of years for his employers to come. Marvin is a survivor. Survivor personalities believe no matter what happens to them they are the ones who are in charge of their destinies. They don't get mad at the world for not treating them better. But they do have an extensive menu of behaviours they can choose from, depending on the situation.



Genuine People Personalities

In psychological and social contexts Genuine People Personalities describe traits or behaviours of individuals who are considered authentic or true to themselves:

- Authenticity: Genuine individuals are authentic in their thoughts, feelings, and actions. They don't conform just for social acceptance but live according to their internal values.
- Consistency: Their actions align with their words, showing a consistent behavior pattern across different settings and with various people.
- Empathy and Honesty: They exhibit high levels of empathy, honesty, and integrity, valuing truth over convenience or popularity.
- Non-Conformity: They are less concerned with being liked or fitting in, often leading to fewer but more meaningful relationships.
- Self-Awareness: These people understand their motivations, accept their flaws, and are comfortable in their own skin, not seeking external validation.
- Emotional Expression: They're open about their emotions, which can lead to deeper connections but also makes them less likely to engage in superficial interactions.

Marketing

The Raydium exchange on the Solana network is where the GPP token will be traded. It will be promoted through a page of the Hodler's Guide to the Multiverse website at https://zarniwoop.info/gpp and via posts by Zarniwoop on X.

Of extraordinary interest to our researchers is Bowerick Wowbagger the Infinitely Prolonged who was a being who became immortal after an accident with a few rubber bands, a liquid lunch and a particle accelerator.

Wowbagger was not consulted in any way whatsoever during the composition of this white paper but *Playbeing* elected to mention him anyway in this marketing material because he is reasonably famous, probably more interesting than a Merkle tree, his picture is cool and this neatly fills up this last page.