Adamnite Litepaper

Summary

Adamnite is a new-generation layer-1 blockchain development platform serving to increase blockchain adoption. By providing a development platform that enables developers to easily build safe and efficient decentralized applications (dApps), Adamnite hopes to be at the center of both dApp development and blockchain innovation.

Adamnite's core philosophy is centered around ease of use, scalability, and security. Its primary focus is on solving two main problems in the space: a lack of proper security tools for smart contract developers, and a lack of widespread use of blockchain technology in both public and private sectors. While these problems are well-known, we believe that there are specific issues with current platforms that significantly increase the likelihood of exploits happening in dApps and hinder adoption.

- Building dApps is difficult, at least for the average developer. While Solidity, a high-level programming language for Ethereum,has become increasingly popular as the go-to programming language for smart contract development, actually building a dApp goes beyond just programming expertise: one must take into account gas fee optimization, the use of different "para" chains, deployment, and of course, security issues. A single developer or a small team of builders simply cannot build a complex dApp without the commitment of significant resources.
- Web3 technology does not offer a significant amount of advantages over its Web2 counterparts. While proponents of Web3 often argue that it is more effective because of its decentralized and open nature, it remains to be widely used because of the difficulties associated with both building and maintaining dApps. Although modern blockchains (both Ethereum Rollups and alternative chains) offer speedy transactions with little to no fees, their programming languages often lack modularity and composability, and their programming clients often have no in-built security features.
- Most modern blockchains are not truly open and decentralized. For a majority of developers, the most efficient way to interact with the blockchain of their choice is through a third-party node service, which allows them to query transactions, write smart contracts, etc. However, this is a significant roadblock for true decentralization, as a large proportion of dApps are left to depend on a centralized node provider in order to keep running.

Adamnite solves these issues by providing a blockchain that is efficient, light, secure, and easy to use. By using a variation of Delegated Proof of Stake (DPOS) for its consensus mechanism, leveraging knowledge verification for its compilers, and employing sound cryptography in the form of zero knowledge proofs for succinctness, the Adamnite Blockchain will be safer, faster and more efficient than current solutions.

Motivation and Background

We believe that the blockchain space is still in its infancy, and that there is a significant amount of value that remains to be captured with both mainstream and enterprise-level adoption. Through the creation of Adamnite, we hope to accelerate widespread adoption by making development accessible and providing enterprises with enough reason to switch to blockchain technology. Adamnite was initially conceptualized in late 2021 in a white-paper titled A*damnite: A secure and scalable blockchain development platform*, written by co-founder Archie Chaudhury. It was created with developers in mind; being a blockchain developer himself, Archie understood firsthand the difficulties of developing large scale smart contracts and dApps without significant financial backing. Since then, the Adamnite project has attracted contributors from all over the world. These contributors include core blockchain engineers, protocol researchers, and designers. Despite their differing backgrounds, Adamnite's contributors share a vision of a future where blockchain technology is used daily by millions of people around the world, and is the software of choice for businesses looking to innovate, while also being a viable option for college students participating in hackathons.

Although we maintain that the blockchain industry is still in its infancy, we also recognize its current market strength. The digital asset market, which comprises of leading cryptocurrencies (Bitcoin, Ethereum, etc), Non Fungible Tokens (Bored Ape Yacht Collection and others), and tokenized smart contracts (Uniswap, The Graph, etc), grew over 10x in 2021. A majority of this growth was driven by smart contract platforms that resulted in the creation of DeFi apps, Decentralized Autonomous Organizations (DAOs), and more.[1] The digital asset market, and the blockchain industry as a whole, is set to continue its sharp trajectory as mainstream awareness increases. In the United States alone, numerous public figures have begun accepting Bitcoin as a salary, and venues that double as sports stadiums have been renamed on account of being bought by cryptocurrency exchanges. Cryptocurrencies, and digital assets as a whole, are no longer a vehicle that few people have access to or understand. Furthermore, with developer events, hackathons, and sponsorships by top institutions becoming commonplace, programmers are becoming more and more aware of concepts relating to blockchain technology such as Web3, smart contracts, and dApps.

Problems with current blockchain development platforms

However, the price of increased mainstream adoption has also brought with it several negatives. Namely, there has been an increased tendency for large scale dApps, especially those in DeFi,

[1] Source: CoinMarketCap

to be targeted for exploits by malicious attackers. These attackers take advantage of logical invalidities within the software that allows them to interact with the underlying smart contracts in a manner inconsistent with the protocol's intentions. Consider a loop in a smart contract built for a decentralized exchange defining a swap for two assets. A small error in this loop could allow someone interacting with the contract to continuously drain the underlying pool of one of the assets while adding nothing in return. In the past year, over $3.2 billion dollars were lost in malicious attacks, with a majority coming from exploits in DeFi protocols.[2] While audits from third parties have become increasingly popular as a mark of validation, they are often expensive, and are only affordable by established companies with proper backing. This serves as a barrier to entry for individual developers or a rag-tag team of builders.

Current blockchain development platforms also suffer from a lack of scalability and accessibility. While the slow transaction speeds and high gas fees associated with Ethereum have been addressed with new layer 1 platforms such as Avalanche and layer-2 roll ups such as Polkadot, blockchain development remains highly underutilized. Most of these chains often need to allocate millions of dollars in funding to actually attract developers to their platforms. Furthermore, newer chains also tend to focus on one specific problem, such as transaction speed (Solana) or light clients (Mina), rather than providing a general platform that works for developers. This leads to a variety of chains that come with their unique problems, forcing developers to sacrifice say speed for ease of use or scalability for security. While Solidity is certainly becoming more popular as a programming language, and more recently has become the language of choice for blockchain developers around the world, it remains difficult to work with for average programmers due to its inherent complexity. While the language itself is easy to learn, actually creating and deploying a secure contract while accounting for efficiency and long-term scalability is a different story. This is reflected in the relative lack of diversity of current dApps. Despite the potential of blockchain technology to be used in sectors such as healthcare, supply chain, and beyond, a majority of dApps today center around DeFi and NFTs, with the former being dominated by yield protocols and the latter by virtual art.

Introducing Adamnite

Adamnite is a revolutionary blockchain development platform, looking to make blockchain technology more suitable for individual developers, startups, and large scale organizations alike. Although Adamnite will have its own native token, NITE, its purpose is not to be a decentralized payment platform like Bitcoin. Rather, Adamnite will be a development ecosystem that gives developers the power to build secure dApps easily. Current blockchain platforms offer little in the way for actual creation; their scalability and security issues often lead to companies choosing to abandon blockchain technology altogether, or worse, only partially integrate with it in the hopes

[2] Sigalos, M. K. (2022, January 7). *Crypto scammers took a record $14 billion in 2021*. CNBC. Retrieved January 30, 2022, from https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html#:~:text=Cryptocurrency%20theft%20rose%20516%25%20from,%247.8%20billion%20worth%20of%20cryptocurrency.

of capturing on the hype. A great example of this are gaming apps, which often integrate NFTs built on various chains for only a portion of their actual software. These are not true dApps: a majority of the actual game, such as user information, graphics, and scores, are stored off-chain. The same is true for virtual worlds, or metaverses, which often use NFTs as validation but rarely use blockchain technology for anything else.

With Adamnite, the creation of a basic decentralized game that runs completely on-chain will essentially be as simple as creating a game that runs using Web2 technology. A developer can leverage Adamnite's succinct nature to directly download a node and validate the blockchain without having to sacrifice a large amount of computing power. Then, they can write smart contracts in one of two high level programming languages: a Script-like language similar to Solidity, and a Pythonic language similar to Python. A key difference however will be modularity; various modules will be made available for developers to download. These modules will increase the efficiency of seasoned developers while helping newer ones acclimate to the ecosystem. A great example is the creation of a digital asset; on Ethereum, the same lines of code are often reused across thousands of smart contracts to create ERC-20 tokens with only slight variations. This is significantly limiting for advanced developers who want to add additional functionality to the core smart contract driving their asset. Adamnite's modular structure will allow developers to download standard code as modules, thus also breaking down the barrier of entry required for newer developers to create on-chain contracts.

Once a developer has finished writing the smart contracts that define their dApp, they will be able to declare statements in the form of knowledge assertions that define how they want their code to function. A developer creating a DeFi protocol for example could define a variable in a loop as a loop invariant, which basically states that it should not change throughout the loop's execution in order for the smart contract to function as intended. They will then be able to execute the program through the compiler for their respective language. At this point, a knowledge verification system similar to the one employed by QuickCheck for Haskell will generate test cases for the assertions made by the developer, and return how successful the assertions were when tested. The developer will then be able to edit the program before compiling again. This serves to add a basic layer of security for dApps built on Adamnite: while creators of larger scale dApps will likely want a formal audit (the compiler still serves as a great first step), individual developers and hackers will now be able to build dApps with the confidence that their program meets their standard of safety. Finally, once a developer is satisfied with the state of their program, they can deploy their smart contracts to mainnet. As a result of its consensus mechanism and use of zero knowledge proofs, Adamnite's blockchain is speedy and scalable: transactions are cost-efficient and fast, while the network itself minimizes congestion. dApps on Adamnite will not only be secure, but they will also be scalable for long-term use by the general public.

Core Team

Adamnite is completely open-source and decentralized in nature. Currently, there are approximately 20 main contributors, with others helping more sporadically. However, there is a core founding team that has taken the lead on implementing the protocol and ensuring the initial development of the platform. This core team is highlighted below:

Name	Background and Role
Archie Chaudhury	Archie is a blockchain developer and cryptocurrency enthusiast based in Atlanta. He previously worked on Choice Coin, an open-source voting software that leverages the Algorand Blockchain for decentralized voting. He is also a part-time contributor to Bitcoin Magazine.
Thomas Petersen	Thomas is a brand designer and consultant who has a keen passion for decentralized technologies. He runs First Principle, a brand management firm based in New York. He also previously worked at Square.
Khalil Shanti	Khalil is a front-end engineer based in Miami. He's currently working on a variety of open-source projects, and has an interest in NFT marketplaces.
Faiz Ali	Faiz is a digital asset consultant in the United Kingdom. He has previously advised blockchain projects in the UK, United Arab Emirates, and United States.
Tsimafei	Tsimafei is a core blockchain engineer with extensive experience in the field. Based in Japan, he has previously led development teams working on blockchains such as Quras.
Nishan Maharjan	Nishan is a software developer with experience developing P2P protocols. He is currently learning more about blockchain technology and its various use-cases.
Dibek Pouydal	Dibek is a software networking engineer who primarily works in the Go Programming Language. He is currently exploring ways to leverage cryptography to create secure blockchain networks.

Conclusion

Adamnite will power a new generation of applications built entirely using blockchain technology. While blockchain development platforms have existed for the better part of a decade, significant adoption is still lagging, with security issues significantly degrading the trust of the general public in the space and scalability issues turning off enterprises from building their core infrastructure using blockchain. Adamnite aims to be a permissionless general purpose blockchain that provides developers of all backgrounds the tools they need to build smart contracts that both meet their standards and the standards of their users. We have a strong belief that the blockchain industry is still in its infancy, and as adopters, we are all early in a space that will soon be utilized on a daily basis by millions around the world. By creating a platform that is at once secure, scalable, and efficient, Adamnite will be at the forefront of this future adoption, and will help blockchain technology reach its true potential.