outlast.me /dfinity/

DFINITY

18-23 minutes

This post was co-authored with Chris Dixon. It pertains to an **a16z**crypto investment. The original announcement is here, on our official blog.

The Promise of Cryptonetworks

Today's web platforms like Google, Facebook, and Twitter command a great deal of power over their users and third-party developers. They are the aggregators who, by virtue of their stronghold over all user and application data, have control over: each and every interaction between users on the platform, each user's ability to seamlessly exit and switch to other platforms, applications' potential for discovery and distribution, all flows of capital, and all relationships between applications and *their* users. They also control the rules of the game. At any time, without warning, and almost entirely on their terms, these companies can (and do) change just about anything about what is allowed on their platforms—often disenfranchising entire companies in the process.

This is especially problematic because the incentives of any centralized web platform and those of its users/developers are fundamentally misaligned. As we've articulated before, a platform's tendency to extract value from its users and compete with its third-party developers only increases with time. Over the past two decades, the inevitable consequence of this has been a slowdown in innovation because entrepreneurs no longer trust that the rules of the platforms they are building on will remain neutral and fair.

The fundamental problem here is that mutual trust between humans does not scale. At the global scale of the internet, meaningful collaboration between strangers has historically been impossible without the aid of a trusted intermediary. Central institutions like the web platforms of today have stepped in as those intermediaries and, because of the strong network effects associated with data ownership and human trust, they've accumulated inordinate and defensible power.

Cryptonetworks will enable the emergence of a new breed of digital platform that, unlike the centrally governed platforms of today, will be owned and governed by their respective communities of users and developers. The resulting broad representation of interests will go a long way toward ensuring that they operate and evolve in a way that is both neutral and fair.

Trustless & Decentralized Computation

The key building block upon which all of this depends is decentralized computation, for it enables the creation of programs that run in a "trustless" manner. That is, programs whose correct execution does not depend on the trustworthiness of any one entity—not even those who control the computers that run them. The correct execution of this kind of program is cryptographically and game theoretically guaranteed by an underlying, decentralized protocol. Such programs are known as *smart contracts*, though a better name for them might be *autonomous programs*. They are not to be confused, however, with autonomous agents from the Artificial Intelligence world. These programs are simply autonomous by virtue of their independence.

Autonomous programs are powerful building blocks. The property of trustless verifiability is the core reason why they can credibly be used to disintermediate the central organizations that today mediate many of our interactions with others. Imagine, for example, building a social network like Twitter whose logic and data aren't controlled by a company, but by a program whose code runs autonomously and verifiably. Its ownership and control could even be tokenized and distributed to its users and developers. Or, just as well, imagine using such a program to encode some of the inefficient and error-prone logic that today runs inside of the brains of humans within financial institutions. Things like contracts about fundraising, trading, lending, derivatives, payments, and insurance might just be better expressed in code than in legalese.

The promise of cryptonetworks is that, by virtue of trustless primitives like autonomous programs instead of intermediaries, it is now possible to dramatically reduce the amount of trust needed for collaboration to happen. So what are we waiting for?

Well, for all of this to work, we need a *world computer* that is simultaneously decentralized and scalable.

Enter DFINITY

DFINITY is a Palo Alto and Zurich based project. It is led by Dominic Williams, a mission-driven and visionary founder who has set out to build a next-generation, decentralized world computer that can scale to billions of users. The group of people that Dominic has assembled over the past several years is, far and away, one of the most impressive teams that we have met in the space. He has brought onboard an impressive number of the world's foremost experts in distributed systems, cryptography, game theory, and programming languages. Top researchers and engineers on the team include Andreas Rossberg (who co-created WebAssembly and led the team that built Chrome's V8 JavaScript engine at Google), Ben Lynn (who is the "L" in BLS Signatures), Paul Liu (who architected Intel's Haskell Compiler), Timo Hanke (who created AsicBoost, one of the few proven algorithmic optimizations for Bitcoin mining), and the list continues. It seems like every time we catch up with Dominic and team they're in the midst of onboarding yet another high profile recruit to the project.

Today, it is our pleasure to announce that a16z crypto is making a significant investment in the DFINITY network. We are excited to see an organization of this caliber steward an open and permissionless platform for decentralized computation. It is ever so rare to come across a founding team that simultaneously: (1) is driven by a powerful and coherent vision for the future; (2) has an extraordinary ability to attract the world's very best talent (without exaggeration); AND (3) has figured out how to build an organization around the project that has its operational bases covered, strikes a balance between innovation and execution, and is set up with the right alignment of long term incentives. This last point is especially important in the crypto world.

We have great confidence that this team is poised to greatly advance the state of decentralized computing. At the time of this writing, they've already made great strides toward solving many of the open problems on the winding path to decentralized computation. They have also succeeded in building a functional prototype that runs across thousands of test nodes and actively stress tests the system's many components. One of the most important innovations that is core to the design of the system, is DFINITY's unique approach to scalability.

The Problem of Scalability

Today's existing cryptonetworks have made great strides toward bringing smart contracts to the world via decentralized computation. Most notably, Ethereum generalized the ideas behind Bitcoin and pioneered the first truly global, decentralized computer. Ever since its original conception by Vitalik in 2014, it has unquestionably become one of the most important projects in the space. The worldwide community of developers that have rallied around Ethereum is by far the largest and most active of all of today's running cryptonetworks. Its community has also become a major hub for every genre of technical discussion and the source of inspiration for much of the state of the art in the space.

At a high level, cryptonetworks like Ethereum work by interconnecting the computational resources belonging to anyone who chooses to participate as a "miner" into a unified computing fabric. No single miner need be trusted for the execution of any one program to be trustworthy. As long as the majority of miners are honest, computation on the platform can be trusted.

An outstanding challenge faced by networks like Ethereum is that, while they can be said to be decentralized, they are not yet scalable. The Ethereum community has been hard at work to address this problem and has led the way with specifications for viable solutions (e.g. plasma, sharding, and state channels). But, there are still many experiments left to be run as of yet. Our foremost

cryptonetworks today can process on the order of tens of instructions per second globally, require users to wait tens of minutes before their computations can be said to be finalized, and are expensive on a per-instruction basis. Their limitations are such that even simple applications with a few hundred thousand users are enough to fully consume the network's capacity. In order for these platforms to support applications that are rich in functionality and reach billions of users, their performance and efficiency will have to scale up by several orders of magnitude.

So, what makes scaling blockchains a hard problem?

The foremost challenge with decentralizing computation is verification. How does the client—the entity submitting a program to the world computer—know whether a bunch of untrusted miners executed the program correctly? How can she trust the results? Because anyone can participate in the network, the protocol has to assume that there will exist malicious agents who will go to great lengths to game the system for profit. For example, what is to stop a miner from skipping the hard work of actually running a program and instead returning random garbage data? The protocol has to assume that no one in the network can be trusted. Trust in the system is derived exclusively from the protocol itself which cryptographically enforces the rules, and from the emergent incentive structure which makes playing by the rules the equilibrium strategy for all parties involved.

A popular solution to this problem today is to require every miner in the network to execute every computation. The output that is produced by the majority of miners is referred to as the network's consensus and is assumed by the protocol to be correct. If more than 50% of the miners on the network are honest and are playing by the rules, then it is guaranteed that nefarious miners returning random data or seeking to corrupt the results will have their work rejected by the honest majority, and won't be compensated.

Of course, this approach has its limits. As you can imagine, it is extremely expensive to require every one of tens of thousands of miners to run every instruction of every computation. As a result, running any kind of computation on a decentralized cryptonetwork today is many orders of magnitude less efficient than it would be to run it on your mobile phone.

There are many other approaches in the works that seek to address these limitations. One natural idea is for miners in the network to elect a smaller group of delegates (say 25 instead of 25,000) and then rely on them to correctly execute computations. They have a strong incentive to be honest because, if they are ever caught being dishonest, they'd almost certainly be ejected from their privileged role by the community and would never be elected again.

The standard criticism against this approach is that it is likely to be vulnerable to the same problems that tend to afflict democracies in the real world: low voter participation, the emergence of marketplaces in which votes can be purchased rather than earned, and the possibility that the elected delegates can be bribed and corrupted. It is also, at least theoretically, not game theoretically stable: The cost of attacking the network by bribing the elected delegates is likely to be smaller than the profit that could be reaped by conducting such an attack. The jury is still out as to whether approaches like this will work well. It may be the case that even though it suffers from problems in theory, it can work well in practice.

DFINITY's Random Beacon

DFINITY's approach to the scalability problem seeks to resolve the dilemma between: on one hand, the inefficient robustness of full decentralization (where every miner runs every instruction of every computation); and on the other hand, the more efficient but likely less robust game theoretical mechanics of vote delegation. DFINITY seeks to strike the right balance between these two extremes such that it gets the best of both worlds.

At a high level, the idea is simple: to obtain the performance benefits of vote delegation, the set of miners that execute any given decentralized program should be small. But, rather than electing a static committee of miners via a human voting process that could become politicized, why not randomly select a new committee for every block that is added to the blockchain?

Doing this does indeed yield the best of both worlds:

1. Performance is far superior to that of existing cryptonetworks because consensus need only be established among a small number of miners. The improvements here are twofold:
    - First, the cost per instruction is much smaller, for its execution is replicated a smaller number of times. The total amount of work done and energy expended by the network is smaller, which translates to lower network fees.

    - Second, because propagation of messages in small groups happens much more quickly than in larger groups, the amount of time that clients must wait between submitting a program to the network and receiving a result that they can be confident about—known as the network's latency to finality—is much smaller. DFINITY's finality is on the order of a few seconds instead of tens of minutes.

2. There is no human voting process, so the problems of voter manipulation and low voter participation go away. A miner's probability of being elected to the committee responsible for computing the next block is proportional to the miner's stake in the network that he/she puts forth as collateral. Subverting the consensus of the committee responsible for computing any one block through bribery or other kinds of collusion is likely to be exceedingly difficult because predicting the set of miners that will be elected to it is not possible beforehand, and once elected they serve in their role for only a matter of seconds.

This idea is quite intuitive; it almost feels obvious. So why aren't other decentralized computing networks implemented this way? The devil is in the details. In particular, it has long been an open problem in the space to construct a secure, decentralized randomness beacon; that is, a protocol that allows a group of participants to agree upon a sequence of random numbers such that, assuming that a supermajority of participants are honest, the following properties hold:

1. Each output in the random sequence is unpredictable given knowledge of all prior outputs. In particular, it's important that the random output of the beacon is unpredictable by anyone until just before it is available to everyone.

2. Each outcome in the random sequence can be neither biased or aborted by dishonest participants.

One of DFINITY's many breakthroughs is a construction for a secure randomness beacon with these properties that is built from what is referred to in the literature as a threshold Verifiable Random Function (VRF). It relies on Boneh-Lynn-Shacham (BLS) signatures, which were introduced in a paper in 2001 and have since become an increasingly important cryptographic primitive.

Bringing It All Together

As you can no doubt imagine, there is more to building a world computer than discovering a breakthrough consensus algorithm. DFINITY is an end-to-end computing platform that's built to embody decentralization as a paradigm at every layer of the stack.

At the level closest to the application and the developer, it offers a native programming language called ActorScript (designed by Andreas Rossberg on the team) that lends itself well for distributed, asynchronous computation. One of its many features is that it greatly simplifies the management of application state for programmers via what's known as orthogonal persistence. Eventually, the DFINITY platform will offer support for many other programming languages as well.

One level below ActorScript is DFINITY's virtual machine. It is the runtime engine at the heart of each node that executes the logic of applications running on the network. It is designed specifically to churn through WebAssembly instructions (which ActorScript programs are compiled down to).

WebAssembly, in turn, is an open standard for bytecode that is universally portable and performant. That is, it can run just about anywhere at near native machine-code speeds. It also was co-designed by Andreas Rossberg while he was at Google, and is rapidly gaining mass adoption. It is now supported by all major browsers. Given its universality and performance, it is a fitting choice for a decentralized, scalable world computer.

And finally, unifying the myriad of nodes in the network (each running its own instance of the stack described above) into a unified computational fabric, is DFINITY's randomness beacon and consensus algorithm, which in turn, rests atop peer-to-peer network protocols whose mandate it is to efficiently interconnect everyone to everyone else.

Decentralized computation networks like DFINITY stand to bring us closer to a world where digital platforms can be constructed from trustless, autonomous, and open source software that is owned and governed by communities of users and developers, rather than companies. The openness and inclusiveness of this new paradigm has the potential to organize human collaboration at an unprecedented scale.

We are thrilled to be partnering with the DFINITY team and are excited to do everything we can to help them along their journey. We eagerly look forward to soon live in a world enabled by the technology that they are building.

Please note that the a16z crypto fund is a separate legal entity managed by CNK Capital Management, L.L.C. ("CNK"), a registered investor advisor with the Securities and Exchange Commission. a16z crypto is legally independent and operationally separate from the Andreessen Horowitz family of fund and AH Capital Management, L.L.C. ("AHCM").

In any case, the content provided here is for informational purposes only, and does NOT constitute an offer or solicitation to purchase any investment solution or a recommendation to buy or sell a security; nor it is to be taken as legal, business, investment, or tax advice. In fact, none of the information in this or other content on a16zcrypto.com should be relied on in any manner as advice. You should consult your own advisers as to legal, business, tax and other related matters concerning any investment.

Furthermore, the content is not directed to any investor or potential investor, and may not be used or relied upon in evaluating the merits of any investment and must not be taken as a basis for any investment decision. No investment in any fund advised by CNK or AHCM may be made prior to receipt of definitive offering documentation and due diligence materials. Finally, views expressed are those of the individual a16z crypto personnel quoted therein and are not the views of CNK, AHCM, or their respective affiliates.

The investments mentioned do not represent all investments in digital assets by funds managed by CNK and there can be no assurance that the investments mentioned are or will be profitable, or that investments made by the funds will have similar characteristics or results. For a list of digital asset investments by funds managed by CNK, plus important information related thereto, please see portfolio.

Please see disclosures and disclaimers for further information.