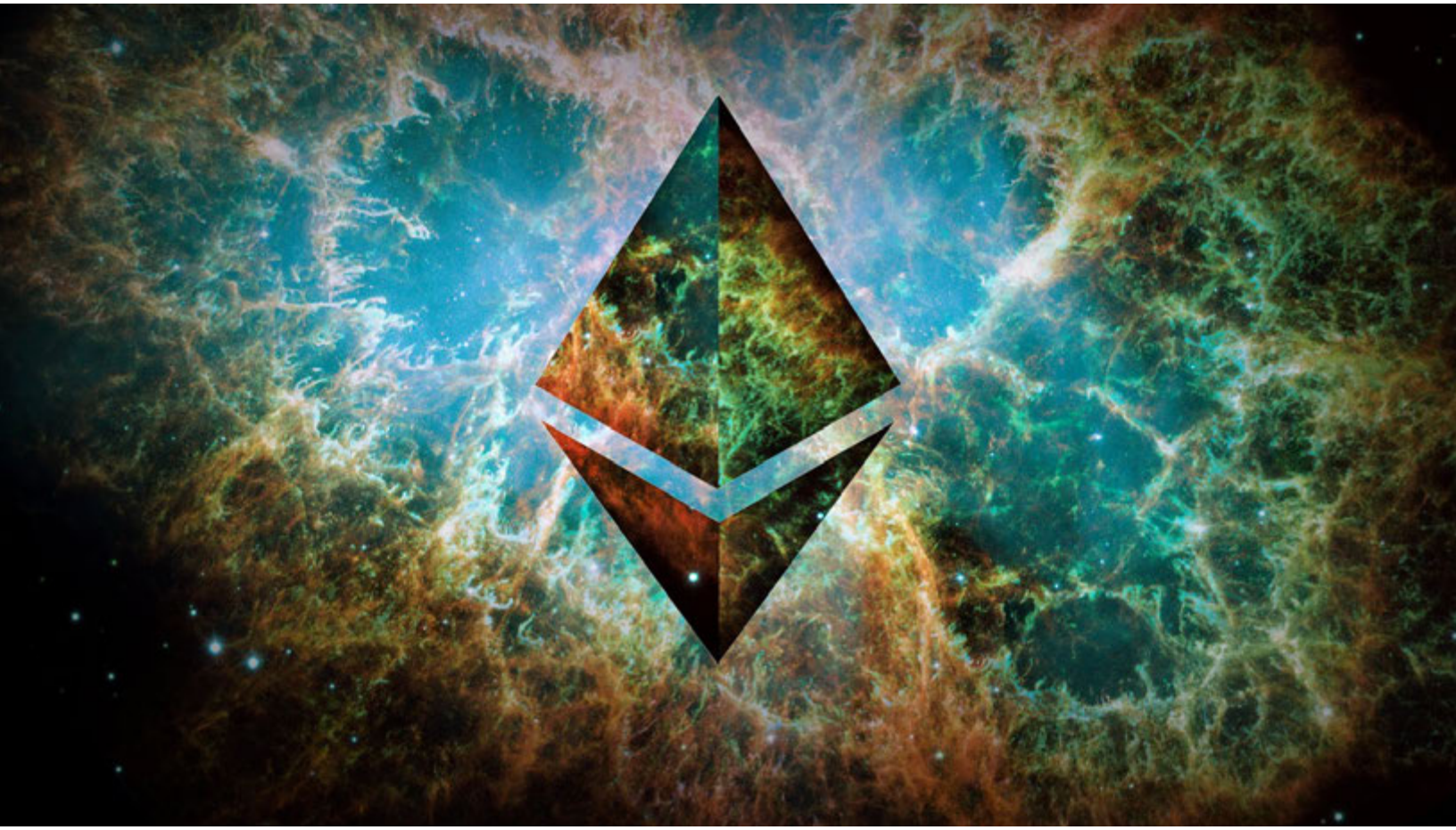


Introduction

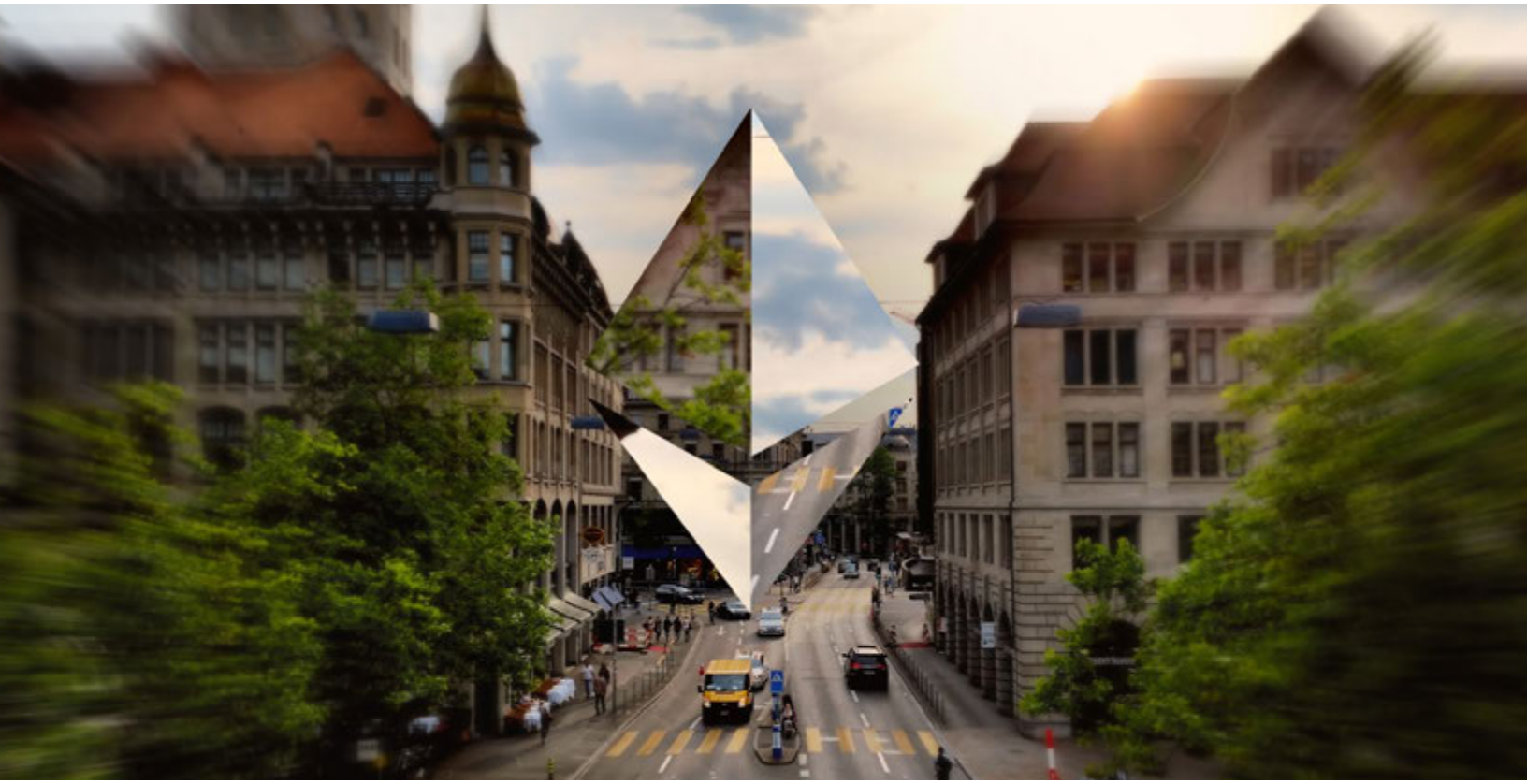
Ethereum is an open source platform which enables the creation and distribution of decentralized applications. For more information, please refer to our white paper for an overview of the platform including distribution, yellow paper for the technical implementation specification and our website (https://www.ethereum.org/) for a brief overview of our platform including an introduction video.

This document describes how ĐΞV plans to develop the Ethereum software platform and how ĐΞV is embedded in the larger context of the Ethereum project.

History & Vision

Vitalik Buterin had a clear vision in November 2013 when he first came up with the core concept of what was to become Ethereum. The intent was to create a cryptographic platform with a built-in programming language, attempting to generalize concepts such as savings wallets with withdrawal limits, multi-signature escrow, bets, contracts for difference, etc. This all-encompassing concept of "contracts" would allow users to come up with arbitrarily complex combinations of arithmetic formulas and nested if-then clauses to set up conditions for how funds could be spent.

For simplicity and ease of development, the project would be built as a metacoin on top of Primecoin (so as not to anger Bitcoin developers concerned about existing Bitcoin-based metacoins bloating the blockchain) and was scheduled to be released by the end of January 2014. Vitalik circulated the original concept white paper in December privately, subsequently expanding this distribution to wider and wider circles over time.



Since then, the scope of the project has expanded considerably. Following a substantial and unexpected inpour of interest as early as mid-December, the project first expanded to incorporate an independent blockchain, and then grew to include side efforts such as centralization-resistant proof of work, a cryptocurrency research group, legal efforts in the United States and Switzerland, and eventually the concept of the EtherBrowser, together with the currently concept-stage helper protocols codenamed 'Whisper' and 'Swarm'. Also, for the Ethereum ecosystem to truly shine, a need has also become clear for some important base-level applications: a development environment and debugger for contracts and distributed applications (Đapps), a reputation system to enhance economic and social interactions, an identity system to fairly distribute application sub-tokens, probably many name registries for contracts and web pages, wallets and of course, an app store itself (but note that downloading an app will be free of charge).

Of course, ĐΞV does not intend to develop everything. Taking the technology that both the current contributors, and hundreds of other cryptographers and developers before, have developed and applying it to tackle tough problems in areas such as consumer protection, civil liberties, international finance and contracts, law, distributed governance and sustainability will be a long and laborious journey - although one where in each case there are groups that have already begun. ĐΞV can only hope to be one small, albeit important, piece in the cryptographically enabled open, transparent and decentralized future that may come.

Organizational Structure

The Ethereum project will be initially divided into three related but independently operated bodies:

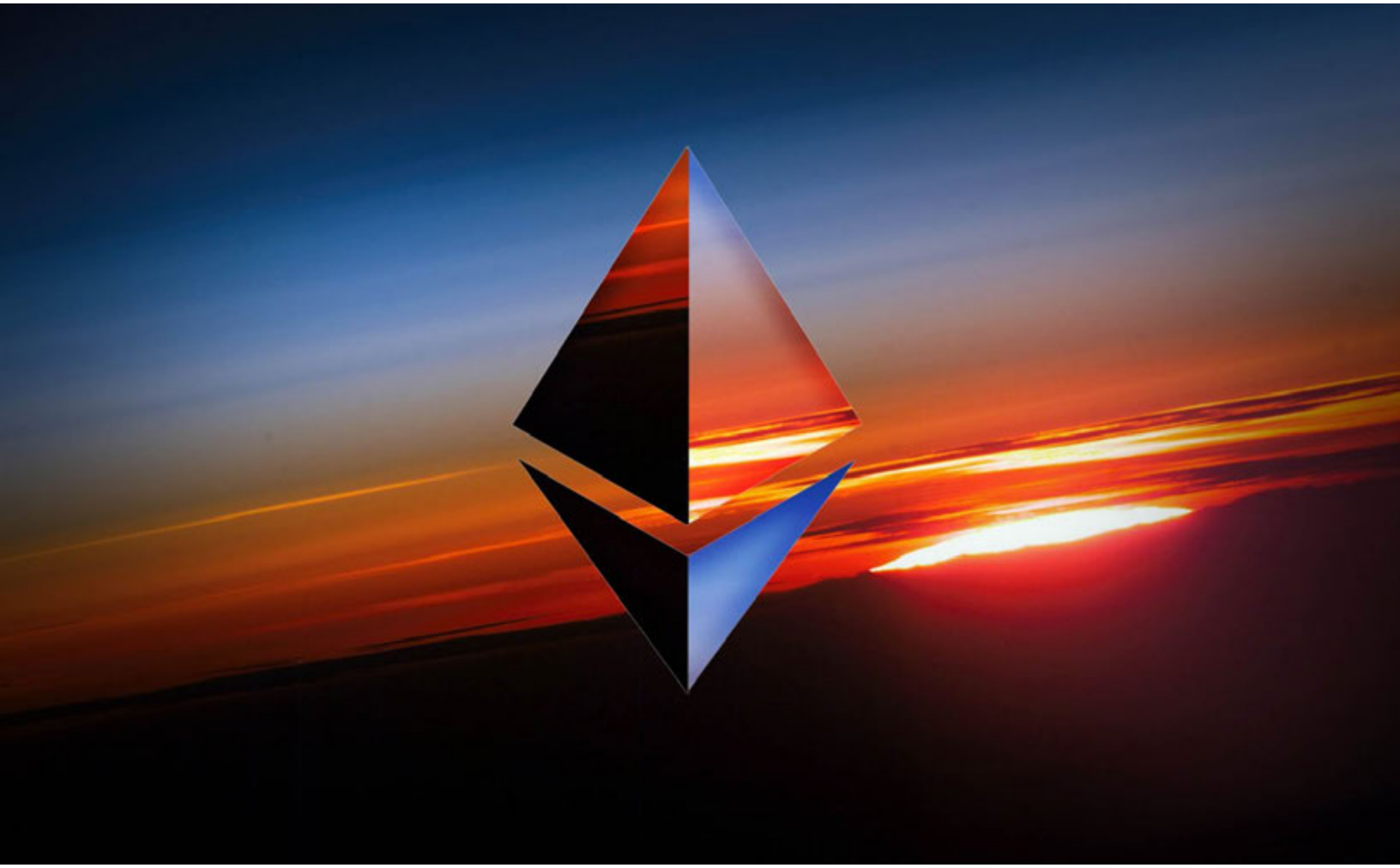
Ethereum Stiftung, a non-profit foundation based in Switzerland, in the Canton of Zug, which will serve as an umbrella organization responsible for allocating resources to other bodies for future cryptocurrency research and development going forward. The board of the Stiftung consists of Vitalik Buterin (president), Mihai Alisie (vice president), Taylor Gerring, Stephan Tual, Joseph Lubin, Jeffrey Wilcke and Gavin Wood. The Stiftung will focus on overarching "mission" and will enable operating organizations to accomplish the day-to-day work.

Ethereum Switzerland GmbH, a corporation based in Switzerland that will be responsible for a subset of operations in 2014 leading to the release of the Genesis Block. The GmbH will be 100% owned by the Ethereum Stiftung and it is expected that it will cease operations once the Genesis Block is released.

ÐΞV, a nonprofit which will receive two tranches of funds specifically for the purpose of building, optimizing and promoting Ethereum 1.0, with Ethereum lead developers Vitalik Buterin, Gavin Wood and Jeffrey Wilcke as its directors.

Other organizations, including a self-regulatory organization (SRO) and a non-profit research body, will likely also be funded. It is anticipated that the GmbH will assist with the initial organization of the research body and the Stiftung will likely oversee the SRO's activities. Ultimately the Stiftung will also oversee the research body.

Funding Priorities It is intended that the GmbH will deploy the revenue from the Genesis Sale as depicted in the Intended Use of Revenue document, but it reserves the right to make changes if it deems them necessary.



Ethereum 1.0

Ethereum 1.0 represents the primary objective of the Ethereum GmbH and of ÐΞV. The Ethereum Stiftung is interested in facilitating developments across the crypto space. At this point, the state of the Ethereum Platform development can be estimated to be about halfway from start to finish, with a view to release 1.0 during winter 2014-2015.

Since inception in January, the voluntary contributor developers have accomplished:

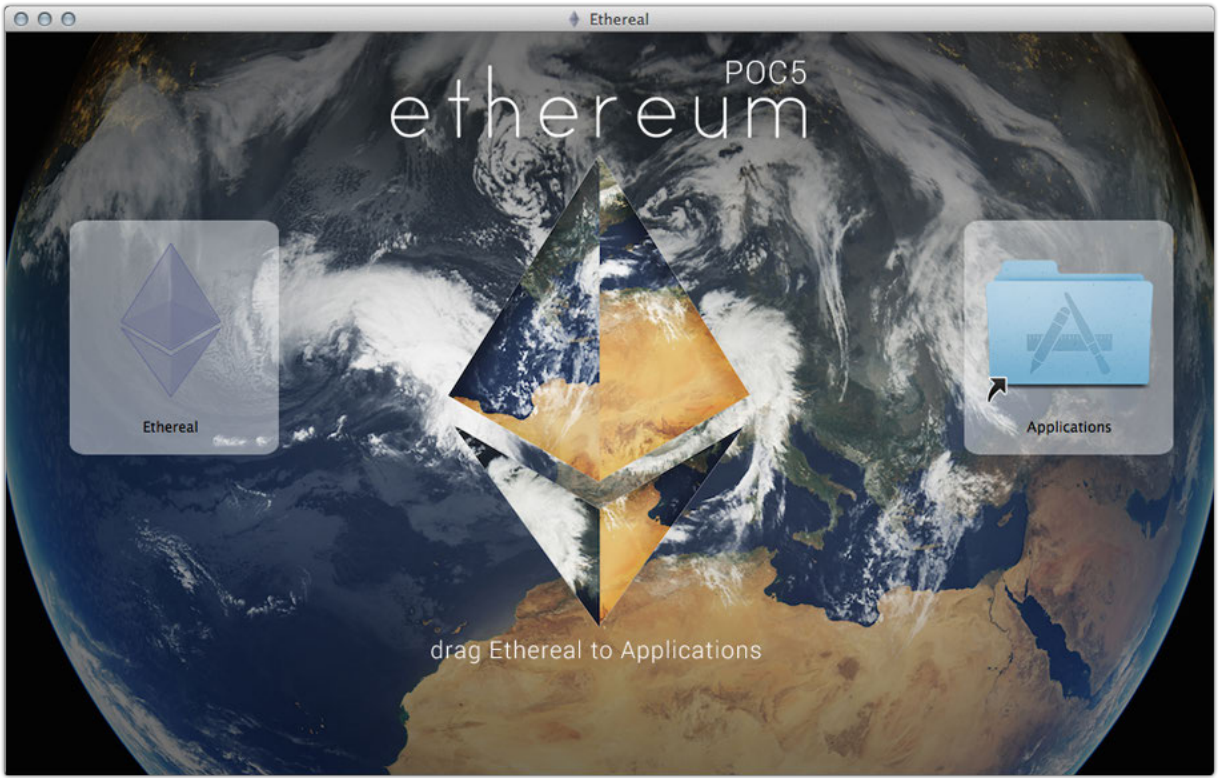
- The complete Ethereum protocol, as described in the Yellow Paper
- Four nearly compatible Ethereum reference clients written in C++, Go, Python and Java
- The Serpent, LLL and Mutan programming languages, which are fully functional with working compilers
- A functional JavaScript API
- A concept block protocol allowing for a 12-second block time, soon to be implemented
- A concept alpha proof of work built on months of research into mining and proof of stake

Thanks to the above, third-party developers already can, and have, built fully functioning decentralized applications ("Đapps") such as name registries, currencies, lotteries, crowdfunding applications, and decentralized governance utilities such as the community-built "People's Republic of DOUG."

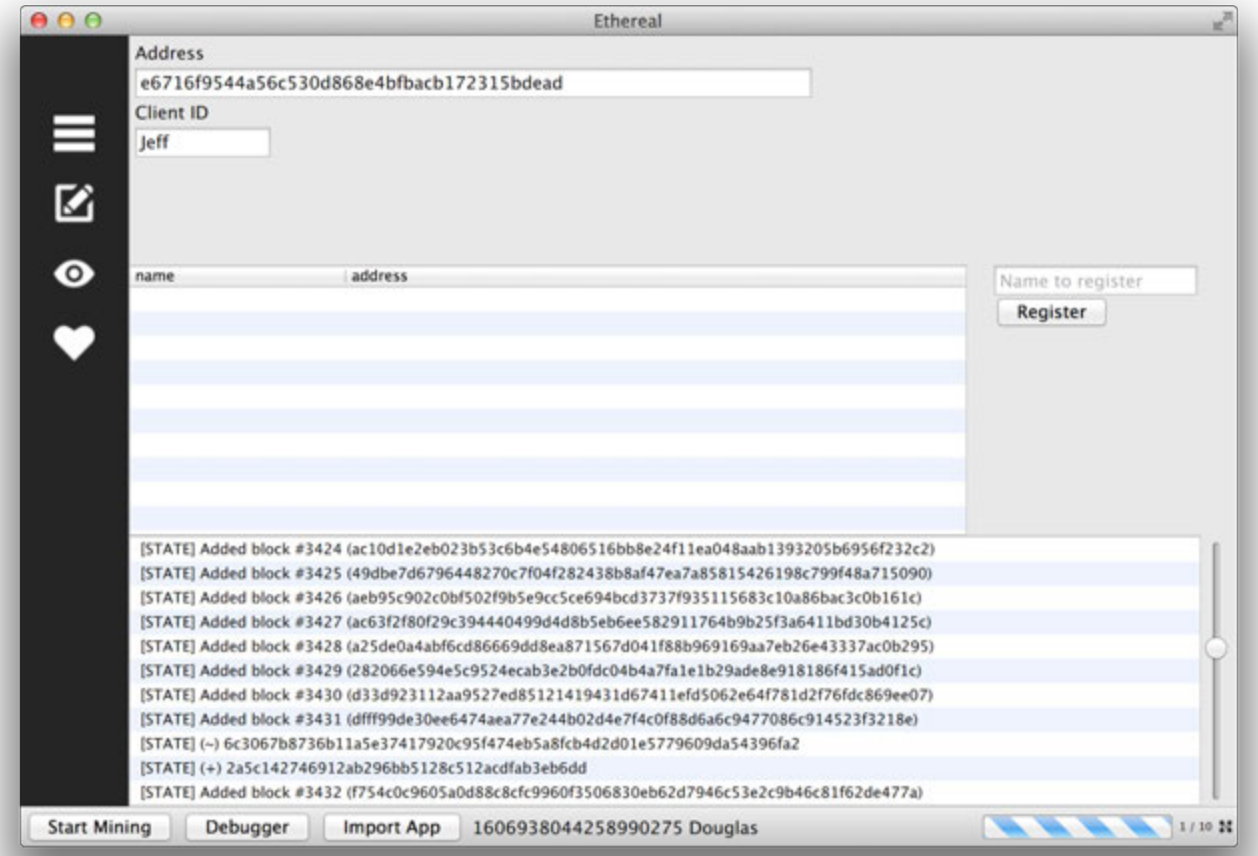
However, much of the harder work, including security auditing, just-in-time compilation as an optimization strategy and building out the interface for the browser and IDE are not yet done. See the Ethereum 1.0 Summary Roadmap on the website.

Ethereum Clients

There are currently four working and almost fully compatible implementations of the Ethereum protocol, written in C++, Go, Python and Java; the C++ and Go implementations are presently fully compatible.



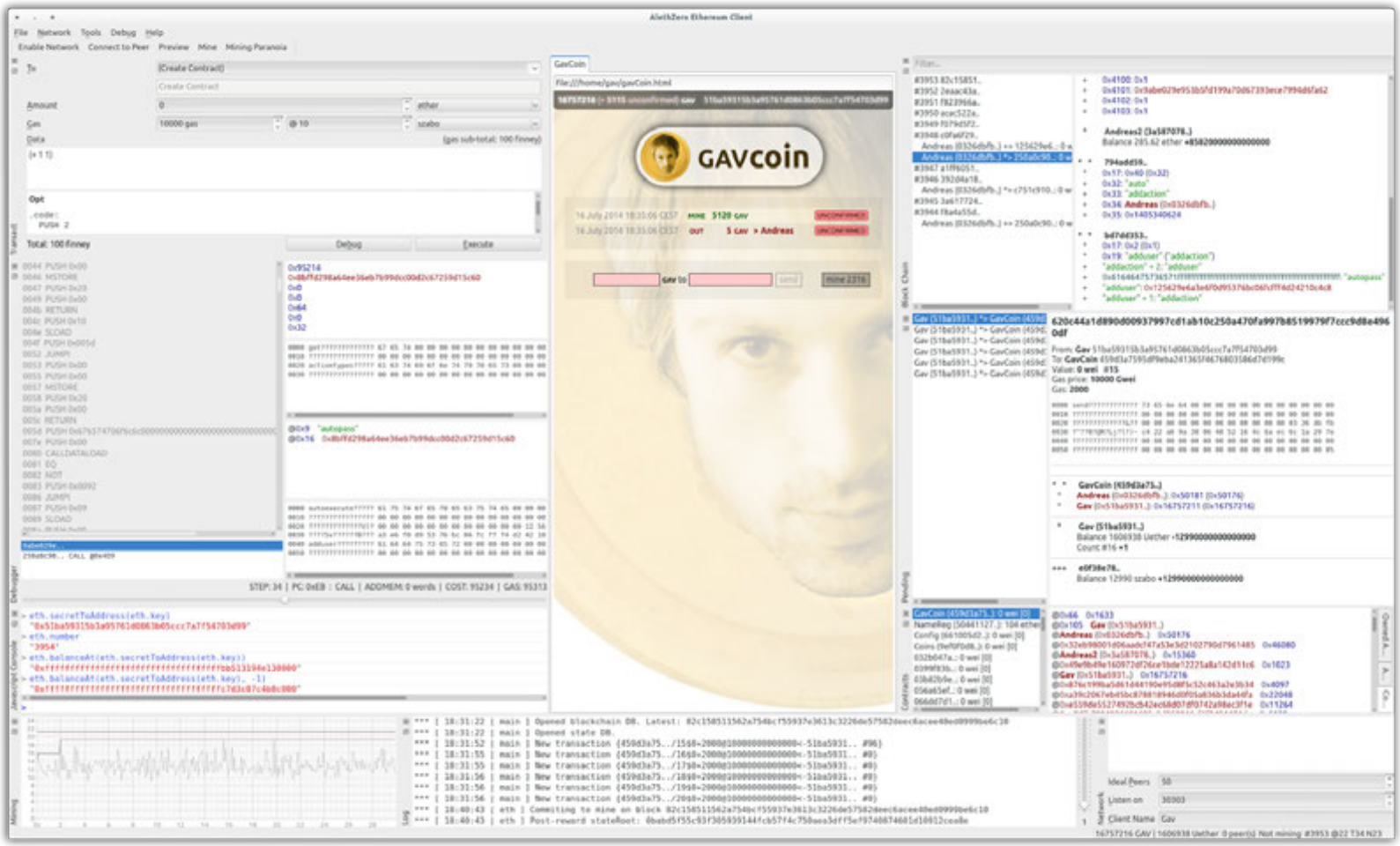
Go-specific client development



ĐΞV intends for the Go client to become the EtherBrowser, the primary client used by individuals for accessing Đapps built on Ethereum. The client, as suggested by the name, will be a fully functioning web-like browser based on Webkit and Qt, with the intent that it be usable for both browsing the traditional centralized web and the decentralized, more ethereal, web, all within one program. Currently, a basic implementation of this functionality already exists; it is possible to write a webpage in standard HTML/CSS/JavaScript, using the `eth` object as a JS API for interacting with the blockchain, and users can visit that page within the Go client in order to use the Đapp. There is also an option for writing Đapps in QML.

There are a number of important tasks that remain to be done, mostly in the area of improving the user interface. Another important component that still needs to be architected and built by ĐΞV is a multi-wallet and permission system, providing users an easy and intuitive way to precisely limit the activity and consumption of ether of individual Đapps.

C++ specific client development



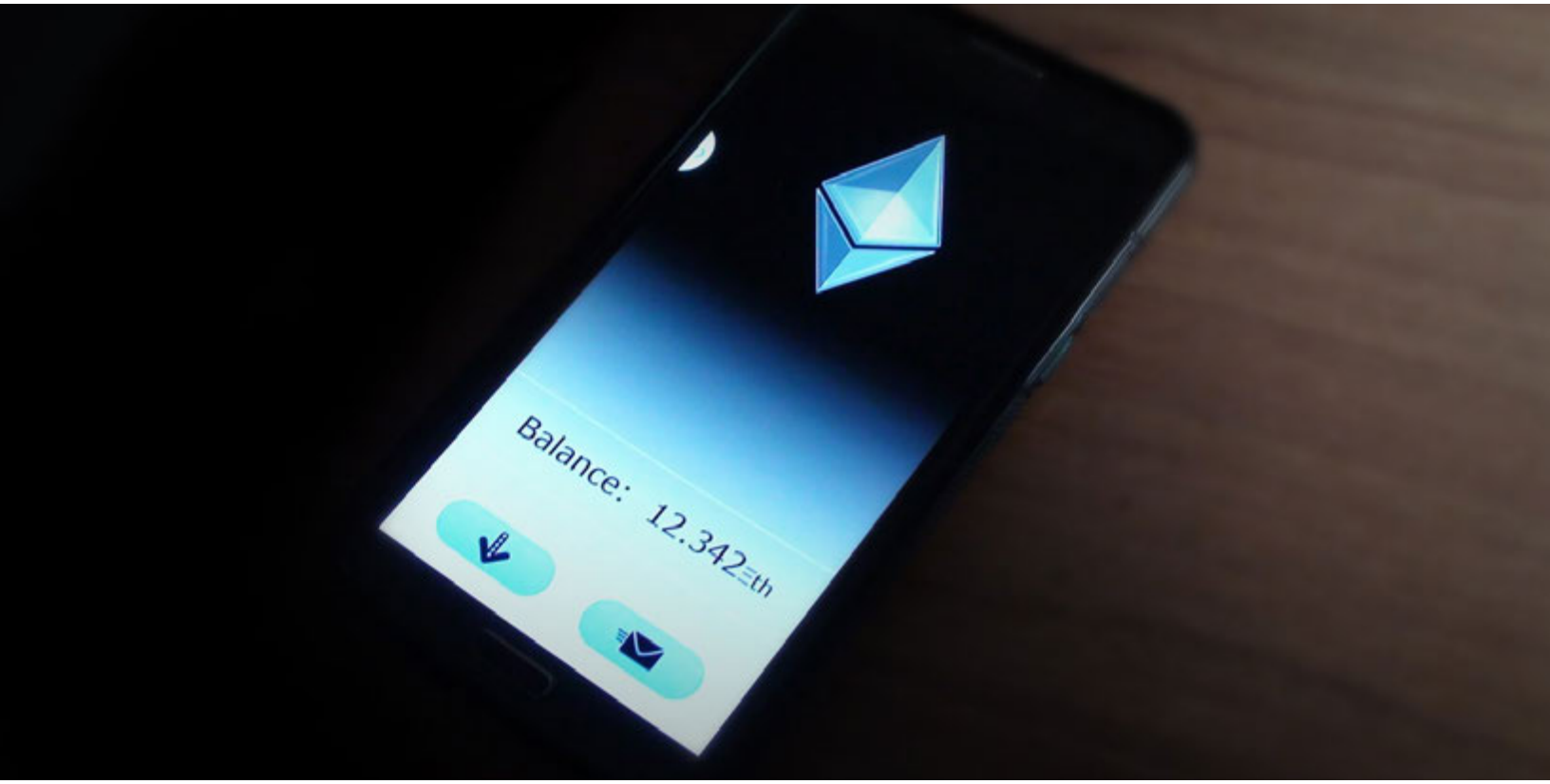
The C++ client is targeted by ÐΞV to be the primary development client, allowing people to easily build and debug contracts and Đapps, including fully featured, syntax-tree-aware code editing tools, libraries and software development kits for both contract programming languages (LLL, Serpent, etc.) and JavaScript.

The C++ client is currently fully featured as an Ethereum client, including full support for the Ethereum Virtual Machine (EVM) and blockchain protocol, and includes a bidirectional stepper debugger to help developers write contracts. However, what still remains to be done is a complete, production-ready development environment for decentralized applications, start-to-finish, including JavaScript/QML and contracts, integration testing, full multi-language support, a syntax-aware code editor, and other components and tools.

Other clients

The other three major reference clients are written in Python, Java and JavaScript.

- The Python client is to become an easy-to-install, easy-to-use, versatile developer-friendly command line client, possibly but not necessarily with a minimal GUI, but generally fulfilling a role similar in spirit to the pybitcointools library.
- The JavaScript client will be a simple and minimalistic installation, useful primarily for in-browser educational purposes, although it may eventually be used in browser-extension-based clients.
- The Java client may serve as the backend of special-purpose hardware and Android smartphone installations.



Maintaining diversity in clients connecting to and running the Ethereum network forces the development and documentation of a cleaner protocol and enables increased robustness of the overall system: an issue with a single implementation will likely not take down the network assuming other implementations are unaffected.

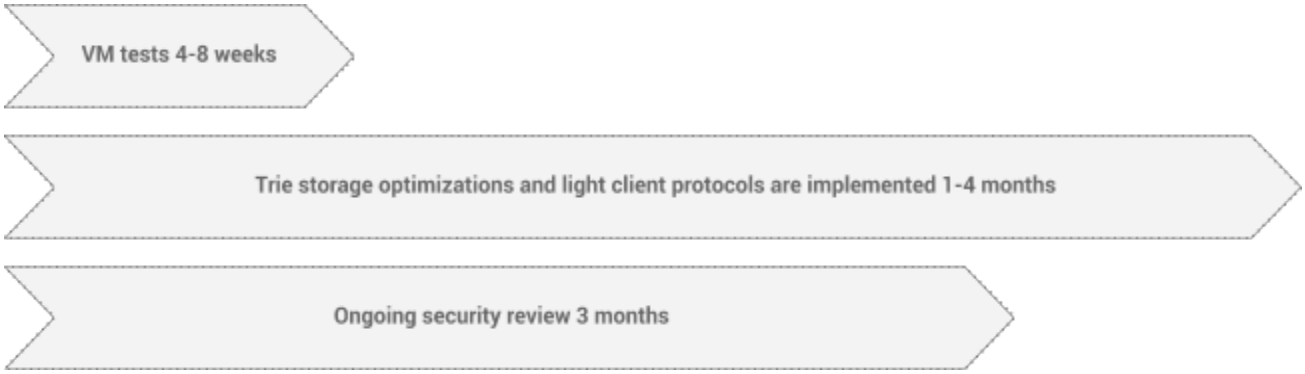
There are other client implementations in development by the extended community, including those built using Clojure, Objective C and Node.js.

Consensus and security testing

Within ÐΞV, **t**he developers of the Ethereum Virtual Machine (EVM) are attempting to overcome a very hard challenge: create multiple implementations of a recursive, Turing-complete virtual machine specification with metered computation such that each implementation handles each program and input data in exactly the same way. Because of the simplicity of the model, where a custom, heavily encapsulated virtual machine language is used and no networking, file system access, direct memory manipulation or I/O of any kind except for transactions is allowed, much of the complexity is mitigated, but a very extensive test suite will still be necessary to make sure that errors probably do not exist.

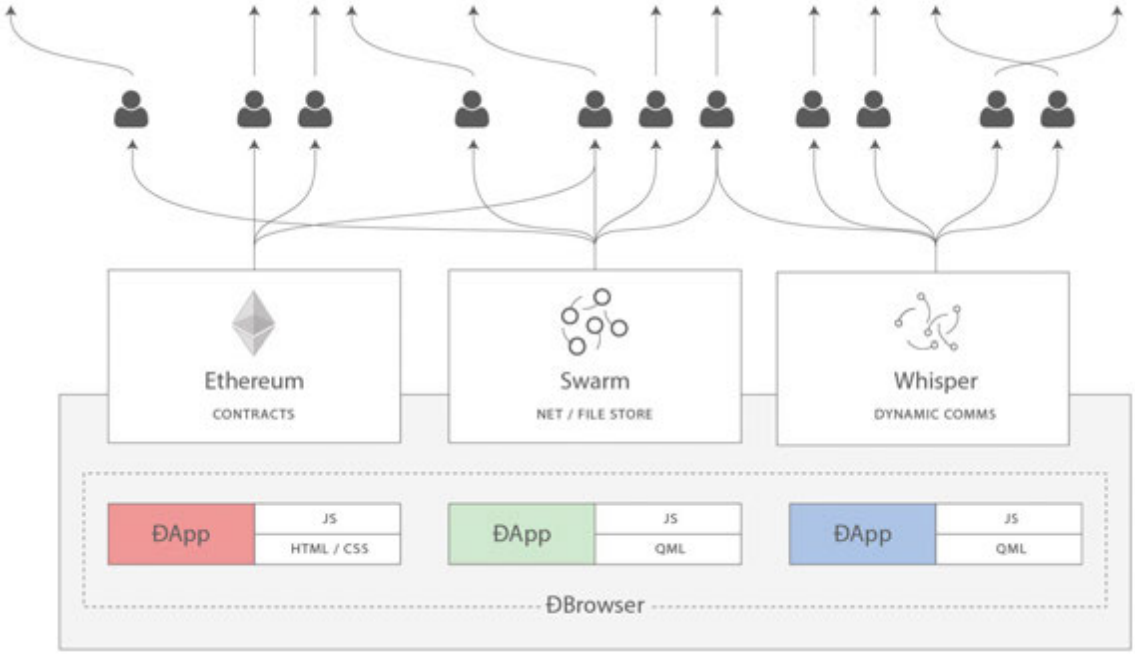
Another important concern is security. There are two types of potential security issues in Ethereum. The first is the security of the virtual machine; concerns are often raised that some kind of buffer overrun attack will be possible. Our primary defenses against this are simplicity, as mentioned above in the discussion on consensus, and the fact that the fragility of the consensus mechanism is itself a highly effective early warning system. If there is a way to access data from the "outside world" in the EVM, then as soon as it's exploited, whether deliberately or by a randomly generated test, different users will process that code differently because they have different outside states leading to an immediate consensus failure that can be detected. If research and consultation leads ÐΞV to believe that these arguments are insufficient, an additional layer of formal sandboxing may be added.

The second security concern is that of malicious contracts or Ðapps that mislead users about what the contracts do. To resolve this problem, a multi-layered approach combining permission systems, contract certification and reputation systems inside the Ðapp store and possibly formal proofs will be used. Contract certification would not be required, but would add a layer of oversight and assurance for certain types of Dapps. And, of course, any developer is free to create their own type of certification system.



Consensus and security is the main critical-path item without which Ethereum 1.0 cannot be released. ÐΞV anticipates that approximate timelines on the important items are:

1. Develop a large and maximally complete library of tests and ensure that each EVM passes all of them (4-8 weeks).
2. Make sure tests continue to pass as just-in-time compilation, trie storage optimizations and light client protocols are implemented (1-4 months).
3. Ongoing security review and testing (up to 3 months).



Whisper and Swarm Protocols

Whisper is currently a concept-stage protocol under development at ĐΞV that is intended to serve as a generic peer-to-peer (P2P) messaging protocol. Every node on Ethereum will be able to generate for itself a public key-based address, and Whisper will allow clients to send messages either to a specific recipient or as a broadcast to multiple recipients by attaching to the message a descriptive tag or "topic." Nodes route messages between themselves intelligently using as much available information as possible. Information includes known-interesting topics (nodes are free to broadcast topic filters of interest to them) and the time to live of a message (short-lived messages tend to be higher priority). All messages include a time-to-live so that the message can eventually get through even if the recipient is offline.

Whisper will likely take 1-2 weeks for the protocol specification to be researched properly and then 4-8 weeks for a dedicated team to implement the initial prototype (this can be done in parallel with other development). Refinement of the prototype to a mature implementation will be on-going.

Swarm is currently a concept-stage file storage and transmission protocol specifically targeted toward static web content hosting. Every piece of content in Swarm will be stored in the P2P network and will be addressable by its hash. The intent is for Whisper, Swarm and the Ethereum Protocol to be implemented together and accessible from the EtherBrowser to serve as a backbone for nearly any kind of application that theoretically can be decentralized. For example, a decentralized messaging system that enables users to send 140-character messages instantly and asynchronously to their subscribers will use Ethereum as a name registry mapping human-readable account usernames to the public key-based identities recognized by the system since you certainly do not want to be sending: `decentralized-blast@cd2a3d9f938e13cd947ec05abc7fe734df8dd826`. This type of decentralized messaging service will employ Whisper for sending messages, and Swarm for storing the static content that

constitutes its HTML/JS/CSS webpage. Swarm is expected to take somewhat longer than Whisper, perhaps up to 3 months, once again developed by a separate team at ÐΞV, in parallel with other work.

Light and Mobile Implementations

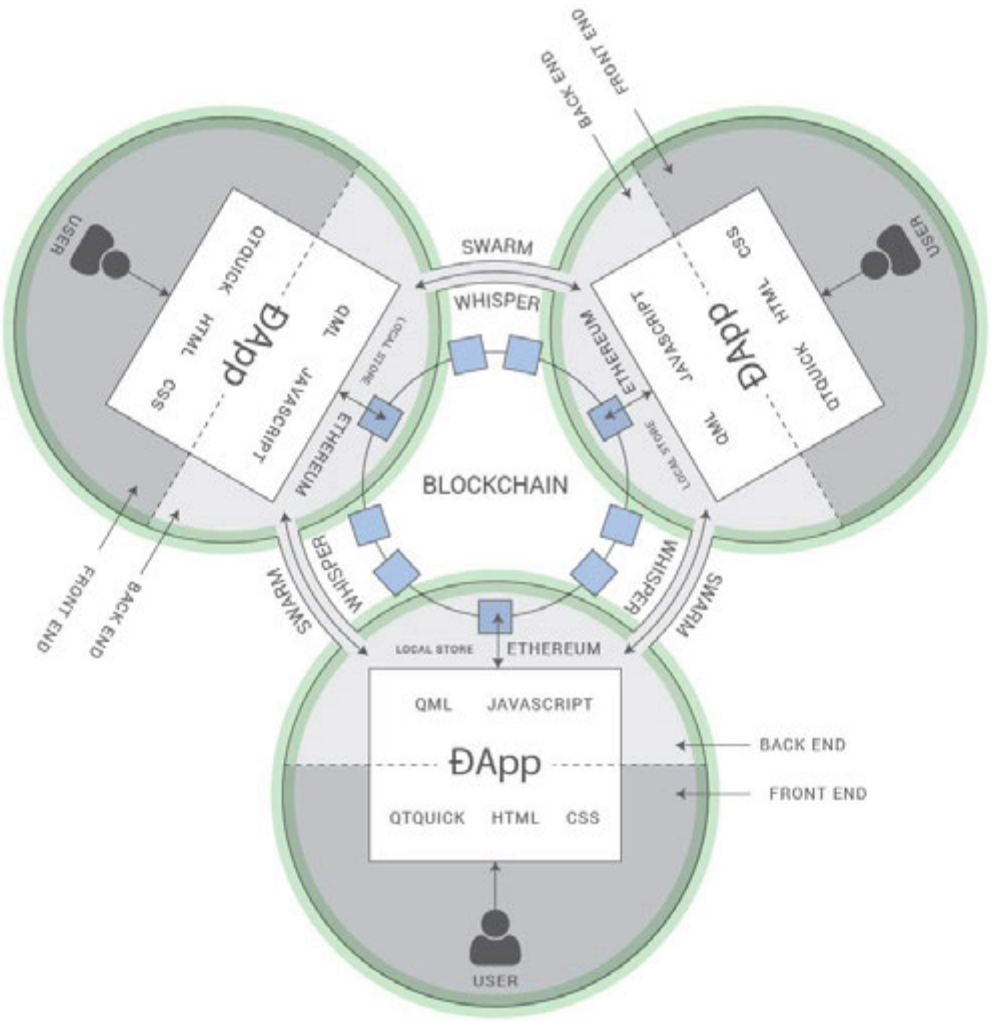
Inclusiveness has been a guiding principle since the inception of the Ethereum project and this implies working to make the Ethereum Platform accessible to everyone. ÐΞV will strive to make light clients suitable for iPhone, Android and other smartphone users, people with old laptops that cannot handle downloading the full blockchain, and people with feature phones that cannot do any substantial cryptography at all. For the former cases, the Ethereum protocol includes a robust light-client setup that enables light clients to retrieve necessary correct blockchain data provided that at least one honest fully verifying node (that's one honest node, not a majority) exists. ÐΞV intends to implement this protocol in multiple languages to allow for across-the-board mobile inclusion. For the latter case, a more centralized server-based wallet is likely in order, and will be produced because all users deserve the best experience that they can get.

Mining Algorithm Research and Development

While originally Satoshi intended for mining to be highly decentralized with everyone having the ability to mine bitcoins on their desktop, resulting in both a highly decentralized consensus protocol and an egalitarian distribution scheme, today Bitcoin mining is a highly concentrated industry. Roughly half of all miners mine through two large pools, and nearly all mining is done with highly specialized hardware that only a few companies produce; one factory in Shenzhen is currently responsible for close to 25% of all new hashpower being added to the system. Figuring out a mining algorithm that is more decentralized and fair is a difficult, but important task, and one that various people have been working on since December.

After two research attempts that proved to be dead ends, a much more mathematically rigorous strategy based on randomly generated hash functions is in the intermediate stages of development and appears to be holding its own well against initial scrutiny. ÐΞV intends to develop this algorithm, and perhaps with the addition of hybrid proof of stake, as the consensus algorithm for Ethereum 1.0. The primary remaining action item is professional review within the academic and cryptocurrency community, a process which is likely to change the algorithm substantially and guide choices in many of the important parameters (e.g. which operations to include, whether or not to make it memory-hard, how to balance circuit length and width).

Đapp Development



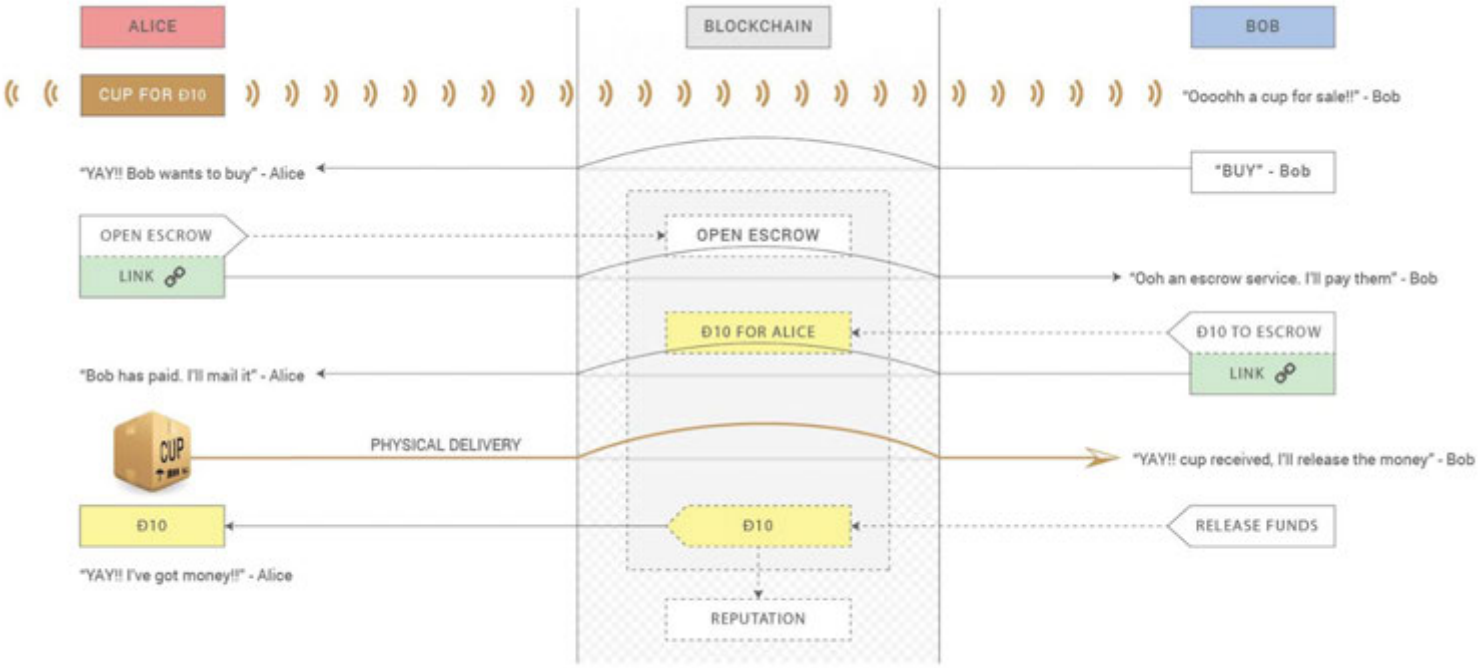
The last few years of cryptocurrency technology development have been progressively making it easier and easier for people to build decentralized applications, and the Ethereum blockchain and the EtherBrowser are important tools in helping to further that trend. However, there are also other components that can be built in order to help bring Đapps to their full potential. In essence, the intent here is to build a suite of core applications which will provide needed utilities for users like wallets and messaging, with specific attention on "meta-Đapps" – Đapps that help other Đapps. Some examples of this include a Đapp store (which is of course itself a Đapp), a name registry (or likely several), a reputation system, an anti-Sybil system (the dream is to make this last component robust enough to serve as a functional replacement for passports in high-trust situations) and decentralized governance utilities. What follows is a short list of the core Đapps that are likely to be important to build and support.

WALLET

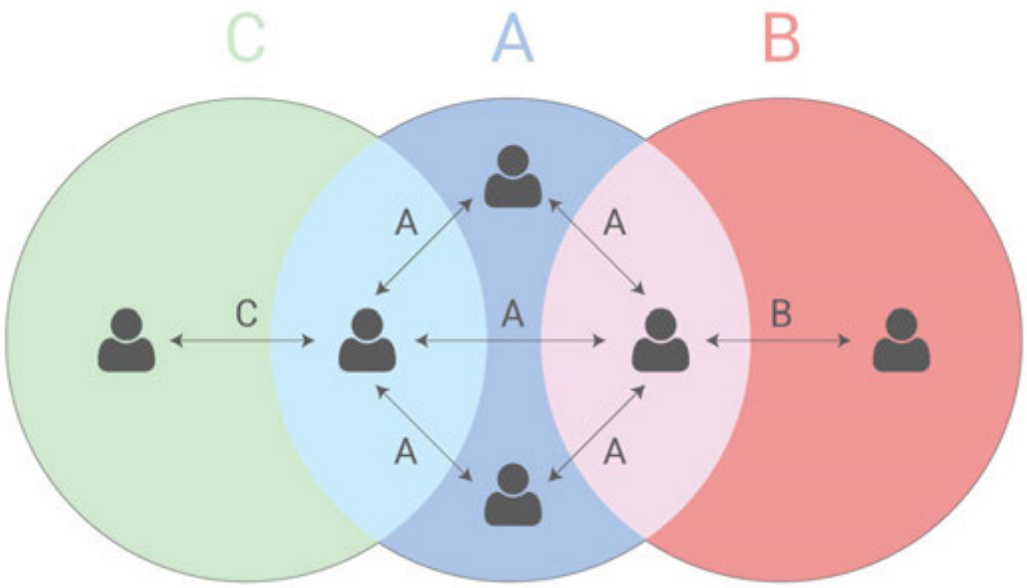
Wallets - The most basic application on a cryptocurrency platform is a wallet. However, the basic Bitcoin wallets that one sees today, with the exception of innovators like BitGo, tend to be quite weak in terms of meeting the challenge of balancing usability and security. The Ethereum Platform allows for the easy development of wallets with advanced withdrawal policies mimicking banking-style protections such as withdrawal limits and two-factor authentication but without trusting any third party with unilateral custody or withdrawal powers. Building a wallet that incorporates such strategies, simultaneously providing an optimal balance between security and convenience for $10, $1000 and $100000 is an important task, and such a wallet with the ability to use both ether, Ethereum-based sub-currencies and even potentially other cryptocurrencies will be an important boon for the ecosystem.

WHISPER

Messaging platform - As much as cryptocurrency users love decentralization, cryptocurrency users also seem to really love Skype. But since Ethereum will have Whisper, and blockchain-based name registries for accounts, why not dedicate some resources to creating an alternative to existing group text chat systems that is open-source and peer-to-peer, using the EtherBrowser and related tools as an onboarding ramp to start the platform off with a large and established community? Over time, such a platform could also expand to audio, video and even asynchronous communication such as email.



Reputation system - In order for e-commerce to be successful, in many situations one must be able to know whom to trust. In some cases, you want to tell honest people apart from scammers. In other cases, you want to tell skilled people apart from the unskilled. Still other times, it matters not just what someone's current reputation is but also how highly they're leveraging it, so you can be sure that they cannot profit from scamming everyone all at once. Even in the modern world today, both online and offline, these problems are hard, but in the context of decentralized autonomous organizations they become even harder. Figuring out what can be done, and what should be done, in terms of effective reputation infrastructure will be a crucial concern even with regard to enabling different forms of trust between Đapps themselves.



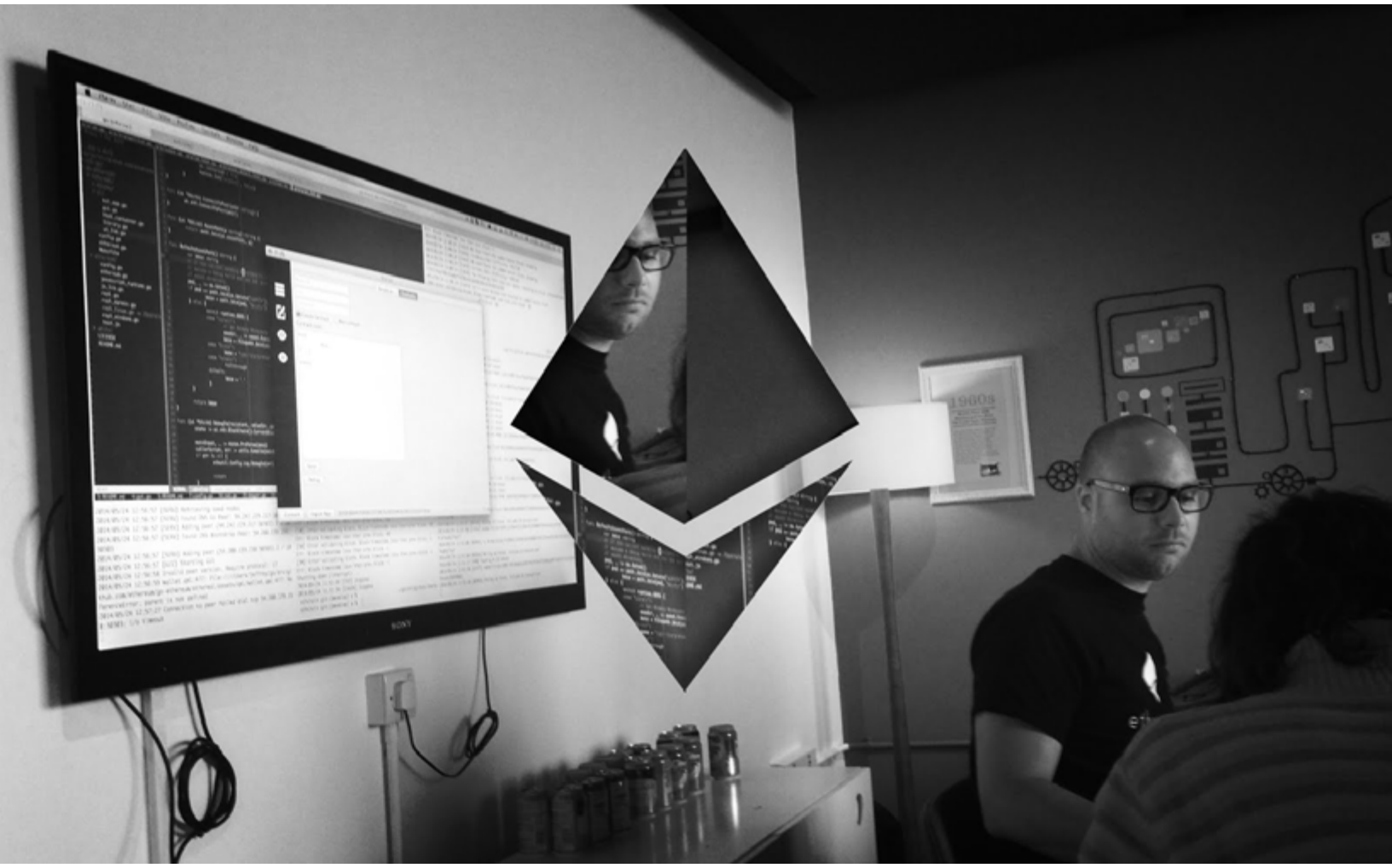
Identity system - There is a special kind of reputation, which deals with one specific question: is someone a human at all, or are they one of 5000 accounts created by a human or an automated system. Solving this question is key to figuring out how to fairly distribute application tokens or application usage privileges so that everyone can have some limited access to the ecosystem even if they do not have money to spend. One interesting proposal for implementing this in a quasi-decentralized way is to use a speculative market of "non-Sybil tokens" where anyone can create a “Completely Automated Public Turing test to tell Computers and Humans Apart” (CAPTCHA) scheme (this can theoretically include transcribing some letters and numbers, playing a game, proving proof of social connections, or something more traditional like a cell phone number or a passport), where breaking any individual scheme can be very profitable but only if done publicly. A ĐAO/Đapp can then look at the entire system and see which CAPTCHA schemes are still secure, and use those automatically.

Decentralized mining pool infrastructure - If the blockchain becomes very large and mining widespread, then just like in the case of Bitcoin, mining pools may become necessary. However, in that case ÐΞV is intent on maximally favoring decentralized alternatives such as p2p mining pools over centralized solutions, and even if centralized solutions are desired it may be prudent to build a make-your-own-mining-pool utility to make the market more liquid, reduce the variance of payment sizes to miners and reduce barriers to entry.

Aside from this important core, there are also a number of other applications that ÐΞV may choose to participate in building given sufficient resources. These include:

- Decentralized exchange (both between ETH-based assets and different cryptocurrencies)
- Decentralized marketplace
- Financial applications (e.g. hedging, SchellingDollar, insurance)
- Crowdfunding
- Escrow, consumer protection and arbitration
- Content publishing (including incentivization for content creators)
- Decentralized advertising protocol
- Decentralized organization management

Although ÐΞV intends to work on "core" applications, our participation in the development of more peripheral Ðapps may come in several forms: ÐΞV may make a full-on effort at a project ourselves, ÐΞV may simply build a kernel of a solution and allow others to continue the work, or ÐΞV may offer financial, technical or development support to external groups from the community that are already taking on the task.



Community Outreach and Education

While the underlying technologies that power Ethereum can be fairly advanced, our main goal has always been to make the power of the Ethereum Platform accessible to a wide range of developers. HTML skills, plus some JavaScript is all that's needed to build most of a decentralized application; the underlying 'crypto' layer is neatly abstracted behind user-friendly APIs. As for end users, if they are comfortable with using a web browser, they certainly will be comfortable using the EtherBrowser.

An Ethereum Platform without developers and end users would see these efforts towards a decentralized web having been in vain. ÐΞV therefore needs to insure that **(1**) people know about Ethereum and **(2**) people know how to leverage it. To that end, an important part of the project is maintaining our online and offline presence, helping to support hubs and communities around the world, and eventually organize or co-organize conferences (either for Ethereum specifically or for the decentralized web as a whole).

The other major part of this effort is education, including the issuance of easy-to-use online tutorials and Udemy courses for understanding the Ethereum Platform, as well as contract/Đapp programming workshops. Hackathons may also fall under this category.

--

The specific deliverables ÐΞV is aiming for are:

--

ethereum

OPΞN COURSES

Massive online open course - A start-to-finish complete online course on Ethereum and contract/Đapp development is slated for development. The course would include videos, text materials, exercises and online programming environments where people can very easily try out writing Ethereum code. The intent is for the course to be usable by anyone looking to learn how to develop for the Ethereum Platform, although ĐΞV may also, whether one its own or in a collaborative effort, create multiple courses for different difficulty/depth levels or different subject areas (e.g. economics, cryptography, social theory, computer science, and programming).

ethereum

OPΞN TUTORIALS

Tutorials and documentation - For those without the patience to go through an entire course, there needs to be easily accessible documents describing all of the high-level and low-level components of the Ethereum Platform and explaining how to do all common operations (e.g. writing a contract, building a Đapp, publishing a Đapp, sending a transaction, using Swarm, using Whisper) that people will want to do as developers. There may also need to be tutorials for users, although the first priority is making the decentralized web as simple and familiar as traditional websites are today.

ethereum

OPΞN COMMUNICATIONS

Online communications - This includes maintaining communication on our public blog, forum, wiki channels, as well as any other 3rd party channels (e.g. Facebook, Twitter, Google+, reddit). The primary objective is to ensure that everyone can easily acquire up-to-date and accurate information on the state of all elements of the Ethereum project.

ethereum

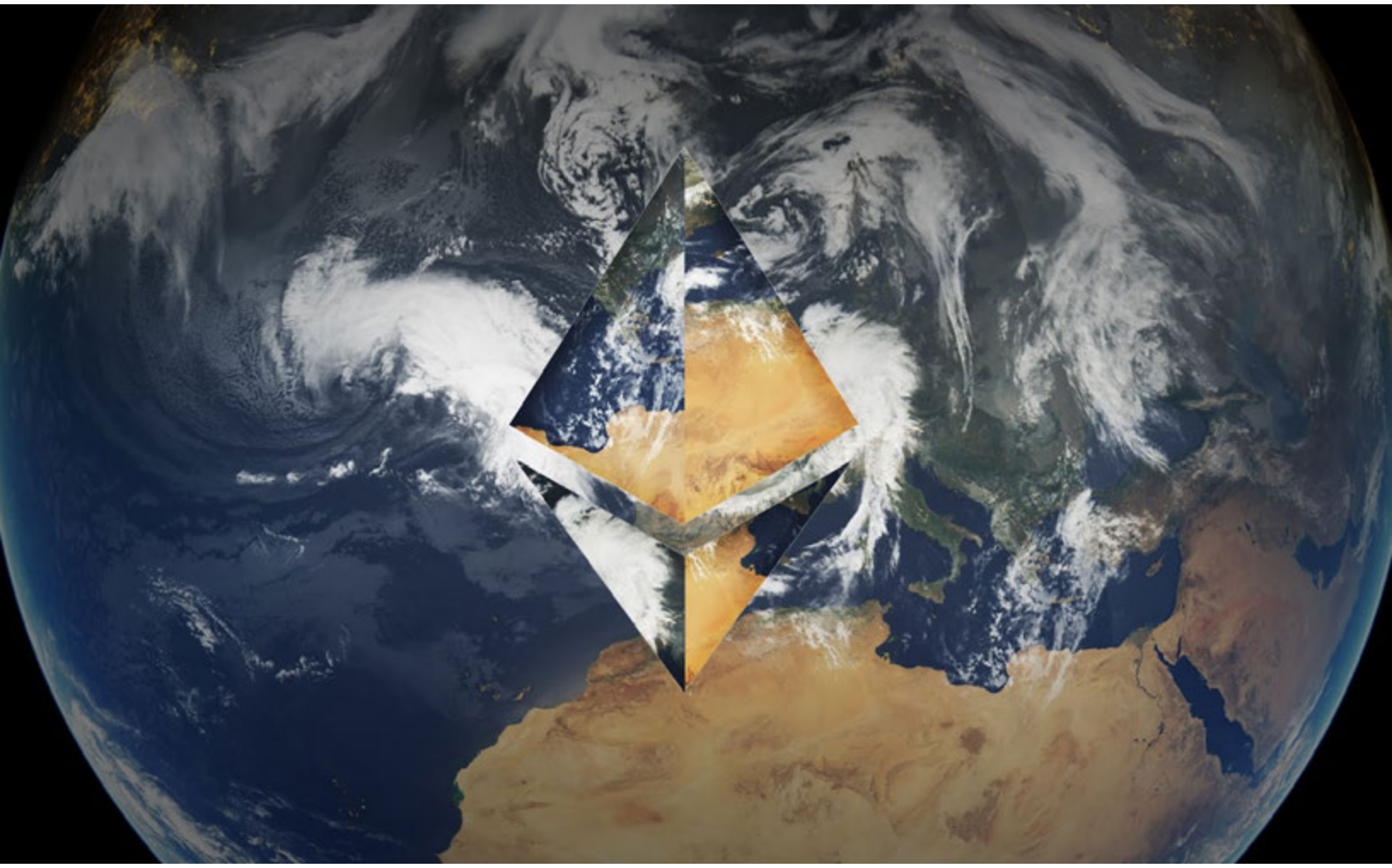
OPΞN COMMUNITY

Offline communications - This primarily consists of supporting Ethereum and decentralized web-focused meetup groups around the world, which could eventually expand into fully fledged conferences. ĐΞV intends to have a presence in as many parts of the world as possible, including North America, Central/South America, Europe, Asia and eventually Africa. Our current network of meetup locations will form the backbone of this effort.

ethereum

OPΞN ACCESSIBILITY

Translation - An important part of being international is supporting use in multiple languages. There are already partial translations in Chinese, as well as some in German and Spanish, but eventually all of the Ethereum Platform clients, documentation and online course material will have to be translated into many languages. ĐΞV is always on the lookout for technology-aware translators in a wide variety of languages.



Cryptoeconomic Research and Continued Development

As powerful as Ethereum is in its current state, and will be when the 1.0 version is released, it is far from perfect. The mining algorithm may well not hold its target of decentralization, or the computing ecosystem as a whole may shift so heavily toward thin clients that decentralized computational power as a whole may become an unrealizable ideal. Its scalability is currently not much better than Bitcoin, as every node still has to process every transaction, and new concepts such as Peter Todd's tree chains, hypercube chains, proof-of-resource as well as possible "moon math" cryptography such as Eli Ben-Sasson's Succinct Computational Integrity and Privacy (SCIP, also known as PCP or zk-SNARK) protocol will likely not be included in a 1.0 release.

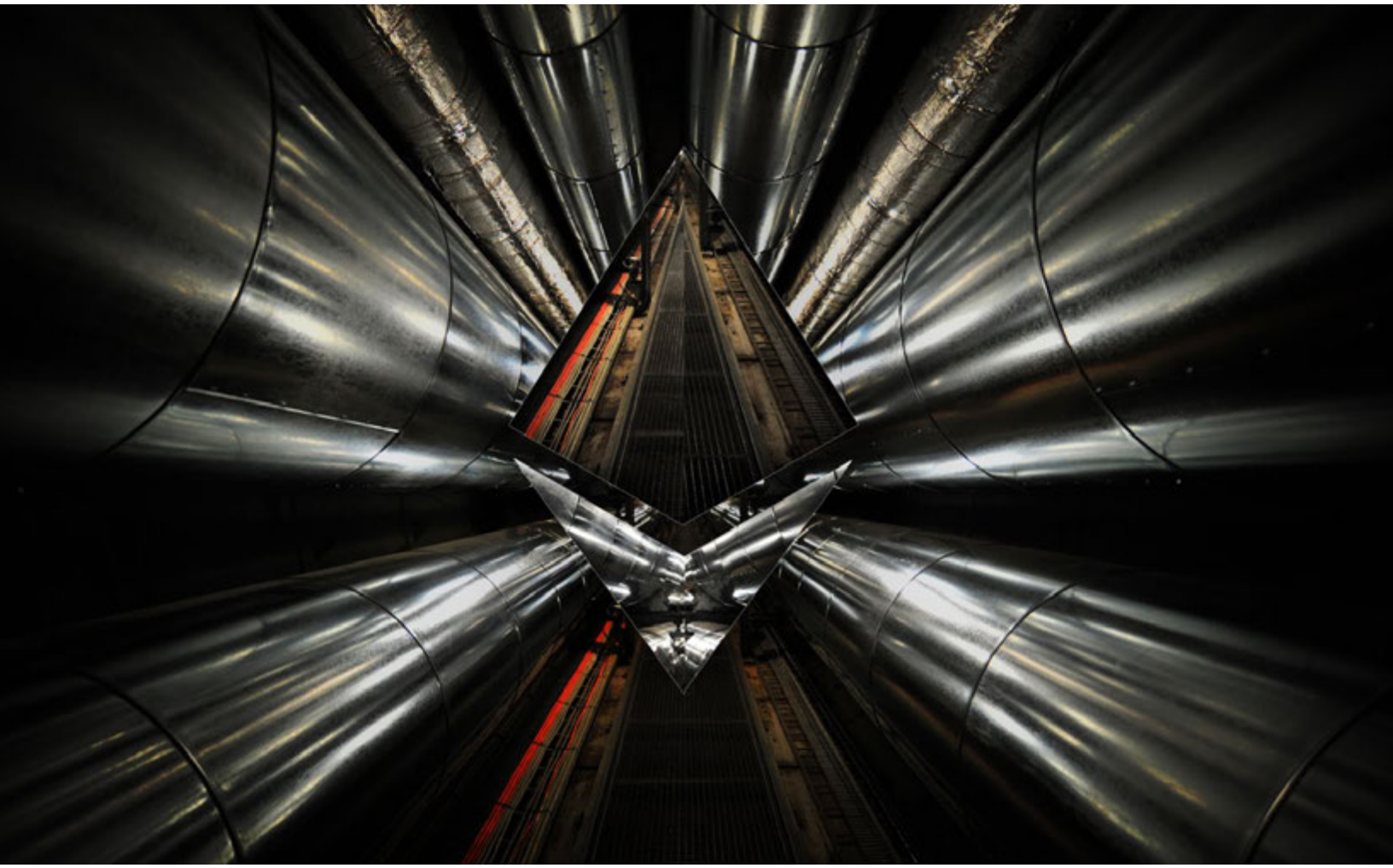
Because the directions in which future cryptocurrency development may go are numerous, and nobody can predict what the right decisions are going to be far ahead of time, no specific promises can be made regarding possible development after Ethereum 1.0 is released. However, a fairly good vision of the general direction in which ongoing cryptocurrency research will go is emerging:

Scalability - The primary challenge here is to come up with a blockchain design which breaks the fundamental barrier of blockchain scalability, namely the fact that every fully verifying node must process every transaction. There have been a few ideas developed in this regard mostly in relation to Bitcoin, such as merge-mined hypercube chains, Peter Todd's tree chains idea and strategies based on advanced cryptography such as SCIP/zk-SNARK, but there is still a lot of research that remains to be done. A successful scalability solution would need to handle moving coins across different parts of the state that are stored by different entities, not sacrifice (too much) mining security, and make sure the protocol keeps working even if some data becomes unavailable; with luck, a solution will be brought to completion over the course of 2014 and 2015.

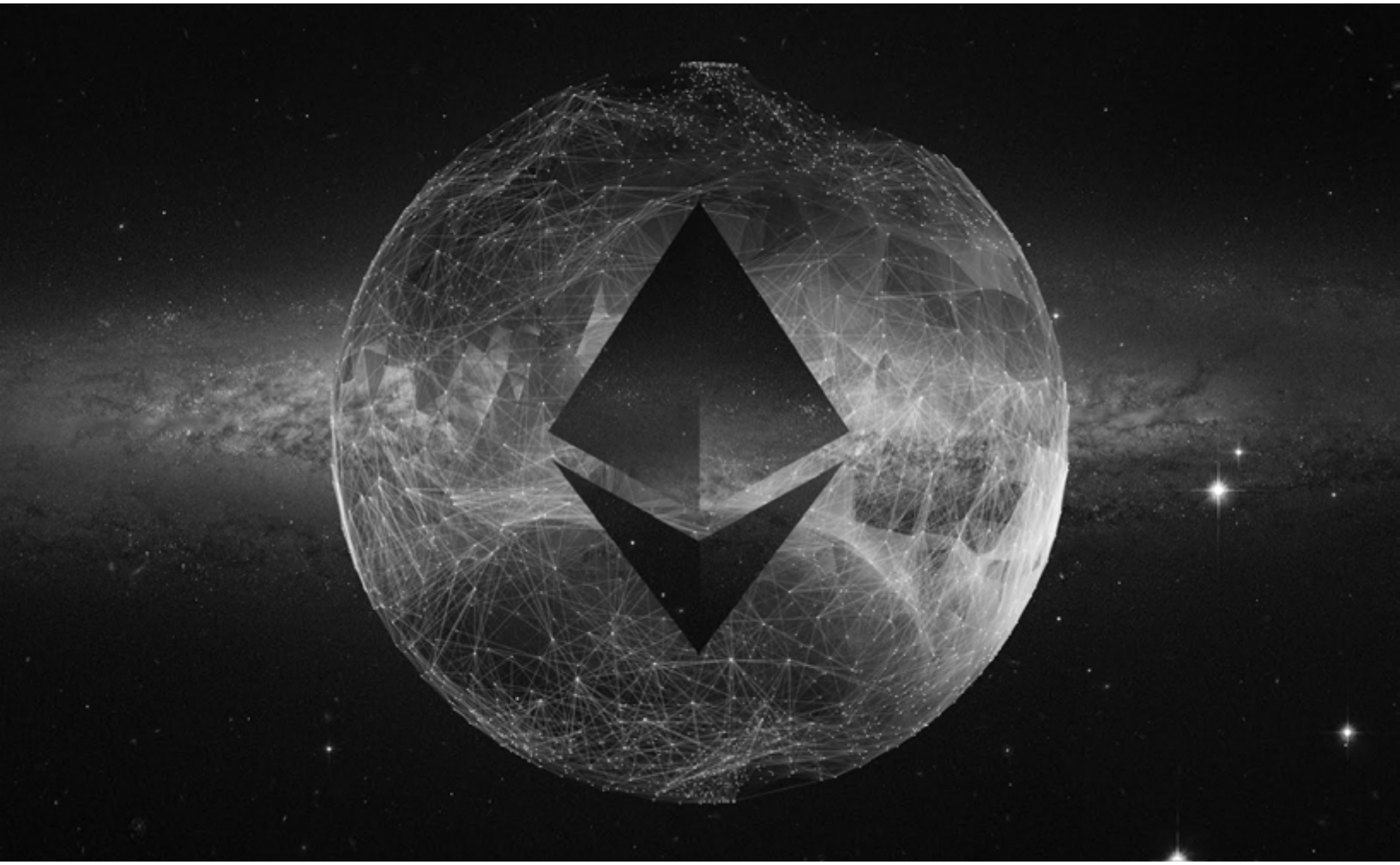
Consensus - As discussed above, consensus algorithms are far from perfect. The plan to solve the problem with blockchain-based proof-of-work (PoW) and random computation trees appears promising, but ultimately version 1.0 of a protocol of this form may well fail to bear the brunt of attacks in the long term. An ideal algorithm, one that is both socially cost-free or cost-negative and promotes a high level of decentralization and security, will likely require a combination of novel approaches such as transactions-as-PoS (proof-of-stake), delegated-PoS, useful PoW, next-generation centralization/ASIC-resistant PoW and maybe even more exotic strategies involving bandwidth and storage. Developing such an algorithm, and making sure that it actually works, is an important priority for securing the blockchains of tomorrow.

Privacy - Blockchains are known for their highly imperfect privacy properties, and the design of the Ethereum Platform as it stands today is admittedly not particularly effective in this regard. However, future developments to improve privacy, such as those based on SCIP/zk-SNARK, are around the corner, and some based on technologies such as CryptoNote and CoinJoin are here already.

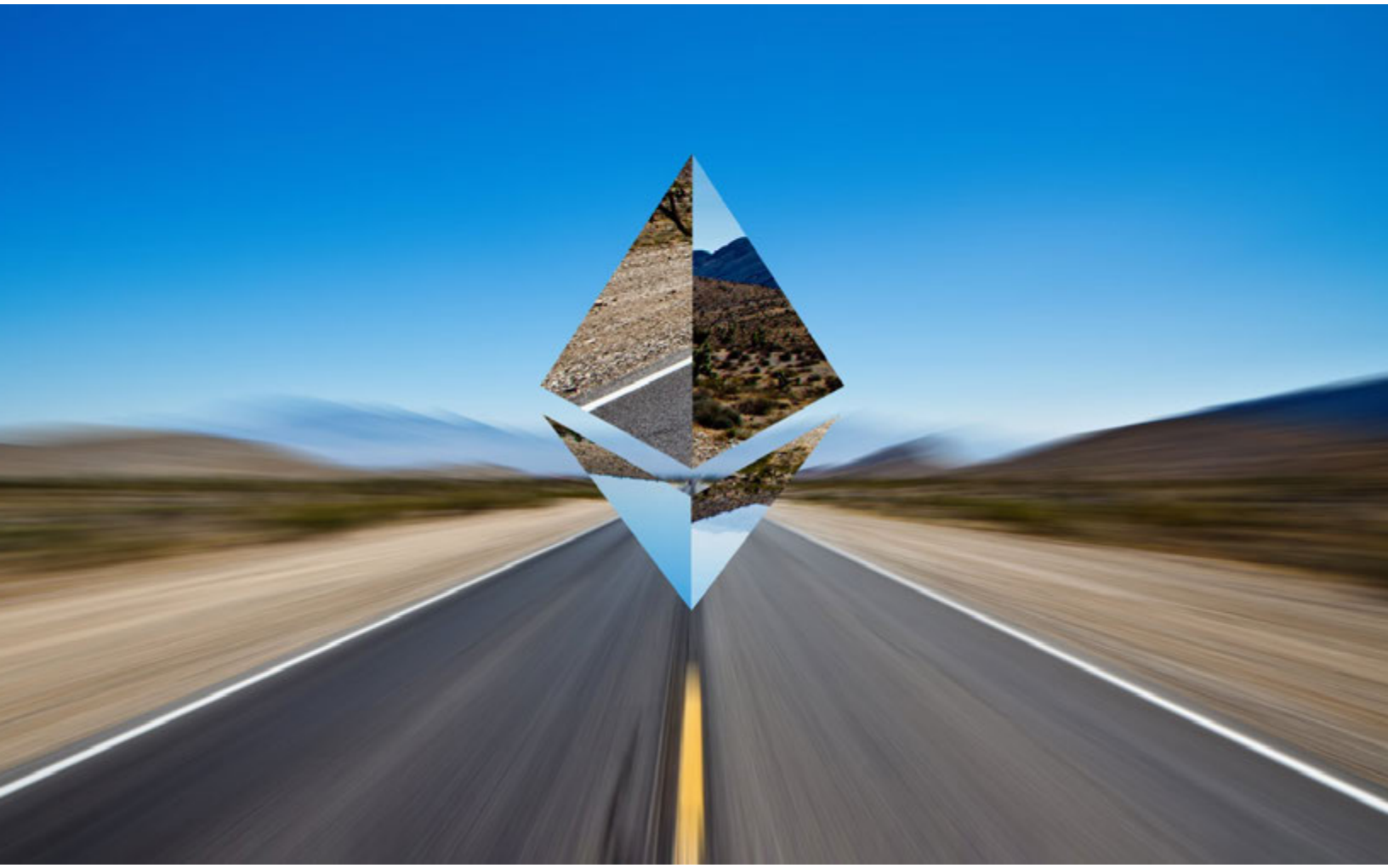
Language and development tool design - Another important sub-deliverable that emerged from early discussions and planning of the Ethereum Platform is the concept of a fully deterministic, computation-metered, state-hashed virtual machine with multiple fully interoperable implementations. The Ethereum Virtual Machine (EVM) is useful in both blockchains and other adversarial and resource-constrained environments, and will benefit from continued development in its own right. If multi-blockchain architectures become a dominant paradigm, the EVM may also need to be updated to handle situations such as asynchronicity. Aside from the EVM itself, there are the Serpent, LLL and Mutan high-level languages, and ĐΞV is beginning work on specialized development environments targeted to building decentralized applications.



Post-quantum cryptography - If quantum computers become widely available, then the elliptic curve signature algorithms that the Ethereum Platform relies on for signing transactions right now will be broken. However, there does exist a class of signature algorithms that is resistant to quantum computing attacks, the best known of which is the Lamport signature. The Lamport signature uses nothing but a hash algorithm in its construction, but it takes up kilobytes of space and is limited to one-time use. Improved strategies known as Merkle signing trees and hash ladders partially address these issues, but still not perfectly. The better these algorithms can get, however, the more one can be comfortable that quantum computing, when it comes, will not be a problem.



Moon-math cryptography - Right now, the most exciting developments in the science of pure cryptography center around three "holy grails." The first is fully homomorphic encryption: being able to run a function on encrypted data and get an encrypted result without knowing what the data is, allowing a near-total degree of privacy in cloud computing. The second is SCIP mentioned above, allowing for efficient and succinctly verifiable proofs that a particular long computation has a given result. Finally there is obfuscation: being able to run an encrypted function on data without knowing what the function is, which allows scripts with private data to be run on blockchains. Each of these problems have solutions in the early-to-mid stages of development, but the solutions currently have massive drawbacks in either efficiency or trust requirement. If solutions could be perfected or at least improved to the point of viability (SCIP is pretty close already), then cryptoeconomic protocols could potentially become much more powerful.



DAOification - One of the most exciting ideas for things that can be built on top of Ethereum is the concept of a decentralized autonomous organization (DAO). A traditional organization, whether corporate or nonprofit, is nothing more than a set of people, a set of resources and a set of rules governing how the people can use the resources. In a DAO, instead of being enforced in "meatspace" and the judicial system, those rules are enforced in a decentralized and transparent way on the blockchain; i.e. unlike a traditional modern multinational corporation, where there is intelligence at the core and automation at the periphery, in a DAO there is automation at the core and human intelligence at the periphery providing the creative inputs. The primary medium-term attractions of DAOs are (1) the dream of eliminating the hard distinction between employee, investor, customer and non-employee, allowing the DAO to facilitate more nuanced and dynamic relationships and take advantage of the entire power law curve of people's contributions, and (2) the ability to experiment with new organizational management mechanisms such as liquid democracy and futarchy. Eventually, the concepts of DAO, factory automaton and AI may even merge completely.

CCRG - In order to promote cryptocurrency research specifically, a body called the Cryptocurrency Research Group is being launched by ĐΞV and is in the early stages of development. Its activities in the fields of cryptography, cryptocurrency, economics, finance, law, politics and others, will be ramped up substantially over the next few months and it is anticipated that it will grow into a fully or largely autonomous organization which seeks funding from other groups in the cryptocurrency space, as well as tech companies and philanthropists. Separate bodies may be created for protocol development specifically. For a more complete view of what cryptocurrency research might entail, see the ongoing "Hard Problems of Cryptoeconomics" paper.

Self-Regulatory Organization - A perhaps unglamorous from a technical standpoint, but nonetheless important part of the general mission of achieving adoption of decentralized technologies is participating in legal processes, and helping to carve out a legal environment in which projects such as the Ethereum Platform, Đapps build on top of Ethereum and other cryptocurrency/decentralized web-related initiatives can safely thrive without undue restriction. One of the initiatives that the GmbH has undertaken, in collaboration with OpenTransactions, Bitcoin Suisse and others, is the development of a self-regulatory organization in its home country Switzerland for that very purpose. The GmbH is working closely with a local law firm with established experience in the formation of SROs, and a minimal SRO can be maintained for less than $100,000. Additional funding will enable the SRO to broaden its scope and influence, and in time allow these efforts to extend beyond Switzerland as well.

Other Projects

Of course, the above is only a guideline, and ĐΞV may choose not to pursue some of the above or to take on other projects beyond the above categories. Some specific possibilities include:



DAOification - Although DAOification will certainly be a primary cryptocurrency research focus, the long term plan was always to turn the different Ethereum organizations into DAOs, by building a long-term governance platform that can be used to continue research and development as a community-driven activity.

Conferences - ĐΞV may choose, whether unilaterally or in coordination with other groups in the industry, to organize conferences relating to the technological, legal and social possibilities of the decentralized web. Such conferences may be run either for-profit as a source of continuing revenue or on a non-profit, at-cost basis. Alongside conferences, there is also the possibility of developer-centric educational workshops.

Hubs - One idea that is popular in the Bitcoin community is the idea of creating specific Bitcoin hubs, facilities where Bitcoin users can work, potentially live, and interact. The Bitcoin Embassies in Montreal and Tel Aviv, Bitcoin Decentral in Toronto and the NYC Bitcoin Center are all prominent examples. ĐΞV may wish to assist in building more such centers as a community-building activity.

--