JEFFERSON
CAPITAL

DIGITAL ASSET WHITEPAPER

Digital Asset Whitepaper:

Part 1: The Scalability Trilemma
- a. Decentralization
- b. Security and Scalability

Part 2: Digital Asset Class Breakdown
- c. Currencies
  - i. Deflationary
  - ii. Stable/Crypto-fiat
  - iii. Anonymous
- d. DApps
  - i. Enterprise Blockchains
  - ii. Financial Services (Fintech)
  - iii. Vertical DApps
  - iv. Retail & Consumer DApps
- e. DApp Platforms
  - i. Smart Contracts
  - ii. Layer 1: Consensus Layers
  - iii. Layer 2: Side-Chains, Oracles, Parallel Consensus, and Off-Chain Protocols
  - iv. Centralization Vs. Decentralization Trade-Offs
- f. DAOs
  - i. Decentralized Banking
  - ii. Decentralized Decision-Making (Governance)
- g. Social/Cultural Rewards
  - i. Traditional Influence Economy: Social Media, Video Platforms, Advertisers
  - ii. Decentralized Incentives
  - iii. Examples
- h. Tokenized Assets
- i. Digital Collectibles

Part 3: The Jefferson Capital Outlook
- j. The Global Digital Asset Trade
- k. Immediate and Near-Term Outlook (6- to 18-month horizon)
  - i. Smart Contracts
  - ii. Vertical DApps
  - iii. Digital Collectibles
- l. Medium Term (2- to 4- year horizon)
  - i. Financial Services
  - ii. Enterprise Blockchains
  - iii. Centralized DApp Platforms
  - iv. Decentralized DApp Platforms (w/ Layer 2)
- m. Long Term (5+ year horizon)
  - i. Retail/Consumer DApps
  - ii. Crypto-Fiat Interoperability
  - iii. Social Rewards
  - iv. Sustainability
  - v. The first widely-adopted DAO

1. The Scalability Trilemma

Decentralization, Scalability, or Security: Pick two.

In brief, the Trilemma refers to the fact that networks in general (and distributed systems in particular) suffer from internal trust issues, proportionate to their size: The larger the size of any network, the greater the degrees of separation between its members and therefore the lower the level of trust. This problem can only be averted by either a) making it harder to join the network, reducing scalability; or b) delegating the responsibility (and associated privileges) of overseeing the network's activities to a handful of specialized nodes, sacrificing the inherent appeal of decentralization.

A secure and scalable system relies on some form of central authority. A secure and decentralized system grows to a ceiling, and a decentralized and scalable system is not trustworthy.

In any instance, it's impossible *not* to give up one of the three.

While not widely known outside of programming circles, the Scalability Trilemma is regarded as a hard law of computer science. It has been understandably absent from public awareness, but the advent of blockchain, and the ensuing investment craze that emerged from it, have made the Trilemma impossible to ignore.

The most important thing to note about blockchain is that it is a supply-side technology. This is to say that its value will be driven in the long-term by the rate at which the providers, not consumers, of goods, services, assets, securities, etc., choose to adopt it. Thus, a good investor must think like a producer: "Which blockchain network best suits the business/enterprise I'm pursuing, and why?"

These three features of a blockchain are all desirable within certain contexts. It is highly likely that, when this space reaches full maturity, multiple platforms will exist, with features that different industries prefer over others.

a. Decentralization (and Security)

Decentralization is by far the most controversial value-add of blockchain technology, and it can be argued that most of blockchain's use cases arise from the core fact of its capacity to be completely absent of central governance. Much like a free and open Internet has done for information, a decentralized blockchain invites creators, entrepreneurs and freelancers to connect and transact value without impediment and, potentially, without oversight.

On the one hand, a blockchain that boasts total decentralization—such as Bitcoin, or Ethereum—can be a problem for regulatory bodies. If there is no way to compel any users to adhere to any rules, then all attempts at even basic accounting will be symbolic at best. Even a basic law that says, for example, that all Bitcoin users in the US register their wallets with the IRS for tax reasons, would be completely unenforceable, so long as free access to online wallets exists. It is on this basis that regulators in many Asian nations have cut off access to Bitcoin-related websites in an attempt to ban Bitcoin altogether (also technically unenforceable, but to that end, so is the drug trade.)

On the other hand, the world is teeming with seemingly infinite programmers, sellers, and entrepreneurs who see decentralization as an opportunity to rewrite the rules of the economy. On a decentralized blockchain, it becomes possible to create an innovative app or produce controversial creative content without answering to a company or service provider. While scalability and security are important from an economic perspective, decentralization invites a brand new class of global economic activity, specifically, that which can only exist beyond the bounds of what companies, governments, and middlemen would typically allow.

Indeed, a blockchain built with decentralization as a core commandment can be thought of as appealing directly to this new class of economic activity.

In summary: Any business venture that doesn't mind operating within the existing social contract—between buyers and sellers adhering to a set of rules on one side, and middlemen with the power to change those rules at will on the other—will find scalability and security to be more important features than decentralization. Any venture that values the ability to write its own rules of conduct, and to trust that those rules will never be changed, will find decentralization indispensible and will gladly sacrifice one of the other two.

b. Security and Scalability

A blockchain provides the benefits of security like no other technology yet invented. By distributing the verification of all inputs across all nodes, the database guarantees the truth of its contents implicitly.

A blockchain network also makes it remarkably easy to scale a business, through automated administrative and accounting functions, and allowing organizations to bring on new members easily.

Eventually, however, one becomes an impediment to the other: Too many new members could lead to fragmented interests within the organization, and a steady erosion of trust. Putting rules in place to ensure cooperation would sacrifice the network's efficiency, and this effect would compound at scale.

In a decentralized network, trust is an obstacle to growth, and growth is an obstacle to trust.

There are obvious instances where one is preferable over the other. An energy microgrid, operating in a fixed grid size, would opt for security over scalability; a social network, in which user data is implicitly private and trust is a non-factor, would optimize scalability over security.

There are open-ended cases, however, in which competition for growth depends on user trust, and neither can afford to be sacrificed. When both security and scalability are necessary, how important is decentralization?

2. Digital Asset Class Breakdown

Depending on the asset class, how a given asset solves the stated Trilemma above becomes not only a determining factor in its viability, but defines its ability to compete with other assets in the same class.

While scalability would obviously seem the most important quality in any investment, there are instances where this is not the case. We examine these exceptions below.

a. Currencies

Digital currency was the first widely explored application of blockchain digital assets. Bitcoin is deflationary, which has helped to accelerate its adoption. Since then, a wide variety of other digital currencies have been attempted.

A blockchain-based currency has obvious advantages to users, who could in theory use it to move money quickly, reliably, and across borders. Accounts would be accessible from anywhere at any time, and there would be no banking fees.

We foresee an inevitable transition from traditional monetary policy into cryptocurrency. There is no scenario where a nation's economy can compete with that of the rest of the world without adopting cryptocurrency technology while the rest of the world does.

As this happens, exchanges of value from one currency to another will be easily mediated by exchange in a single global standard. That standard could be a digital asset representation of the global gold supply; or, it could be an entirely separate measure. Some projects anticipate this need and are developing digital assets that will be programmed to serve as an exchange currency, as well as a global reserve currency, to be used on the one hand as a means of facilitating global trade and expressing national monetary policies, and on the other hand, as a tool for keeping the global economy solvent.

This concept will be further expounded upon in 2d.

i. Deflationary

Like Bitcoin, some cryptocurrencies are deflationary, existing either in fixed supply or at a scarce growth rate. This creates artificial scarcity for the asset, allowing a single unit to represent more and more value as use of its network grows. The inherent appeal of a deflationary currency is in its early stages: The first adopters of a currency that later becomes widely used will find themselves rich. This is also the appeal of most pyramid schemes.

The fierce competition within this asset subclass has led to incredible innovations in transaction speed, and some have brought unique features.

None, however, have come close to the level of use of Bitcoin, whose supporters include virtually the entire "cryptocurrency" community, millions strong.

The Trilemma

Bitcoin was also the first decentralized program to run up against the Scalabiliy Trilemma. This happened more or less officially at the end of 2017, when transaction fees became inordinately high—for a time, as high as $30 for a $5 transaction. In the name of Security and Decentralization, Scalability had taken a blow.

Bitcoin's advantage in resolving this issue is the nature of Bitcoin Core, a volunteer organization of computer science experts, programmers, engineers, and enthusiasts constantly sharing ideas on how to improve the Bitcoin software. These ideas are then proposed to a forum where the Bitcoin network's validators can choose to accept them or not.

The solution proposed by the Bitcoin Core team was an innovative program called "Segregated Witness" or SegWit for short. This solution eliminated the requirement that all nodes
validate all transactions, instead designating subsets of nodes to serve as validators for subsets of transactions.

This solution is not *itself* scalable, however. Eventually, as the Bitcoin network grows, one imagines there would need to be another layer of delegated nodes, further consolidating the power of the network in a handful of nodes. It is not clear if the community will be prepared to solve this issue when it does arise.

However, as far as Bitcoin is concerned, these are good problems to have; no other deflationary digital currency is immediately concerned with reaching so many users, and all newer currencies hoping to compete with Bitcoin have thus far achieved little other than to give the Bitcoin community of developers and miners new ideas of how to adapt and improve the Bitcoin platform.

Conclusion

Bitcoin's community support is immense and shockingly well organized, giving it the maneuverability and momentum it needs to continue growing well into the future. We expect Bitcoin fever to increase, not decrease, in the short term, with a binary outcome for its continued viability in the longer term that should become clear in the medium term.

ii. Stable/Crypto-Fiat

Crypto-fiat is the inevitable outcome of the cryptocurrency industry. All cryptocurrencies invented by the community, even Bitcoin, serve, if nothing else, to demonstrate cryptocurrency's tremendous viability as a medium of exchange; as with the Internet, there is no doubt nations and central banks across the globe will hasten to adopt this technology in the issuance and internal accounting of their own currencies, as well.

Some startup ventures have already invented "stable" cryptocurrencies, backed by dollars that their organizations hold in a bank and used on online crypto exchanges seeking a convenient hedge against the market. However, these so-called

"stablecoins" carry with them the burden of trust: Users must have faith that the organization that administers them is actually solvent. USD Tether, for example, was at one point robbed, some undisclosed amount supposedly stolen from their bank account. They have since stopped accepting new users, while the supply of USDT currently in circulation on the market has not increased or decreased. In the long run, this coin and others like it may become decoupled from their real value due to unforeseen problems. Jefferson Capital does not hold any, as none of the current ventures that provide them seem solvent, and hedging our risk via cash holdings has served us just fine.

It is conceivable that a nation like South Korea soon issues a cryptocurrency controlled and audited by the government, and declares it legal tender within their country. Their incentives for doing so would include eliminating cash dealings, and keeping a close watch on their GDP to improve monetary policy. With the right features enabled, a national cryptocurrency would also allow the use of DApps or the purchase of tokenized assets.

This would increase the speed at which these DApps and digital assets are improved upon, as the available market for these assets would now include an entire nation.

The Trilemma:

The Trilemma does not apply to stablecoins, because they by definition are not decentralized. Security and Scalability are both easy in this case.

Conclusion:

A national cryptocurrency would introduce a flood of new users into the DApp and digital asset economies, and these innovations are without doubt taking place right now. Countries in East Asia are quick to adapt to new technologies and a national cryptocurrency in South Korea, Singapore, China, Japan, or Hong Kong within the year would not be out of the question.

iii. **Anonymous**

When Bitcoin was still widely misunderstood, it was often touted in the media as an untraceable currency, used by drug dealers and pedophiles in the darkest reaches of cyberspace.

This is in fact very nearly the opposite of the truth: Bitcoin keeps a permanent and detailed record of all transactions, and allows anyone to audit the cash flow of the entire Bitcoin economy from any point in history, all the way back to the very first BTC transaction in 2009.

The reason for the misconception is because a Bitcoin address is not *itself* tied to any name. Therefore, while participation in the Bitcoin network is always a public event, all of its addresses are anonymous by nature. This has been the point of interest for criminals and law enforcement alike. The challenge for both has been to establish (or hide) any possible links between a Bitcoin address and a person's identity. Once having done so, any regulator can use Bitcoin's inherently public ledger to immediately account for all of an individual's transactions.

In response to this, a community has formed around the desire for better anonymity. Anonymous currencies have expanded upon the notion of a blockchain-

based currency by adding features such as Zero-Knowledge Proofs and Ring Signatures, which enable users to transact value peer-to-peer without making anything about their transaction visible on the public blockchain.

Different anonymity coins accomplish this to varying degrees. Some encrypt the addresses of the sender and receiver, but publicize the balances being sent. Some encrypt everything including the transaction volume, as well as offer encrypted messaging services, VPN services and anonymous forums. Some simply mix transactions together, making users' balances untraceable yet publicly verifiable. Depending on the purpose of the transaction, as well as to what degree of oversight a regulatory body deems necessary, anonymous currencies may be desirable, tolerated, or not permitted at all.

They cannot, however, be regulated in and of themselves. They are inherently immune to censorship; a fact that we believe creates an entirely new subset of economics, as-yet unexplored.

b. **DApps**

Decentralized Applications, often called DApps, are the smart contract *coup de grâce,* the reason for all the blockchain hype. Ambitious startups have raised millions merely on the suggestion of building them. DApps with sound roadmaps have already found a first-mover advantage, signed partnerships and raised significant investments from extremely wealthy sponsors, corporations, and national governments. Lawyers, financial services brokers, and salesman of every kind stand to lose their income streams and be sent back to school, pending the arrival of the right kind of DApp.

DApps are also the building block of a new kind of consumer ecosystem, creating demand for completely new services and providing economic incentives that were simply impossible until now.

However, the major caveat to this is that, because so few people in the world are actually capable of programming a blockchain from scratch, the vast majority of DApps (whether sought by startups or legacy corporations) will have to be built on DApp platform infrastructure (as elaborated on in 2c). DApp platforms are still experimental in and of themselves, and while a successful DApp would take years to grow, it will take at least as long before any DApp platforms have shown the time-tested robustness necessary to appeal to more risk-averse investors. Only then will DApps have the chance to earn trust of their own, on a case-by-case basis

In general, a DApp creates an open and secure marketplace for a particular type of good or service. This makes the DApp token roughly representative of the good or service being traded. Variations to this theme are discussed below.

A note on the Trilemma:

DApps are purpose-built applications meant to solve specific problems or offer specific services. As such, there is no catch-all rule as to how a DApp should go about solving the Trilemma. Vertical DApps will likely opt to let go of the decentralization aspect in favor of security and scalability, but may find that a

decentralized competitor fares just as well in the long run. As the value provided by any two DApps in the same industry is essentially the same, the difference comes down to marketing, functionality, and consumer preference.

i. Enterprise Blockchains

ARK, Lisk, NULS, Microsoft Azure, IBM Workbench. These are all examples of services that anyone—individual, startup, or large corporation—can leverage to create their own DApp. They are to DApps what Wordpress and Wix are to websites.

There are vast differences in their design and scope: While the first three are themselves examples of DApps, whose use depends on their own native cryptocurrency, the latter two are enterprise solutions.

The former are used by purchasing a digital asset, which represents license to run a user's DApp on their blockchain, and a means of liquidating DApp token value across DApps on this blockchain. Thus, their platforms are more analogous to DApp platforms.

The latter are not DApps; they are Blockchain-as-a-Service (BaaS) business models, which collect subscriptions from users and add a new revenue stream to Microsoft and IBM.

Both are catalysts for the future growth of the DApp economy. We expect millions of DApps to eventually be created using enterprise blockchain services, just as tens of millions of websites have been created using Wordpress and Wix. We will watch the growth of this industry as an indicator of the growth of the DApp market as a whole.

ii. Financial Services (Fintech)

The range of financial services offered in the DApp economy is enormous, growing daily, and potentially far larger than the range of financial services offered in the traditional economy. This is because any exchange of value, verification, regulation, or even adjudication that takes place within the financial sector today can be accomplished with greater efficiency and perfect transparency on a blockchain. In addition, a blockchain allows for transfers of value to completely bypass many of the brokers and clearinghouses typically involved in large transactions, reducing margins for all involved.

Many DApps currently exist for daytrading cryptocurrency; it is not inconceivable that the most popular and innovative among them may be adapted for use in the legacy stock market (pending requisite approval from financial regulators).

Neither is it inconceivable that they may actually retain most of their value from simply continuing to operate in the digital asset market. This is for a simple yet devastating application of DApps in the financial sector, namely, the potential tokenization of any commodity or security. With the right paperwork, a private company could take itself public through a smart contract for selling tokens, which represent shares of the company. As a more complex example: Those same tokens could themselves license tokenholders to a smart contract that automatically pays

out dividends from the company's revenue. Such digital securities would have to be designed with the proper regulatory framework and built-in KYC/AML requirements for purchasers, which are as of now the only major hurdle to this becoming a reality. Some enterprising startups have built DApp templates with all the necessary built-in regulations, or "Smart Regulation," and are simply awaiting a stamp of approval from regulators.

A more simple and equally revolutionary form of digital asset in this sector would be the tokenization of an actual asset. A homeowner, for example, could issue tokens representing ownership of his or her home, which would license its buyers to timeshares of the house. In another example, tokens representing gold from a gold mine could be bought internationally and redeemed for actual gold.

The advantages of digital assets are plain. They can bring instant, global liquidity to illiquid assets, keep track of ownership rights and liability, and even verify the legality of any transaction.

This is a massive investment opportunity, one that will not be available to the average crypto-trader but only to the investor with the foresight to predict the next developments before they happen. Those with the capacity to monetize these new opportunities will race to be the first to do so, and thus the window in which to capitalize on these predictions will close fast.

iii. **Vertical DApps**

Because DApp platforms are still too nascent to support the widespread adoption of new DApps, especially DApps that would require massive hardware installations to run properly, many companies have taken the more direct route of simply providing Blockchain-as-a-Service packaged with all the requisite hardware of their service.

Many industries have been disrupted in the past year by Blockchain-based newcomers who adopt this strategy, supply chain management and energy distribution most notably among them.

Energy "microgrids," as they have come to be called, are springing up all over the world, from Europe to Africa, from Australia to the Caribbean. Combining cheap energy sources with "smart metering" and the ability to transfer and account for units of value on a blockchain, these microgrids represent a new competitive market for energy in which anyone with a generator or a solar panel can offer a cheaper alternative to the local state-regulated monopoly.

Some companies have opted to scale this approach to reach a global audience. While energy prices from location to location may vary, this can still be accomplished through a digital asset licensing system. In this system, energy producers must purchase a license, of which there are a fixed supply, in order to sell their energy over a local microgrid. Once the license is purchased, a producer then issues a commodity coin backed by one kilowatt of electricity, and sells these coins to their community at the local market price. As the producer market grows, smaller and smaller fractions of a license can be purchased instead of a full license, meaning that early holders of these licenses stand to profit by reselling them at a later date.

The company, meanwhile, makes no revenue on the buying and selling of licenses, which all takes place in the secondhand market. Their business model revolves strictly around building the physical infrastructure on which the grid operates; this is an example of a "Vertical" DApp.

The other most readily available example of a vertical DApp is in the supply chain sector. Several startups have developed blockchains for the purpose of shipping, tracking, and quality assurance. These blockchains reward participants with an economic incentive to be honest, and a means of allowing anyone to query anyone else in the chain. Once built, the blockchain itself ceases to be a source of revenue; instead, the startup then manufactures and sells the chips, barcodes and scanners that the blockchain requires.

Vertical DApps are, essentially, centralized businesses whose service is to provide access to a decentralized good or service. Their major advantage over other DApp startups is that they do not need to wait for the market to mature in order to start expanding today. Their major disadvantage is that, once the market finally does mature, they could find major competition from DApps that either do not share the same hardware requirements, or find ways to distribute these requirements. For example, a supply chain blockchain supported by a centralized chip manufacturer could not possibly compete with an open-source location services DApp, in which any locator device could potentially earn rewards for its users (truckers, distributors, farmers, etc).

iv. **Retail & Consumer DApps**

The final category of DApp is the broadest and most far-reaching. This category can be defined quite simply as any DApp built by a developer or startup enterprise by using a Platform (2c) or Enterprise Blockchain (as described above). Because these tools allow the less experience and not as well-funded ventures to bring their ideas to life, and because all peer-to-peer applications could (potentially) access a global marketplace of users, this category is where most of the market disruption that Blockchain enables will take place.

The obvious limitation to the growth of the retail DApp economy is the existence of a scalable and user-friendly DApp platform with a tenured trust. Many DApps have already been built using the Ethereum blockchain. Ethereum, however, has not yet proven that it can scale to the levels necessary to support more than a few DApps of even moderate size. Other platforms have set out to solve the problem of processing and transaction speeds by taking centralized approaches; this mean that, by extension any DApps built using their platform will be subject to whatever terms and conditions the builders have set forth. This, plus the fact that Ethereum has already had some years to demonstrate its security, is why Ethereum continues to gain more and more support among the developer community even while it remains the slowest platform currently available.

We will further detail this race in the next subsection, but for the purposes of this paragraph, the important takeaway is that consumer DApps which are not a) built on Enterprise blockchains, b) built to offer financial services, or c) built as part

of a BaaS vertical, will all depend on the outcome of the platform race, as defined below.

Anything that fits the above description and yet claims the potential to disrupt major industry within some definite time horizon is most likely a scam.

c. DApp Platforms

A DApp platform is any open-source network that supports and facilitates user creation of new digital assets.

In a world where Blockchain were as easy to program as http/ip, DApps would already be as common as websites and there would be no need for DApp Platforms.

As it is, too few people understand Blockchain technology well enough to even properly vet the technology behind a new DApp, let alone build DApps from scratch.

The DApp Platform—a class of blockchains that package the most complex aspects of Blockchain programming for any developer to build on top of (namely, the platform's consensus layer and its smart contract, along with any other features of its architecture) is a solution that allows new DApps to be built quickly and easily by the majority of developers, within the parameters allowed by the particular Platform they opt to use.

This works by allowing an open network of cloud computation providers (miners) to host the DApps created by other users of the network, earning rewards and fees.

However, because they can only be built by people who understand Blockchain technology, they run into the same vetting problem: Not enough people exist to effectively convince a majority of the world's programmers that these platforms can be trusted.

Nor should they: We believe longevity can only be proven by longevity.

After a critical period of time, successful DApp platforms will come to attract use by developers, and DApps will become as common as websites.

The economics of the DApp Platform have no precedent, but are straightforward enough: All require the use of their own native digital asset as a transaction fee, to be used by any DApp built on top of the platform.

DApps still have their own utility tokens, as described above, and those tokens represent the actual good or service being traded between DApp users. However, any transaction of the utility token will incur a transaction fee, payable in the platform token.

The platform token, meanwhile, corresponds only to the network use—the computational power being transacted between the DApp and the platform's nodes, for any given transaction.

Fees may be distributed among the network's miners, stakeholders, or both, depending on the platform's structure.

Here we will discuss the levels of variation that exist between the different platforms

i. **Smart Contracts**

The smart contract is the core selling point of any platform, the reason any developers would want to use it.

The smart contract is a self-executing line of code that automatically trades values between any two accounts upon meeting whatever requisite conditions its developers have set.

To build a smart contract from scratch would require building a blockchain to record its transactions, and then finding a substantial network of users to contribute to that blockchain's validation, as well as the computation required for all transactions. Platforms allow developers to skip all of these steps by providing the smart contract, as well as a blockchain network with a substantial of users, for developers to apply to any market sector in a one-size-fits-all schema.

The platform requires only that the contributors to their network are paid by the consumers of the network in the platform's native token—which is of fixed supply, and whose value, one anticipates, must increase with time, as more and more such payments are demanded.

From one platform to the next, smart contracts come equipped with certain features that make them more or less suited to specific tasks. NEM, for example, allows users to write smart contracts that pay to organizations, rather than to users. Bitcoin's new RSK layer allows users to specify any number of parties on either side of a transaction. However, the basic architecture of a smart contract is constant, and any seasoned developer can build whatever types of transactions they can imagine using even its most basic iteration, Ethereum.

There are two exceptions to this rule, and one further point of interest:

1. The EOS network's smart contract would allow the construction of DApps wherein consumers do not pay transaction fees, and fees are instead charged to the businesses/sellers making use of the network. This is not possible on other blockchains and gives EOS a possible advantage over other networks.
2. Likewise, the Matrix AI blockchain (part of China's Belt/Road initiative) plans to allow users to create smart contracts through voice commands, translating speech directly into smart contract code. If successful, this would mean maximum accessibility to smart contract language to anyone with an idea, dramatically increasing the volume of DApps in the world and giving China an immediate monopoly on most of the market. *If* successful

Aside from the above two exceptions, smart contract technology is a relative constant among all other platforms currently marketed for developers today.

A point of intense interest for Jefferson Capital is the prospect of smart contract interoperability. Today, each digital asset, once constructed, is forever locked in to a particular function by its associated smart contract, making any value it contains transaction-specific. However, it will soon be possible to create digital assets that serve multiple functions simultaneously, and execute different kinds of contracts.

In general, smart contracts are the engine driving the entire DApp economy; a platform that demonstrates some kind of unique innovation in this respect, especially any innovation at the level of the blockchain itself (i. e., that would be therefore impossible for the average developer to build from scratch on, say, Ethereum) stands to dominate the market.

ii. **Layer 1: The Consensus Layer**

This is the DNA of a blockchain network—the algorithm that determines everything from its security, to its transaction speed, to its capacity for growth and even the economic incentive of its users.

Proof-of-Work has been the dominant method for consensusing blockchains since it was first introduced by Bitcoin in 2009. Ethereum follows a Proof-of-Work model as well. It is not the best possible consensus layer one can create; it is simply the first, oldest, and as of now the only one with more than a two-year track-record of working properly.

Proof-of-Work allows contributing users (miners), whose computer perform computations for the network (work), to earn rewards and fees from other users proportionate to the amount of work they put in. In theory, this makes the network secure, decentralized, and scalable.

In practice, only two Proof-of-Work systems have ever reached a scale worth talking about—Bitcoin and Ethereum—and both ran into the same problem: A few organizations, devoting masses of computation power, now dominate the network's consensus layer, and now collect most of the rewards and fees.

In principle, this means for scalability to continue, decentralization must be sacrificed. For Bitcoin and Ethereum—whose *raison d'être* has always been decentralization—that was a failure.

Bitcoin's community found a temporary fix to this problem, by requiring that the largest miners' results be consistent with those of all other miners, and simultaneously raising rewards for smaller miners. Meanwhile, independent developers are working on Layer 2 solutions to this problem (more on that below).

Ethereum's founder, meanwhile, intends to create a Proof-of-Stake alternative to Ethereum.

Proof-of-Stake is another Consensus layer with a different economic incentive for its users. Rather than rewarding miners for work, the platform divides the workload evenly among all of its "stakeholders." Stakeholders can be anyone, and are paid rewards and fees proportionate to how much of the platform's digital asset they own. In this model, the platform asset holders become shareholders, and fees are paid out as dividends.

EOS and NEO are two examples of Proof-of-Stake networks. In EOS' case, the platform's workload is "delegated" to the 21 stakeholders with the most votes by other users, reflecting a kind of voter republic in which other stakeholders don't need to contribute any work of their own, but can still earn dividends from their stake. In NEO's case, all the work is done internally by the NEO Company, and holders still enjoy payouts.

One can clearly see how different consensus layers hold different implications for future valuation. In a Proof-of-Work platform, the platform asset is a guarantee of a particular service, namely, the right to use the platform's smart contract in a DApp. In a Proof-of-Stake platform, the platform asset is a security, representing fractional ownership of the platform, and are a guarantee of future payouts.

The security and the fees need not be represented by the same asset, either: In the case of EOS, they are one and the same token, whereas in the case of NEO, one asset represents the users' shares, and the other (called "GAS") is paid out from DApp fees to holders of NEO.

Proof-of-Stake is the preferred consensus mechanism for centralized platforms, for obvious reasons. However, it does not provide an effective incentive for users to put in more work for the network, like Proof-of-Work, and therefore does not leverage the network effect that a successful blockchain network must inevitably attain. In addition, securities on a blockchain are not a unique feature of PoS: Any developer with the right expertise can accomplish this on any blockchain for any particular use case. Making it a central feature of the consensus mechanism is not necessary, meaning that the only question to be answered is one of scale.

If solutions to the scaling problem of Proof-of-Work can be found in the second layer (more on that below), then it is feasible that a Proof-of-Work network could perform all the same functions as a Proof-of-Stake network, including the issuing of securities within DApps, if need be.

Proof-of-Work and Proof-of-Stake are only the first two kinds of consensus to be seriously discussed in this context. There is no good reason to believe they will be the last.

iii. Layer 2: Side-Chains, Oracles, Parallel Consensus, and Off-Chain Protocols

Layer 2 refers to any characteristic of the blockchain's confirmation process—including its input data, its validation method, and its outputs—that are not recorded on the blockchain itself.

Classifying all the different kinds of Layer 2 operations would be extremely time-consuming, so for the purposes of this whitepaper we explore the four that have the most impact on the Platform race as described above.

A **Sidechain** is a blockchain built to carry out the confirmation of another blockchain—the "main chain".

For example: Bitcoin's Layer 2 now features a side chain called RSK, or Rootstock. While Bitcoin's Layer 1 consensus only clocks ~6 transactions per

second alone, Rootstock is a high-speed blockchain, capable of confirming up to 1,000 Bitcoin transactions per day, and supposedly anywhere up to 200,000 by the end of 2018. It accomplishes this by recording Merkle Roots, instead of complete transaction data, and allowing users to turn Merkle Roots back into complete transaction data upon request.

Ethereum's sidechain, Loom Network, combines a high-speed Merkle Root confirmation blockchain (like RSK) with a decentralized marketplace for developers to sell toolkits, share ideas and teach one another how to program blockchains.

Sidechains are the most promising means by which a PoW platform could continue to grow without compromising decentralization or security.

An **Oracle** is a network that queries and records off-chain data to be used in other blockchains. Oracles typically reward users for sharing their data and allowing it to be traded/sold to users on other blockchains. An oracle can itself be a blockchain (XYO Network), or can be built in to an existing blockchain. Ripple (XRP) is currently building an oracle that can query data from existing bank ledgers.

Current oracles attempt to ensure the truth of their users' input data through a combination of third-party evaluation and economic disincentives for bad actors. True oracles without third-party mediation are a difficult problem to solve. Centralized or not, Oracles are a necessary stage in the evolution of blockchain economics towards accurately reflecting real-world transactions of value. They are the missing key that will allow all real-world value to be quantifiable on a blockchain.

Parallel Consensus refers to a variation of side-chain technology in which the main blockchain records not a linear chronology of transactions, but chunks of transactions computed in parallel, parsed out among the network's validators and submitted simultaneously. Ethereum's founder, Vitalik Buterin, proposed a version of this idea he called "sharding," and its pursuit has led to various independent innovations throughout the space. If successful, it could exponentially increase the amount of transactions per second that a traditional Proof-of-Work blockchain could execute.

Off-Chain Protocols refer to any computation that is performed off-chain, and whose result is recorded on-chain. Maximizing the amount of work that can be performed off-chain by one node conserves the amount of work that needs to be done by the other nodes on the blockchain. However, this is not practical to do with every single transaction, as the entire purpose of a blockchain is to provide indisputable proof of a transaction's validity, and off-chain information makes this impossible because it is essentially taken on faith.

Clever protocols that utilize off-chain information are ones in which off-chain validators can be checked for fraud, or otherwise have some kind of incentive to perform honestly. A good example of this is 0x, in which independent "relayers" can act as exchanges between parties transacting the tokens of different DApps. Relayers keep order books off-chain, while submitting only the results of final trades into the blockchain to be published. A relayer's popularity among users depends on his or her track record of honesty, and so in this particular scenario, an off-chain protocol makes sense because no rationally acting relayer would attempt to deceive

a network whose participants would know immediately if they were being cheated and would destroy his reputation as a consequence.

A non-example would be an off-chain protocol in which a business records revenue off-chain, and publishes only a quarterly report on the blockchain; there would be nothing in the blockchain proving where the revenue came from, rendering the information meaningless.

The realm of layer 2 is as diverse as the realm of Internet protocols, and becoming more so every day. Jefferson Capital believes that many of the core problems faced by blockchains at the consensus level, including DApp platforms, will be solved or are already being solved in layer 2.

A major point of interest for Jefferson Capital is the capacity of independent developers to create these layer 2 modifications on particular platforms. Specifically: A decentralized platform provides a far greater incentive for public innovation than does a centralized one.

iv. **Centralization vs. Decentralization Trade-Offs**

Decentralization can appear to exist on a spectrum, with some platforms being more decentralized than others. In our experience, and in our conversations with developers, blockchain programmers, and business owners seeking to migrate to a blockchain, we've discovered the opposite is true: Decentralization is a dichotomy—a 0 or a 1.

If a DApp platform is not truly and completely decentralized—that is, if it is not one in which no person, no entity and no group has the singular ability to monetize their creation—it has disqualified itself from the share of the market to whom decentralization is the singular focus.

On the other hand, to those for whom decentralization is not so important an issue, the choice is clear: Centralized platforms are faster, better, and more reliable.

There are obvious reasons that a developer might prefer decentralization—the chance to skirt regulations, for one thing—but there are some less obvious ones as well.

Chief among them is community. To the developers, it's not a choice between slower vs. faster transaction speeds. To the developers, it's a choice between receiving the support of a community of others just like you, all incentivized economically to assist one another's understanding of this technology and to support one another's projects (Ethereum); or receiving the support of a company, that may or may not promise to invest capital into your project—a project which, if it's a DApp, probably doesn't need much capital to begin with (EOS, NEO, Matrix).

This, however, is strictly the perspective of an independent developer—one who has a vested interest in keeping control over his or her creation, and who is as eager to learn new things, as he is to create. We concede that, while it can be argued this constitutes the vast majority of programmers in the world, it does not constitute the vast majority of *money* that will eventually be invested in the creation of DApps.

Established businesses, or new businesses seeking to adopt blockchain as a business model, would have no need of the developer community of the Ethereum

blockchain and have no incentive to help the Ethereum network grow. A centralized blockchain could provide them the speed and scalability they need to provide a suitable customer experience from day one.

Matrix AI is a good example of a blockchain seeking to fulfill this niche. As part of China's Belt/Road initiative, the Matrix blockchain will be used by businesses conducting international trade along China's new global infrastructure project. It will be used not only for any task involving recordkeeping (placing orders, shipment tracking, transparency of funds, ownership records, etc), but can even allow its computations to be leveraged for the creation and hosting of AI (Artificial Intelligence) programs.

One imagines healthcare data hosted on the Matrix blockchain, in which a computer network thousands of times more powerful than IBM's Watson crunches medical data provided by hospitals, clinicians and insurance companies to produce diagnoses with far more accuracy than has ever been seen before.

With visions like this in mind, the Matrix blockchain is centralized in the sense that the only nodes running on it are all state-of-the-art supercomputers with state-of-the-art processing units. We predict that Matrix will be the first of its kind, and other centralized blockchains will follow suit in major trade corridors around the world, hosting data for multinational corporations including banks, agriculture, pharmaceuticals and energy distribution.

We predict that Centralized blockchain platforms will be the means through which a large portion, if not the majority, of global GDP is transacted in a few years' time (more on that in the Outlook section of our whitepaper). However, in that time, most of the innovation in the blockchain space will be happening on the Decentralized blockchain platform of choice among the developer community, whether that be Ethereum or some future usurper. The reason for this is simply that, while centralization attracts financial capital, decentralization attracts intellectual and cultural capital. And it is the latter that will eventually produce disruptive DApps, of the Facebook- and Google-killing kind.

d. **DAOs**

The Decentralized Autonomous Organization (DAO) is a potential alternative business model in which there is no CEO, manager, or central board of directors; something only made possible with the use of smart contracts.

A DAO would incentivize its members through proportionate rewards for a set of specified actions.

Take, for example, a hypothetical supermarket run via a DAO. In this supermarket, money spent by customers is held in a smart contract, and automatically paid out to cover the store's expenses: Rent, electricity, water, inventory, etc. The remainder is allocated to the employees, and the structure of this payout is determined collectively.

Management decisions, such as whether to bring on new hires or fire someone, or whether to stock new inventory, could also be made collectively, with

employees in different roles carrying heavier or lighter votes. For example: Workers in the Deli could decide they need a new hire, and the DAO would calculate a new budget proposal for the rest of the store. The other departments could approve or deny the new budget, but if they deny, they must propose an effective alternative, which is eventually passed, because they can't deny the Deli workers the right to make their hire.

There are problems in any hypothetical scenario involving a DAO, simply because nothing like it has ever been successfully attempted before, especially via automated governance. For this reason, DAOs are currently the most heavily explored topic in the blockchain space, and Jefferson Capital believes it all but inevitable that a successful DAO of any kind can be designed and deployed in any industry as soon as both of the following points of contention are resolved: Decentralized Banking (Who manages the money, and how to decide if/when it should be deployed), and Decentralized Decision-Making (The right voting structure).

i. **Decentralized Banking**

Decentralized Banking exists in the form of Bitcoin: My money is mine, and the shared record can prove it. This is banking in the purest sense of the word, and more complicated financial architecture (loans, bonds, etc) can in theory be built around it. However, until an entire banking infrastructure exists on a blockchain—and not just exists, but also is accepted and used by major governments and financial institutions—we do not consider the question of decentralized banking resolved.

We envision a decentralized banking infrastructure that has the makings of a prototypical DAO, such that anyone with a smartphone can have access to global financial services, and anyone can borrow *or loan* money just as easily as they can call an uber.

As we perceive it, there are two reasons why this has not yet happened: 1. Blockchain-based media of exchange are deflationary, and therefore highly volatile, making any attempt at a stable financial infrastructure built around them laughable; and 2. No stable crypto-fiat asset has presented itself in such a way as to be easier, rather than harder, to use than traditional fiat currency.

We believe both of these problems are solvable immediately, and that a crypto-fiat asset can in fact be built that is not only easy to use, but carries inherent advantages to its use over an ordinary dollar, such as Smart Regulation—the ability to prevent itself from being spent in a manner not compliant with local regulations.

That, and a near-infinite range of other possible utilities, can be programmed into a decentralized banking blockchain already today. In this case, the process is held up not by technology, but by regulation—the time it takes for bureaucratic agencies to properly review and approve the use of cryptocurrencies in this fashion.

ii. **Decentralized Decision-Making (Governance)**

Decentralized Decision-Making is the technologically intensive piece of the puzzle to solve before a truly independent DAO can compete with an established corporation in the same industry.

The hard problems to solve include: How does a *growing* organization, with new members performing different roles, properly weight the opinions of all its members? How does it allow everyone to voice their opinion, without sacrificing speed and efficiency? And, if not all members' opinions are necessary for a given decision… Says who? And so on.

There is no way to give a timeline on when, or indeed if, these problems are ever solved.

Currently, developers at a project called DAOStack are compiling the collected works of the blockchain developer community on this subject and building an open-source template for decentralized voting structures, such that anyone will be able to build a safe, scalable, 100% decentralized governance model for their organization. It is their hope to have a "stack" of DAO templates completed by 2019, but given the difficulty of the problems they're dealing with, we deem this unlikely, and predict that, because of the problem of decentralized decision-making, a working DAO will not be technically possible for at least the next five years.

e. **Social/Cultural Rewards**

One of the properties of a blockchain digital asset is to commodify and create liquidity for things that would otherwise have remained illiquid. We will explore that in more detail in the next section (Tokenized Assets), but for the purposes of this section, it is important to accept that some abstract commodities—representing real-world value—have up till now remained relatively illiquid, and can suddenly now be quantified and traded in a global supply/demand market.

One of these abstract commodities—possibly the largest—is influence.

The age of Facebook, Instagram and Youtube has enabled people to monetize their ability to capture other users' attention. The means by which they monetize, however, are inefficient, permitting them to sell this influence only to a small market of a few potential buyers—big-name brands who pay hundreds of thousands of influencers at a time.

In other words, their influence is an illiquid commodity.

i. **Traditional Influencer Economy: Social Media, Video Platforms, Advertisers**

On Facebook, a user's data is crunched to create a profile of their likes & interests, their diet, their browsing habits, political beliefs, even their physical health. Advertisers then pay Facebook to direct their advertisements to the right people. A Facebook user or page that gains a large amount of followers has no direct

way to monetize their influence, except perhaps by offering adspace to other users, in the form of posts.

On Instagram, users with high numbers of followers can be paid by big-name brands for direct product placement.

On Snapchat, users can join Snapchat Premium in which members pay fees to view their content. Snapchat Premium fees are paid to Snapchat, and content providers are given a commission on views.

On Youtube, advertisers pay Youtube to direct ads in a model similar to that of Facebook, while Youtube splits that ad revenue in a 45/55 split with content creators.

Not a single one of the above models provides a clear avenue for content providers to make a business out of their content within the platform. Youtube comes close, allowing content providers to directly monetize on their views, but this model is still dominated by 1. A small market of advertisers who are only wiling to pay a fixed rate for adspace, and 2. A platform (owned by Google) who takes *half* of a content creator's revenue. As a result, only a small percentage of Youtubers actually make enough money to cover their rent.

ii. **Tokenized Influence**

In a tokenized influence model, users could sell "adspace" peer-to-peer with other users, in a liquid market where local businesses could market via local influencers, and content creators can negotiate their own prices at all levels of scale. "Adspace" is in quotations here because, while it's technically applicable, the broad range of uses for this commodity extends far beyond mere advertising. Content creators and influencers could selectively sell their influence to promote causes they agree with, artists they like, family members' business ventures, and so on. Likewise, average users could buy space from willing sellers to do the same.

Tokenized influence could even extend beyond content creators and into the realm of commenters and reviewers. A Facebook user whose comments routinely get above average appraisal could monetize their ability to uplift posts' visibility by commenting on them (Facebook's algorithms already do this secretly—if a user with a high rate of "Likes" on his or her comments "Likes" your comment, your comment will be prominently featured on other users' feeds). This capacity to uplift others' posts would be diminished if used too often, so users would have to lean on their natural ability to select posts that they believe will do well in future—keeping the natural selection process alive.

Finally, a blockchain-based alternative to existing social media would inherently mean data privacy for all users: User profiles would no longer be owned by Facebook and ads would no longer be directed toward users. User profiles would be purchased directly from the users themselves, again and again by every potential advertiser who wished to see them, and ads would be featured at the discretion of the content provider, in a competitive bidding war that now includes not just big-name multinational brands but a flood of capital from local businesses, small-time artists, and everything in between.

In summary, one envisions that by bringing liquidity to the illiquid influence market, blockchain-based social media alternatives will bring a dramatically different cultural undertone to the social media landscape. Content creators will begin to see these new alternatives as a means of making a real living for themselves while retaining the power to choose which products, businesses, causes or cultural phenomena to support. And personal data ownership will make it impossible for adspace buyers like Cambridge Analytica to target and exploit the psychological habits of Facebook's users.

f. **Tokenized Assets**

The logical extension of the principle described above, Tokenized Assets—that is to say, real-world assets with digital representations in the form of Blockchain-based digital assets, or "tokens" –will allow illiquid assets of any kind to reach maximum liquidity in a globally traded market. There is ample reading material available from Nasdaq, Reuters, Bloomberg, etc. about the possible effects on the economy of tokenizing assets. The key takeaway is this: a tokenized asset has far greater reach than a traditional asset, and while it will not ultimately have greater inherent value than the asset would otherwise have had, it can allow that value to be extracted in new and unprecedented ways. The precise details vary from one asset class to the next.

We at Jefferson Capital anticipate tokenization of assets to become the single most widespread use of digital asset technology, greater than DApps or DApp platforms (both of which can simply be thought of as a means for transacting unique tokenized assets). However, because analysis of a tokenized asset is not fundamentally different from analysis of a traditional asset, we propose that the true value-add of a tokenized asset is in that it provides access to the greater global digital asset trade, which we discuss in Section 3a.

g. **Digital Collectibles**

A Digital Collectible is the naked concept of a digital asset, stripped down to its most pure and raw essence: Something digital, and therefore not truly real, yet impossible to destroy, copy, edit, or alter in any way. Digital Collectibles of arbitrary purpose and functionality have been created and traded as though they were art. Most notably was one "Cryptokitty," a designer digital cat identified by its own digital asset, which found a buyer for $100,000.

While Jefferson Capital does not feign any interest in digital collectibles as a viable investment, they are nevertheless an important part of the digital economy. The Cryptokitty trade helped to kickstart the biggest bubble in Ethereum's history at the end of 2017, and so much metadata about Cryptokitties was being stored on the Ethereum blockchain that the entire network momentarily clogged, prompting

Ethereum's founder to begin seriously considering abandoning Ethereum's PoW consensus layer in favor of PoS (as described above, in 2cii). Thus, we will continue to monitor activity in the Digital Collectibles sphere, especially as it eventually begins to overlap with real-world collectibles, (antiques, fine art, etc) as we have no doubt it will.

3. The Jefferson Capital Outlook

a. The Global Digital Asset Trade

All tokenized assets, be they traditional assets, securities, DApp or DApp platform assets can be bought, sold, and traded at unprecedented levels of liquidity in exchange for cryptocurrency. These sales may take place privately, on national exchanges, or on global cryptocurrency exchanges. Together, the global trade of all tokenized assets can be thought of as the Global Digital Asset Trade.

Right now, Bitcoin and Ethereum represent the entirety of liquid wealth transacted in this global market, which trades less than 2000 different digital assets at unimpressive liquidity. However, there is no ceiling to the number of digital assets that can exist, or the number of buyers of assets, and no floor to how tight liquidity can be for any of them. The function of the Digital Asset Trade is to provide the same opportunities for every asset. As the volume of assets traded in the Global Digital Asset Trade increases, demand for cryptocurrency—specifically, Bitcoin and Ethereum—will necessarily follow.

We assume increased total wealth transacted in the digital asset market overall, leading to increased demand for BTC and ETH as a medium of exchange between these assets.

In particular, our time horizons for various asset classes are as follows:

b. Immediate and Near-Term Outlook (6- to 18-month horizon)

i. Smart Contracts

Smart contracts, even as they exist today, are already applicable to a wide variety of uses, especially in the Financial Services sector. Crowdfunding and venture capital have already proven to be ripe for smart contract disruption; we would include any transaction for which the good/service being traded, plus all the requisite data, can exist online: Securities payouts, trading bots, auditing services, identity protection, prediction markets, casinos, and so on. All of these can be represented via smart contract.

To be specific: we would caution against investing in any DApps that offer these smart contracts as a service, as we do not expect retail DApps to be viable for some time (more on that below), and are merely suggesting that many businesses will likely seek to incorporate smart contracts of this nature within their business models and internal operations. Therefore, we are not making any particular

investment suggestions; merely pointing out the availability of a technology for any entity to use, as they may like.

ii. Vertical DApps

Vertical DApps are, for our purposes, already in play. Businesses like VeChain and Power Ledger have already demonstrated the effectiveness of a strategy that involves providing Blockchain-as-a-Service for free, alongside another revenue stream. We foresee these companies, and others like them, enjoying a first-mover advantage everywhere they operate for at least the next 18 months, as it would take far longer for competing groups to rise to their current levels by building blockchains from scratch, yet we predict that in ~2 years, it is possible that new businesses could scale and become competitive quickly by building on Enterprise Blockchains.

iii. Digital Collectibles

As stated above: While Digital Collectibles are already being bought and sold at enormous margins, Jefferson Capital does not have any interest in pursuing this asset class as an investment in the Jefferson Fund.

c. Medium Term (2- to 4- year horizon)

i. Financial Services DApps

This subject was touched upon in section 3bi, where we indicated that DApps offering smart contracts in the financial services sector should not be taken seriously. This was for two reasons: 1. The technological infrastructure, i. e., a viable DApp platform that could support these DApps, does not yet exist; and 2. The SEC and CFTC are slow to act on allowing the use of these smart contracts, smart regulations, etc., in transacting financial instruments.

~2 years is our predicted time horizon for the development of a DApp platform with proven scalability and security and which regulatory agencies are prepared to trust—at least enough to begin allowing smart-contracts into the financial services sector. When this happens, it will be the indication needed for developers of financial services DApps to finally begin marketing working products to consumers—including smart-contract financial instruments that don't strictly trade cryptocurrencies. These DApps may exist today, but cannot be expected to reach their full growth potential until such time as is required for a platform, trusted by regulators and developers, to emerge.

ii. Enterprise Blockchains

These are those smart-contract-enabled blockchains that can be bought from Microsoft or IBM, and hosted by an open network of users. As Wordpress and Wix were to the Internet, these will be to Blockchain: a means by which less experienced developers can bring ideas to life in crude-but-effective fashion.

There is technically no reason these could not become popular today, but it is our opinion that blockchain-based business models need a proof of concept (possibly in the form of a Vertical DApp that exists today) before the public really gets behind the idea.

2 to 3 years is our time horizon for a trending wave of blockchain-based business models to emerge using Enterprise Blockchains as a base. We do not consider this to impact the other digital asset classes in any substantial way; it will be more significant for the internal operations of various businesses than anything else.

While many people will use these to create DApps, with digital assets of their own, none of them will necessarily scale any better than any other blockchain built from scratch. There is nothing fundamentally different about a DApp built on an Enterprise Blockchain or one built from scratch, and both lack the advantage of being built on an established Platform (with users, scalability, security, etc)—we give all the same time horizon before they are viable investments, **~5 years**, as explained below.

iii. Centralized DApp Platforms

We predict more than 50% of global trade will be ledgered across various Centralized DApp Platforms within 4 years—**before 2023.**

Our reasoning stems directly from the scalability Trilemma as described in section 1, and again in 2civ.

In addition, we make three assumptions:

First, we assume that, for every transaction that involves value moving across borders (i. e. changing hands from one nation to another), a blockchain smart contract would be in every way preferable to the manual verification processes and redundant paperwork currently involved.

Second, we assume that centralized platforms will be preferred among business that already exist, and for whom allowing a third-party to manage and maintain a blockchain to ensure that all international transactions therein remain in compliance with any applicable trade laws would be a step up from their current workload and would be welcomed as a convenience, not an impediment.

And third, we assume that the third parties behind these centralized platforms will implicitly accept the responsibility and liability for any non-compliant activity within their networks, and that this responsibility will drive them to build highly regulated and highly secure networks which will at the same time continue to perform at orders of magnitude higher volume and speed than decentralized platforms for the foreseeable future.

Given these three assumptions, and the inherent advantages to scalability, security and compliance that a centralized managing body entails, the centralized

DApp platform becomes the ideal solution for any business seeking to grow and gain access to a global market for their products, while cutting operating costs.

Right now, centralized DApp platforms exist in a highly competitive way, in which companies and national governments alike immediately recognize faster and more sophisticated platforms. Partnerships and seed investors have thus clustered around a few promising projects, which already use the best technology currently available.

There are thus only two possibilities in the short-to-medium term: 1. Either this first-mover advantage for these projects continues, allowing the favored projects of today to set a standard for other centralized platforms going forward in the near future, or 2. One or more projects that are substantially more innovative in some regard are invented, attracting the partnerships and seed capital that would previously have gone to the favored projects of today.

In either scenario, the eventual widespread adoption of centralized DApp platforms by big businesses and national interests becomes more, not less, likely over time.

We fully expect that, given current levels of investment and the rate of progress in this sector, it should take no more than 4 years for that adoption to tip into a majority.

iv. Decentralized DApp Platforms (w/ Layer 2)

While big businesses and national governments don't mind a third party managing the speed and security of their blockchain platform—and in fact, would feel safer with a third-party to take on some liability in the event of a mistake or crime committed against them—there is an underrepresented sector of the global economy for whom a decentralized blockchain economy would be a major point of interest.

Take, for example, the social media industry. More broadly, include in this example any web platform whose business model is built around monetizing the interactions of users—especially those in which the company itself produces and directly sells precisely nothing: Youtube, Facebook, Twitter, Instagram and Snapchat are all perfect examples.

While the above companies allow their consumers to access their hosted content for free, the content creators have, for years, also operated on a completely voluntary basis. It wasn't until the 2010's that Youtube ads became common, and content creators were given a share of ad revenue; Snapchat recently began featuring Snapchat Premium, in which popular users can choose to allow snapchat to sell their content for a commission; Instagram models are directly hired by big-name brands for product placement; Twitter and Facebook do not, as of yet, feature any way for creators to directly monetize their activities, but still use creators and influencers as vehicles to target ads to other users.

A decentralized network could easily disrupt any of the above companies' revenue streams by distributing ad revenue amongst all users from whom advertising revenue is produced. In effect, this scenario means that the hegemonic

ad-generating business models favored by Youtube and Facebook will fall out of favor, giving way to a perfectly liquid supply-and-demand commodity trade of user data in which content creators choose to sell (or not sell) their own advertising space.

A centralized DApp platform could theoretically enable this, but could also theoretically choose to monetize ad revenue at any point in the future, a fact which one would assume most content creators would take into consideration. Only a perfectly decentralized DApp platform guarantees creators a proportionate share of rewards for their work.

We cite the evolution of this industry as one example of how the emerging global Internet culture would be easily incentivized to migrate a significant proportion of its economic activity onto a decentralized blockchain platform, were one readily available.

We predict that the below will be possible in less than four years:

- A decentralized DApp platform, with enthusiastic support from a global developer community, will make a breakthrough in scalability that allows it to rival centralized DApp platforms of today insofar as transaction speed and uptime.
- Developers on this DApp platform will have had time to perfect a theoretical ecosystem of DApps, targeted towards specific industries in which the community most desires to see disruption
- Regulatory bodies in many nations, anticipating the use of decentralized platforms for illicit (or merely unregulated) activity, will seek to strictly limit the ability of DApps built on this platform to affect their economies and drastically narrow the viability of these DApps into a select few industries
- DApps of every kind, black, white, and grey area, will continue to flourish in this ecosystem regardless of attempted regulation, which users and developers alike will simply ignore and which in fact are only effective in restricting the activities of centralized DApps, because no one need publicize their actions. A nation would, in theory, face a choice between turning a selective blind eye to the actions of its citizens on this network, or blocking access to its use entirely via a dramatic restriction of Internet freedom.

The Decentralized DApp platform asset itself would increase in value as sections of the global economy migrated to it, just as in the Centralized DApp platform asset class.

The difference can be summarized as follows:

Centralized DApp platforms have direct appeal to big business, and many of them will be competing in the coming years to acquire chunks of this trade, and all will be managed by entities (or nations, in some cases) who can be held directly responsible for allowing violations of international trade law committed by the actors on their networks. Their assets will together constitute an asset class, which

will grow even as one or more assets within the asset class struggle or fail to compete.

Decentralized DApp platforms, on the other hand, do not appeal to big business, and instead attract the economic activity reflected in global popular culture. These platforms do not compete, and instead tend towards assimilating one another. One imagines that a single asset will emerge that will define this class and come to be regarded globally as "the" decentralized DApp platform, whose network includes the entirety of global cultural exchange, in much the same way as Facebook is "the" social network and Google "the" search engine: a decentralized DApp platform with enough scalability could disrupt them all.

d. Long Term (5+ year horizon)

Note: The Long Term outlook can be better thought of as the category of investments that depend on a viable decentralized DApp platform. In other words, we submit that it will take no less than five years for all of the below asset classes to become tenable investments.

i. Retail/Consumer DApps

DApps created by amateur developers should eventually constitute the majority of DApps in existence. This, however, is impossible unless these developers are given the means to do so—means that they can actually trust.

We anticipate that in the long term, this will be the case, due to the reasons stated above: a competitive field of centralized DApp platforms, in which funding and market liquidity are promised from day one, and a growing community of enthusiastic developers pooling the world's sum of intellectual resources into make decentralized DApp platforms equally viable.

While the former already exists, regulatory points in every nation need to be fine-tuned before retail DApps can be coherently designed and deployed on these platforms without the risk of being banned or failing to find investors due to regulatory uncertainty.

And while the latter allows developers a way to circumvent regulatory uncertainty (due to the nature of decentralized DApp platforms, in which no users need publish their identities and no central authority bears the responsibility), technical points need to be hammered out by the community-at-large before these platforms can even support DApps.

Therefore, we expect that in either case, it will take at minimum five years before DApp tokens can be realistically bought and sold at retail or utilized by the average consumer.

ii. Crypto-Fiat Interoperability

This is not so much an asset class as it is a relevant technological breakthrough, one which could massively impact the existing market for every other digital asset class, for better or worse:

As mentioned above, regulatory points regarding the nature of digital assets and their classification as asset classes for investors still need to be fleshed out in more detail. We expect at minimum five years before there is enough understanding and comfort with this new technology globally, such that international transactions are possible and even common.

When this happens, we are *certain* that crypto-fiat interoperability will immediately follow. That is to say: Once a national regulatory body is comfortable and secure in allowing their national currency to be used in the purchase and sale of digital assets, it is no question that the nation will then move forward in integrating their national currency itself with this technology.

This means:

- A Federal Reserve-issued cryptocurrency ("cryptodollars?" "Fedcoin?") Featuring smart regulation, smart taxes and smart fines
- An app (or DApp) in which users can directly exchange their national currency for select digital assets, depending on their restrictions as investors OR a means of integrating the functionality of other digital assets directly into the national currency's functionality.
- An explorer in which regulators and auditors can track the transactions of all users

This second point is of the most interest: If all citizens of a nation now have access to a national cryptocurrency, and if this cryptocurrency comes equipped with a means of exchange across other digital assets, this means that digital assets in every sector can now be instantaneously bought and sold by anyone. This would be remarkably easy for the cryptocurrency's designers to implement, and would give a tremendous boost to any nation's GDP.

The important detail is whether the designers choose to construct the currency in this way, or opt for the more difficult (but even more advantageous and power-consolidating) route of enabling their national currency to do all the things that all other digital assets can do. They could achieve this by steadily adding updates with new features, and subsequently banning the use of digital assets that compete with the national currency. We do not predict they would do this, because to do so would be to isolate the national economy from the steadily growing global digital asset trade, analogous to isolating one's citizens from the Internet in the 1990's.

We would put the development of a national cryptocurrency for any given nation at a point in the timeline immediately after the complete codification of digital asset trade regulation for that nation.

iii. Social Rewards

This asset class was briefly discussed in the above page re: Decentralized DApp platforms and the possible disruption they could cause.

To elaborate further:

One imagines that, in a decentralized social media platform, any user has complete autonomy over the spaces on their page that display advertisements. That is to say: Imagine two users visiting a content creator's page, and this page features a space for an ad. Rather than one user seeing one ad, and another user seeing another ad (as would be the case on Facebook, which personalizes ads through data mining), the creator in this scenario would rent out this space to one or several companies, and the users would see one of so many ads, on a rotating basis, each time they reload the page. The creator would be compensated any time their users click the ads.

The appeal of this to a content creator goes without saying: They monetize 100% of the ad revenue they generate, as opposed to receiving none of it. Alternatively, since creators on Facebook are currently quite accustomed to receiving no revenue, they could choose to use the ad space in any other way they please: Promoting a cause they like. Preferring ads by businesses they favor. Etc.

Because the growth of such a platform would be driven entirely by the migration of content creators, one must imagine that the users themselves would move to where their favorite creators have gone. They would not do so if it were not free. A 100% decentralized network in which users must pay transaction fees to use the network's features would not be appealing. Therefore, the network in question must be 100% decentralized *and* 100% free of transaction fees, while remaining secure and scalable. This is perhaps the most difficult question in blockchain today; the answer may look something like a model in which users are rewarded for uplifting new content creators, and creators are rewarded for producing popular content—not only through direct sale of adspace, but through periodic distribution a native asset token, which can be used to purchase ad space and is gifted to new users. Some prototype blockchain social networks are experimenting with variations of this idea as we speak.

None will be viable before the questions of decentralized DApp scalability have been answered—which, as stated several times above, we predict will take at minimum five years.