



The Convergence Ecosystem

Convergence 2.0
Building the Decentralised Future

Disclaimer

This document (the "Document") has been prepared by Outlier Ventures Operations Limited ("Outlier Ventures"). Outlier Ventures Operations Ltd is registered in England and Wales, company registration number 10722638. Outlier Ventures Operations Ltd is an appointed representative of Sapia Partners LLP ("Sapia") which is authorised and regulated by the Financial Conduct Authority (Firm Reference Number 550103).

No undertaking, warranty or other assurance is given, and none should be implied, as to, and no reliance should be placed on, the accuracy, completeness or fairness of the information or opinions contained in this Document. The information contained in the Document is not subject to completion, alteration and verification nor should it be assumed that the information in the Document will be updated. The information contained in the Document has not been verified by Sapia, Outlier Ventures or any of its associates or affiliates.

The Document should not be considered a recommendation by Sapia, Outlier Ventures or any of its directors, officers, employees, agents or advisers in connection with any purchase of or subscription for securities. Recipients should not construe the contents of this Document as legal, tax, regulatory, financial or accounting advice and are urged to consult with their own advisers in relation to such matters. The information contained in the Document has been prepared purely for informational purposes. In all cases persons should conduct their own investigation and analysis of the data in the Document. The information contained in the Document has not been approved by the Financial Conduct Authority. This Document does not constitute, or form part of, any offer of, or invitation to apply for, securities nor shall it, or the fact of its distribution, form the basis of or be relied upon in connection with any contract or commitment to acquire any securities.

Any forecasts, opinions, estimates and projections contained in the Document constitute the judgement of Outlier Ventures and are provided for illustrative purposes only. Such forecasts, opinions, estimates and projections involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by such forecasts, opinions, estimates and projections. Accordingly no warrant (express or implied) is or will be made or given in relation to, and (except in the case of wilful fraud) no responsibility or liability is or will be accepted by Sapia, Outlier Ventures or any of its directors, officers, employees, agents or advisers in respect of, such forecasts, opinions, estimates and projections or their achievement or reasonableness. Recipients of the Document must determine for themselves the reliance (if any) that they should place on such forecasts, opinions, estimates and projections.

Information contained in the Document may not be distributed, published or reproduced in whole or in part or disclosed to any other person. The distribution of any document provided at or in connection with the Document in jurisdictions other than the United Kingdom may be restricted by law and therefore persons into whose possession any such documents may come should inform themselves about and observe any such restrictions.

Foreword by Jamie Burke CEO



Since we released our first 1.0 white-paper on the subject in late 2016 we continue to see 'convergence' evidenced all around us. As predicted, deep tech communities are beginning to adopt distributed ledgers to scale securely and more recently utilise innovations in cryptoassets as a digital commodities layer to power the mass coordination of decentralised networks.

Ultimately this means a more open source, resilient and less fragile Web as we shift away from the closed proprietary systems and data silos of the past. From where 90% would fail and disappear forever to something that is more biological in nature. Something that evolves in multiple, potentially parallel, iterations. This is an infinitely more efficient, effective and sustainable way to finance innovation and for the first time offers a highly profitable, but also potentially more equitable, business model for open source.

Furthermore, cryptoassets allow us to hardcode fiscal and monetary policies, as well as behavioural economics and game theory, to govern these new digital economies. In theory they can become more rational and orderly however we only need to look at existing financial markets and the impacts of algorithms to understand there are many risks and challenges to overcome.

This will likely become the greatest period of socio-economic experimentation humanity has ever seen, bringing about leaps in technology, economics and governance models. However it is important we are both cautious and critical to avoid building utopias.

This also makes convergence perhaps the most challenging investment strategy to execute upon precisely because of the range of increasingly complex and interdependent technologies and innovations. Each a life-time's area of specialism in its own right. As great as our growing team at Outlier Ventures is how can any one group of people possibly predict it's future? That's why we continue to open up our thinking so it can be shared, discussed and improved upon, with your help.

So we invite you to join us in a number of initiatives. Starting with an open slack community that can be found at <https://outlierventures.io/community> and culminating into an ambitious annual conference to bring together convergence startups (including those from our own portfolio), developers, academic and corporate partners. I look forward to seeing you there!

Jamie Burke
Founder and CEO



Lawrence Lundy
lawrence@outlierventures.io

Authors

Lawrence Lundy

Lead Author
& Head of Research

Joel John

Analyst

Harry McLaverty

Analyst

Shaquile Noor

Research Intern

Contributors

Jamie Burke

CEO & Founder,
Outlier Ventures

Aron van Ammers

CTO &
Founding Partner,
Outlier Ventures

Eden Dhaliwal

Head of
Cryptoeconomics,
Outlier Ventures

Matt Law

Head of Marketing,
Outlier Ventures

Anesu Machoko

Associate,
Outlier Ventures

Geoff LeFevre

Analyst,
Outlier Ventures

Special Thanks

Dele Atanda

CEO, Metâme Labs

Chris Burniske

Partner, Placeholder.
vc & Author of
Cryptoassets

Dr Rose Chan

Founder, Ladyboss.
world & Founder Head
of Blockchain Working
Group, World Bank

Professor

David Lee Kuo Chuen

Professor, FinTech &
Blockchain, Singapore
University of Social
Science

Matt Chwierut

Director of Research,
Smith + Crown

Dr Anne Hsu

Assistant Professor,
Department of
Computer Science,
Queen Mary University

Dr Stylianos Kampakis

Research Fellow, UCL
Centre for Blockchain
Technology

Samuel Klein

Fellow, Berkman Centre
for Internet & Society at
Harvard University

Professor

William Knottenbelt

Director, Imperial
College Centre for
Cryptocurrency
Research and
Engineering

Dr Robert M. Learney

Lead Technologist
Blockchain & DLT,
Digital Catapult

Trent McConaghy

Co-founder,
BigChainDB & Ocean
Protocol

Mark Stephen

Meadows
CEO & Founder,
Botanic Technologies
& SEED

Teemu Paivinen

Founder, Equilibrium
Labs & Author of Thin
Protocols

Samuli Poyhtari

Founder, OrbitDB &
Haja Networks

Drummond Reed

Chief Trust Officer,
Evernym

Toby Simpson

Co-founder, Fetch.AI

Dr Phillip J. Windley

Chairman, Sovrin

Contents

04	Disclaimer
06	Foreword by Jamie Burke, CEO
10	About Outlier Ventures
11	Introduction
15	Tokens, Communities & Governance
15	Tokens
19	Communities & Governance
21	Data Collection
22	The Internet of Things
23	Software
26	Authenticate, Validate & Secure
26	Distributed Ledgers & Blockchains
27	Consensus
29	Identity & Reputation
31	Storage & Data Integrity
34	Transport
34	Messaging
35	Value Interoperability (On-chain)
37	Data Interoperability (Off-chain)
38	State Communication
41	Marketplaces
41	IoT Data Marketplaces
43	AI Data Marketplaces
45	Personal Data Marketplaces
47	Digital Assets Marketplaces
50	Process, Analyse & Automate
50	Distributed Computation
51	Smart Contracts
53	Decentralised Machine Learning
55	Conclusion
59	Further Reading

About Outlier Ventures

Venture
Capital for the
decentralised
future

We invest and
partner with the
communities
that will create
the new
decentralised
economy

Founded in 2014, Outlier Ventures is a venture platform focused on building the infrastructure for the next phase of the Internet. Our investment philosophy is based around the idea of the Convergence Ecosystem. We view blockchains and other decentralised tools like tokens as a new data layer enabling other technologies like AI and IoT to combine and converge.

We partner with remarkable teams to seed and grow tokenised open source communities that will become the digital economies of tomorrow. Our team of experts build momentum in the projects, and ensure these economies are sustainable and equitable for all their stakeholders for a better Internet.

Introduction

The Convergence Ecosystem: Open-source. Distributed. Decentralised. Automated. Tokenised.

Our Journey

Back in late 2016, we published a paper titled: 'Blockchain-enabled Convergence' outlining the Outlier Ventures investment strategy. This paper was the result of over a year of research and over three years' experience investing and building blockchain-based businesses. Our insight was that blockchains are not just the technological foundations for Bitcoin and other cryptocurrencies; they aren't even limited to a new type of trusted recordkeeping for digital assets.

We asserted that blockchains and the broader set of distributed ledger technologies represented something more profound and transformative: the beginning of a new decentralised data infrastructure. Infrastructure that had the potential to solve technological and market problems across a range of emerging technologies like artificial intelligence, autonomous robotics, the Internet of Things, 3D printing and augmented and virtual reality. These technologies all face a common core problem: data centralisation. Data centralisation leads to a host of issues from lack of robustness, lack of verifiable audit trail, lack of transparency and opportunity for censorship.

An even more pernicious problem is the market dominance that flows from data ownership in digital markets. Ownership of data is power. As software goes on to eat the world - ever more data is being captured, stored, analysed and used to make decisions about every aspect of our lives. The Internet of Things will collect ever greater amounts of data allowing artificial intelligence to interpret and automate it. As laggard industries like healthcare, education and energy

come online - the existing centralised digital infrastructure will no longer do. From a societal and competitive perspective, we cannot let a few select companies own all the World's data. It is under these conditions where open blockchains and decentralised technologies come in. So we started investing.

Over the last year we have partnered with and invested in IOTA, a foundation building Internet of Things infrastructure with a new type of decentralised data structure. Botanic and the SEED Vault foundation it founded, creating a platform for developers to publish trusted software bots. Evernym, a company using the Sovrin Network and Protocol to establish self-sovereign identity. Fetch, a startup building an emergent intelligence protocol combining distributed ledgers with machine learning. And most recently, Ocean Protocol, who are developing a decentralised data exchange protocol to unlock data for AI. Each of these investments are a complimentary piece of decentralised infrastructure.

2017 saw a vast change in the cryptocurrency and blockchain markets to arguably the peak of inflated expectations. The ERC20 smart contract industrialised the token sale crowdfunding model raising over 4 billion dollars in funding. So-called 'ICOs' or token sales captured the attention of everyone in the industry and diverted valuable time and energy away from the real goal of building decentralised data infrastructure. Price, security-tokens, bull runs and scams replaced more critical technical questions around scalability, energy efficiency, and smart contract tooling. That said, it is now clear, in a way that wasn't in late 2016, that crypto-tokens are a critical missing

The Convergence Ecosystem

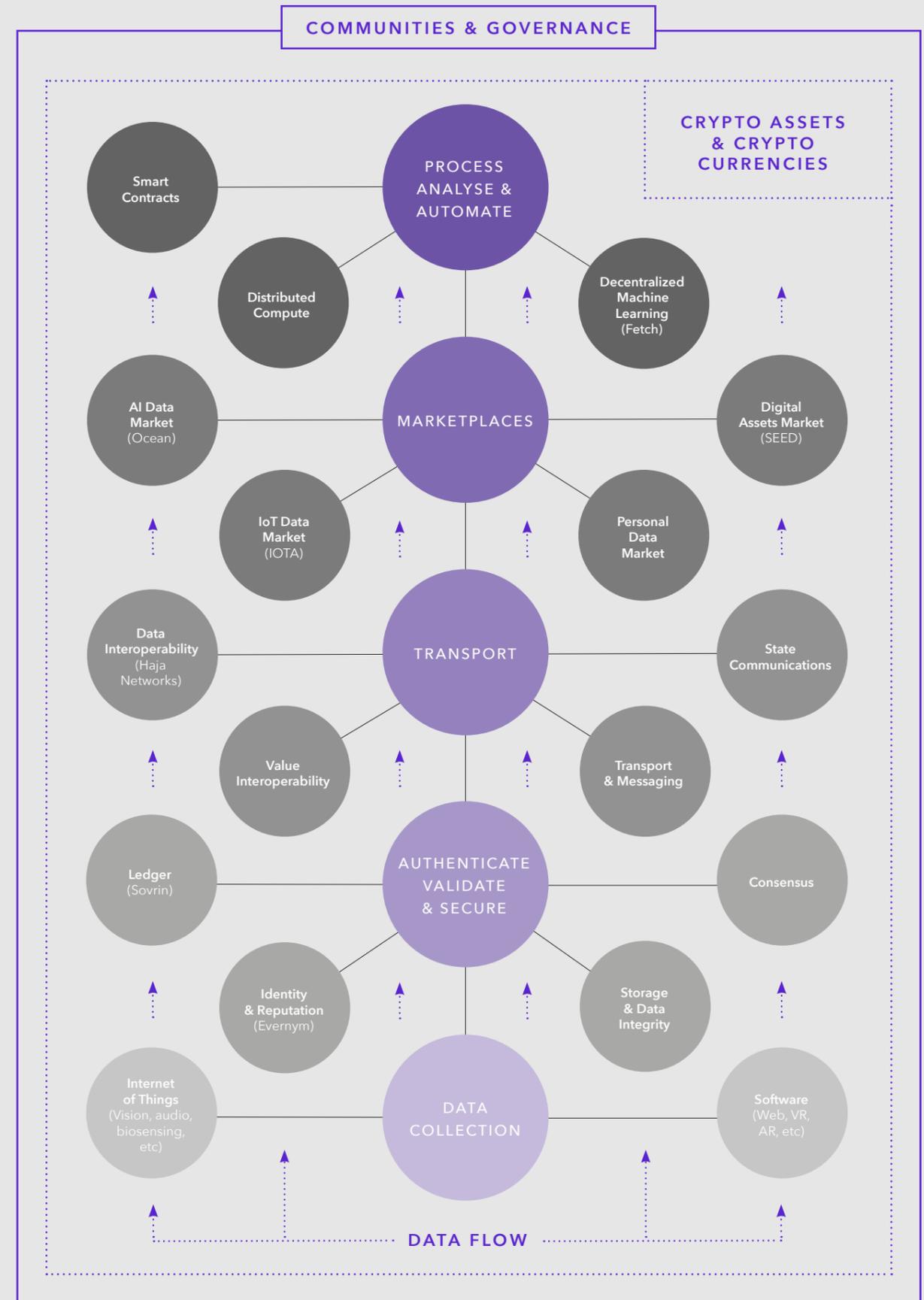


Figure 1. The Convergence Ecosystem

component in decentralised networks - the first digitally-native mass coordination mechanism for humans, bots and machines. As the hype falls away, we start the slope of enlightenment phase with a transformative digital incentivisation tool. In 2018 we need to focus on the job at hand: building and scaling new networks and protocols that will underpin a new data infrastructure.

Introducing the Convergence Ecosystem

All of our investments, corporate and academic partnerships, and research over the last four years' has led us to believe that markets are moving into a new era. They are becoming open-source, distributed, decentralised, automated and importantly tokenised. We call this new era: the Convergence Ecosystem. This is the Outlier Ventures investment strategy.

In the Convergence Ecosystem, data is the core asset. Collected by the Internet of Things and software, data is authenticated, validated and secured using distributed ledgers, consensus and other decentralised technologies. When needed, data is transported and shared before ending up in marketplaces to be packaged up and sold. Finally, it is processed, analysed and automated using a range of technologies including distributed computation, decentralised machine learning and smart contracts.

This entire data flow is coordinated and incentivised using crypto-assets, crypto-currencies and nascent crypto-consumables designed to incentivise behaviours for people, machines, devices and agents to the benefit of the overall

ecosystem. New emergent governance models will have differing levels of decentralisation and automation depending on the values of the community. Some will value censorship-resistance above all else. Others will value self-sovereign identity or equalitarian wealth distribution. Communities can use traditional governance structures like corporations or newer structures like decentralised organisations or decentralised autonomous organisations (DAOs).

The open-source nature of the technology; ease of forking; almost zero costs of digital distribution; and interoperability protocols will mean projects will struggle to differentiate using technology in the long-term. Successful projects will differentiate through values and trust. This makes the Convergence Ecosystem structurally different from other markets in which value capture happens at friction points. With very few friction points and lock-in, we are unlikely to see the same market consolidation dynamic that has dominated previous digital markets. When technology and data are open and free, lock-in will come from brand and values. There will be as many protocols as there are value-systems and personal priorities. There will not be one chain to rule them all. In a world of scarcity, competition is the optimal strategy. In a world of abundance, we must change our mental models. The Convergence Ecosystem drives collaboration rather than competition.

In this paper, we introduce the Convergence Ecosystem. We will explore each layer in turn: the coordination layer of communities, governance systems, and tokens. The collection layer which brings in data from the Internet of Things and software. The authentication, validation

and security layer which uses decentralised infrastructure like distributed ledgers and self-sovereign identity. The data transportation layer which defines how data moves across databases, networks and systems. The marketplace layer where data is packaged up and sold. Finally, the processing, analysis and automation layer where distributed computation, decentralised machine learning, and smart contracts are used to inform decision-making.

The existing centralised data infrastructure is no longer fit for purpose. It poses not only technical problems, but more far-reaching economic and social problems. A new decentralised infrastructure must be built.

We welcome you to the next era of economic activity: The Convergence Ecosystem: open-source, distributed, decentralised, automated, and tokenised.

“

The Outlier Ventures Convergence strategy provides a clear, cogent and coherent perspective on the evolution and impact of distributed technology in general, and on the emerging field of crypto-economics in particular. Recommended reading for anyone seeking a deeper insight into the decentralised token-based ecosystems of the future.

”

Prof William Knottenbelt
 Director, Imperial College Centre for
 Cryptocurrency Research and Engineering

Tokens, Communities & Governance

Networks and ecosystems that make up the Convergence Ecosystem need to be coordinated and governed.

The industry is rapidly experimenting with new (and old) consensus mechanisms and decision-making techniques. This experimentation began with Bitcoin and spawned thousands of tokens each with different rules to encourage or discourage behaviours within the network and allocate resources. Tokens and automated decision-making tools allow for the mass decentralisation of entire industries through a distributed coordination network. These networks are birthing new types of resource allocation structures such as decentralised and autonomous organisations, pushing forward our conception of what an organisation should be.

Tokens

Cryptographically secure and digitally scarce tokens are the key innovation that makes a group of technologies into a living, breathing ecosystem. Tokens are a native digital coordination mechanism for the Convergence Ecosystem. Until now we have been retrofitting a financial infrastructure designed for cash and cheques to the digital, software-defined era. Ever since the emergence of Bitcoin, it has been clear that distributed ledgers with automated consensus held the potential for new forms of asset and value exchange. It was not until the ERC20 smart contract on Ethereum that experimentation around digital and programmable money began at significant scale. There is now a mechanism to fund open-source protocols that would have previously struggled to raise financing because open-source lacked a business model. As Albert Wenger has noted: "Now, however, we have a new way of providing incentives for the creation of protocols and for governing their evolution."¹ In early 2018, we are still at the very beginning of this evolution.

Over the next year or so, we expect to see a much clearer delineation between two types of tokens: crypto-assets and cryptocurrencies. Cryptocurrencies will be designed to be a medium of exchange and crypto-assets will be designed to be a store of value and offer utility in a digital economy. Despite the fact dominant token ecosystems have a element of both; design challenges abound when attempting to incentivise usage with digital scarcity. It is unclear if single-token systems like Bitcoin and Ethereum can provide a sustainable balance; instead it is likely we will see multi-token systems as a more effective mechanism.

Most projects will fail, but the open-source nature of the ecosystem means learnings and code will be available to all. We can learn and build faster than ever.

Experimentation is happening at a rapid pace on both the supply and demand side. We have tokens with a deflationary economy, scheduled inflation and others that let the community vote on how and when new tokens are minted and/or burned. That is just programmable money supply; we are also experimenting with demand-side economics: variable transaction fees, demurrage charges, interoperability, and different consensus rules. Non-fungible tokens such as cryptokitties and the new Ethereum ERC 721 NFTs will also impact demand by incorporating historical ownership creating a subclass of crypto-assets called crypto-collectables.

In addition, a currently underutilized token model is the crypto-consumable, a token that is programmed to reduce in value over time using a decay or burn function. This could be a continuous decline in value like a used car or a step decline like a ticket to a live event. This sort of token design would not be a store-of-value and would be a powerful way to increase network token velocity.

Today the industry is focused on the initial distribution of these tokens in generation events. But the initial distribution is just one stage of building a sustainable ecosystem. Token distribution schedules will become more sophisticated over time to include staged releases like traditional equity fundraises and mechanisms such as airdrops or token faucets. Continued network engagement will separate successful networks from unsuccessful ones. 2018 and beyond will show that the much of the ICO class of 2017 was prepared for initial distributions but underprepared for sustainable growth and utility. It must be remembered that prior to 2017, tokens

were distributed to the network in exchange for utility; Bitcoin distributes Bitcoin as a reward for the secure clearing and settling of Bitcoin transactions. By giving away the majority of tokens upfront, many 2017 ICO projects are left with few tokens to reinvigorate demand later down the line.

Most projects will fail, but the open-source nature of the ecosystem means learnings and code will be available to all. We can learn and build faster than ever. Unlike economic modelling or theory, the industry is testing economic theories in real-time with real money. It is the greatest experiment in socio-economics we have ever seen.

Tokens are the first native coordination mechanism for the digital and now machine economy. We expect tokens to be issued at each layer of the stack to incentivise behaviours within each particular network and to connect with the broader ecosystem through a series of exchanges and interoperability protocols. The model would be similar to today's global economy in which each nation issues and uses their own currency within their own borders and trades foreign currency with other countries for products and services that it needs. If Bitcoin is indeed the digital store-of-value in the same way gold is the physical store-of-value, it is likely we will see a digital hierarchy of money emerge with Bitcoin as an apex token, protocol tokens like Ethereum, NEO and Cardano below Bitcoin, and utility or application tokens below the protocol tokens. As the Convergence economy develops and core infrastructure is developed, tokens will become increasingly liquid and frictionless leading to extraordinarily complex economic dynamics.

¹ Albert Wenger. Crypto Tokens and the Coming Age of Protocol Innovation. <http://continuations.com/post/148098927445/crypto-tokens-and-the-coming-age-of-protocol>

Communities & Governance

Tokens themselves are simply a type of value instrument. The rules under which these instruments are generated, distributed and managed are decided by community members through agreed governance rules. These governance rules are set and decided by the community members using different forms of decision-making. For protocol tokens like Bitcoin, Ethereum et al., governance includes decision-making on changes to the network. The explosion of tokens and blockchain-based networks has led to a renaissance in thinking about governance, especially decentralised governance.

We have the Bitcoin network with a strong libertarian value-system valuing decentralisation above all else and therefore there is a separation of 'powers' between developers, miners and users; no one stakeholder group can 'force' a decision on the others. This results in a very slow-moving but stable network. Ethereum, while still aiming to be a decentralised network, does not have quite as strong libertarian streak but does have more leadership with Vitalik Buterin who is often able to push through changes because the community follows his lead. An example is the 2016 summer fork to return funds lost through the DAO bug.

New projects are experimenting with automated governance in an attempt to avoid messy human decision-making. Tezos is hoping to enable governance to be 'upgraded' through community voting. DFINITY is doing something similar but allowing retroactive changes to the ledger. These types of 'on-chain' governance as they are known are still technically immature and open up a whole

new attack vector. Other projects like Augur and Gnosis are testing futarchy, a type of voting model in which the community defines a set of values and then prediction markets are used to decide which decisions will maximise those values.

We are also seeing exciting experiments with curation markets and reputation staking from projects like Colony and Ocean. This type of decentralised and automated model is extended further with decentralised autonomous organisations (DAOs). In these sorts of organisations, all decision-making is offloaded to smart contracts and decisions would be automated based on the rules encoded in the smart contracts. One of the first examples was of course TheDAO, a DAO for venture funding, that was never able to allocate capital after a bug was exploited. Other live examples include Dash, a privacy-focused cryptocurrency; DigixDAO, a gold payment system project; and Aragon, a platform hoping to provide the entire governance service for other token projects.

The end-point of blockchain-based automation will come through AI DAOs as articulated by Trent McConaghy. These theoretical organisations will be managed and owned by AI algorithms enabling AI to interact in the economy by earning and spending tokens. An AI could own a fleet of self-driving vehicles, charging fares which it then uses to pay for maintenance, tolls, insurance, and taxes.

Blockchains and tokens will be issued, distributed, governed and owned in increasingly diverse ways. Governing models will evolve and we are likely to see an industry with multi-types of governance

each co-evolving around the belief-systems of the community they serve. Bitcoin will remain staunchly libertarian; Ethereum has more of a central leadership which appeals to pragmatic developers; and self-sovereign identity underpins the value-system of the Sovrin blockchain. We will soon see more projects with social democratic values that prioritise wealth redistribution through 'network' (read: State) intervention or pre-agreed taxation rules. Others will prioritise ethical and environmental values with green-friendly policies that use non-consumption based consensus mechanisms (eg Chia) and focus on common-ownership and resource sharing.

The Convergence Ecosystem should support a diverse range of different governing models that support different communities. There is no optimal model of governance; only a perpetual tension to maintain alignment amongst stakeholders. We have millenia of literature exploring politics and governance, everything from Plato's five regimes to John Locke's libertarianism to Jeremy Bentham's utilitarianism. Philosophers and political scientists will never settle on an 'optimal' governance model because 'optimal' can only exist for individuals in limited contexts never for society at large.

As with almost all information and communications technologies that have come before, blockchain technology was born decentralised. Bitcoin with the first blockchain implementation was a libertarian movement created as a direct reaction to a centralised financial system. Early adopters shared this value-system. As more and more blockchains and tokens are created, the industry attracts an audience with different belief-systems. As it continues to mature, different communities

will have unique objectives and priorities that will require specific design trade-offs. The financial community requires more and faster transactions and will sacrifice decentralised consensus to achieve that, as can be seen with Ripple and its XRP token. The healthcare community must adhere to privacy regulations and so will require more privacy than public blockchains currently afford. The ecosystem will support a variety of communities using different governance models with differing levels of decentralisation and automation depending on the values of the community and the needs of the market.

We are in the very early stages of understanding how to design token economies and the governance models that support them. As an industry, we must be more supportive of new ideas and implementations. It is not a zero-sum game in a growing market. Some tokens, communities and governance experiments will fail. Let's learn quickly from their failures and compound learnings. The biggest advantage the decentralisation community has is momentum and the brightest minds from around the world are working together to solve tough problems. Communities will co-exist and thrive. Let's be inclusive and supportive.

Data Collection

Data is the lifeblood of the ecosystem arriving through the IoT (hardware) and software.

Sensors measuring the external environment are often bundled together under the umbrella term the 'Internet of Things'; and they include all sensors in smartphones and wearables such as gyroscopes, accelerometers, and proximity sensors as well as hundreds of others sensors measuring our world.

It is estimated that the amount of data created annually will reach 180 zettabytes (one zettabyte is equal to one trillion gigabytes) by 2025 up from 4.4 zettabytes in 2013 and an average person anywhere will interact with connected devices every 18 seconds (nearly 4,800 times a day).²

Decentralised technologies potentially provide a more secure, shared data infrastructure whereby data use isn't a zero-sum game.

The Internet of Things

The industry lacks a standard definition of the IoT, and in its broadest sense, it will come to include every physical object that has a sensor, microcontroller and Internet connection. Today that mainly means connected home devices like Amazon Echos, wearables like the Apple Watch, industrial and agricultural connected sensors, and smart meters measuring home energy usage. But the range of applications is growing, and it has been estimated that by 2024, the automotive industry will account for the almost a third of all IoT connections, followed by consumer electronics and FMCG (fast moving consumer goods) and the utility sector. Other sectors including Smart Cities, supply chain, manufacturing, healthcare and others will make up a relatively small proportion of

the connections.³ The IoT market intersects with the robotics market in the sense that a robot has the same features as an IoT device, but with the addition of actuators and the means to move and respond to the environment. We would consider connected vehicles, service robots and other types of robotics as data collecting machines.

The IoT market is often measured in the number of connections - roughly 30 billion by the end of the decade⁴ - or the economic impact - 11 trillion dollars over the next decade says McKinsey.⁵ A less-asked question is: what happens to all the data? The same McKinsey study found we may be using as little as 1% of data being generated. As well as under-utilising data, how data is being used is unclear. In a survey by Ponemon Institute, 82% say IoT manufacturers had not provided any

details about how their personal information is handled.⁶

The emergence of distributed systems like IPFS, Filecoin, and other blockchains offers a new model for data storage and usage. It has been expected that data would be fought over by devices makers, software providers, cloud providers and data analytics companies. In fact, the reluctance of car makers to put Android Auto or Apple CarPlay into their cars is an awareness that they would lose control of valuable data.⁷

Decentralised technologies potentially provide a more secure, shared data infrastructure whereby data use isn't a zero-sum game. IoT data creators can retain ownership rights of data and engage users of data in marketplaces, a subject we will discuss in more depth later.

Software

Adding to the 50 billion IoT connections, we also need to add digital media and human-generated digital data. We are on our way to quantifying and digitising our external world, and we are even further along in gathering data on our digital lives. We use the term 'software' as a producer of data broadly to capture all personal and business data produced through the interaction with databases, operating systems, applications and APIs. These interactions build up digital dossiers including cookie and web browsing data as well as active traces like social media and messaging.

On the business side, as we continue to digitise and bring online our offline interactions and documents like electronic health records and learning records, key sectors will have an

overwhelming amount of data to handle, which they do not have the capabilities to utilise.

On the consumer side, digitally-created and digitally-augmented environments with augmented reality (AR) or virtual reality (VR) will lead the growth in available personal information.

Half the world's population - 3.82 billion - will have an Internet connection by the end of 2018 and by 2020 it will be 4.17 billion. Mobile data traffic will grow to 49 exabytes per month by 2021, a sevenfold increase over 2016.⁸ We are creating unfathomable amounts of data, and the growth shows no sign of abating. Adoption of AR and VR will further drive the amount and granular detail of data that we can collect, enabling deeper insights into individual and collective behaviours. Whether it's from the IoT or software, we have a massive data problem.

We are creating and collecting more data than ever, but we are storing it in insecure private databases with no incentives to share the data. Data breaches and hacks are commonplace, and the data can be censored or tampered with. Software-generated data is lost, hoarded or latent. There is no reason for consumers to do anything other than to give data away for free and for corporations to hoard it. Decentralised infrastructure offers a solution.

Previous page

² Amount of Data Created Annually to Reach 180 Zettabytes in 2025. <https://whatsthebigdata.com/2016/03/07/amount-of-data-created-annually-to-reach-180-zettabytes-in-2025/>. Accessed 17 Jan 2018.

³ Cambridge Consultants. Review of latest developments in the Internet of Things - 07 March 2017.

Current page

⁴ IEEE Spectrum. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>

⁵ The Guardian - Data could be the real draw of the internet of things - but for whom? <https://www.theguardian.com/technology/2015/sep/14/data-generation-insights-internet-of-things>. Accessed 17 Jan 2018.

⁶ Ponemon Institute. Privacy and Security in a Connected Life - https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rt_privacy_and_security_in_a_connected_life.pdf. Accessed 17 Jan 2018.

⁷ The Verge. Why carmakers want to keep Apple and Google at arm's length - <https://www.theverge.com/2017/1/13/14268252/apple-carplay-google-android-auto-vs-carmakers>. Accessed 17 Jan 2018.

⁸ Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper - <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>. Accessed 17 Jan 2018.

Authenticate, Validate & Secure

After data is collected from the Internet of Things and software, it must be authenticated, validated and secured.

This is the layer in which blockchains and distributed ledgers fit into the framework and add value. Without these decentralised technologies, authentication, validation and security would be provided by a third party without the characteristics provided by blockchains such as increased external transparency, provenance, tamper-evidence and censorship-resistance.

Distributed Ledgers & Blockchains

And so onto the wonderful world of blockchains. If you are already familiar with distributed ledgers and blockchains, go ahead and skip to the next section. Often the terms “distributed ledger” and “blockchain” are used interchangeably, but a blockchain is a particular type of a distributed ledger which is simply an asset database that can be shared across a network, structured like a chain of blocks. You can find full definitions and variants of blockchains and distributed ledgers elsewhere. But for clarity when we talk of blockchains, we are referring to a specific type of data structure that is cryptographically linked together in a linear sequence of blocks, each of which contains a record of transactions.

The type of consensus mechanism used to validate the blocks will vary and evolve, and we will explore this in more detail in the next section. There are many types of distributed ledgers that vary across many vectors including the number of participants, and who can view and amend the ledger. Another class of distributed ledgers is structured as directed acyclic graphs (DAGs); IOTA and Byteball are both prominent examples. Broadly speaking though, distributed

ledgers and blockchains provide a mechanism for transaction, verification and storage of digital assets on distributed ledgers. The specific type of distributed ledger that is needed will depend on the use case being served and the features that are most important.

A public blockchain, for example, is a distributed ledger in which every transaction is visible to all parties, and which is accessible to anyone to write a new block to the chain according to its consensus rules. Examples of these include Bitcoin and Ethereum. Consensus for adding new transactions to the ledger takes longer as no central authority has the right or power to force a change. These are chains where anonymity, decentralisation and immutability matter more than efficiency. Public permissioned ledgers are similar in the sense that they are openly accessible for verification of transactions to all parties, but the validators are known parties and admittance of new validators requires the approval of the existing group.

The grade of decentralisation depends entirely on the extent to which validators are independent. For instance, R3 and Hyperledger Fabric can revoke a transaction or make changes to their blockchains relatively faster due to the centralised nature of their consensus formation. These chains function magnitudes faster than public, permissionless chains as they value efficiency over decentralisation. Private blockchains are used in situations where a handful of entities that may be individuals or enterprises require real-time settlement of digital assets. The emphasis here is on trust, storage and speed over being openly accessible.

Whether public permissionless blockchains, public permissioned blockchains, private distributed ledgers or DAG-based ledgers, this class of distributed data structures offers a mechanism for multiple entities to transact without the need for a trusted third party. The removal of a trusted third party provides operational efficiency and cost saving benefits, as well as censorship-resistance and security advantages. Each will matter more to different companies and markets. We believe that regardless of the success of any particular distributed ledger implementation, this set of technologies will offer a trusted storage, verification and transaction platform for the Convergence Ecosystem.

Consensus

The distributed, decentralised nature of blockchains makes the need for verification and agreement on what transactional data on the chain is accurate a prerequisite. If every party on a blockchain does not agree upon the legitimacy of a transaction and attest to it, different entities within the network would share databases that vary. Consensus can be defined as the process through which every system within the connected network agrees upon an event within the network. The “event” can be a simple transaction, as in the case of a Bitcoin transaction, or a relatively sophisticated smart contract function being triggered, as in the case of Ethereum. Blockchains provide a reliable solution for solving what is referred to as the Byzantine Generals problem⁹ in an open, anonymous network. They allow the majority of the distributed entities within a network to come to an agreement on what information is accurate and enforce algorithms that replicate the data across every entity.

Depending on the nature of the ledger, the consensus mechanisms may vary. Bitcoin, for instance, uses “proof of work” (POW). To validate transactions occurring on its chain, a node has to prove that it has done some amount of computational work in finding a cryptographic hash. This is akin to solving a puzzle, except in this case exceedingly powerful computers around the world are committed round the clock towards solving these. Miners who dedicate computing power to the puzzles are incentivised to do so through coins that are rewarded for mining each block. POW is used to make the ledger byzantine fault tolerant in a public, permissionless environment where Sybil attacks need to be dealt with. In a permissioned network, Sybil attacks can be prevented, allowing for more efficient Byzantine fault tolerance algorithms. Permissioned networks can be private, such as in an enterprise blockchain environment, or public, such as in Sovrin.

A more energy efficient - but less proven - alternative approach is proof of stake (POS). In these chains, nodes do not engage in finding hashes. On the contrary, accounts with high enough stakes (token balances), validate transactions. Since the implicit trust in a network can diminish if bad actors validate illegitimate transactions, those with large enough stakes in these networks have an incentive for not engaging in malpractice. Other mechanisms exist such as proof-of-space (PoSpace), which uses disk space rather than computation as the resource used for mining. For DAG-based ledgers, there are yet other ways in which consensus is reached, many based on probability theory.

⁹ Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper - <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>. Accessed 17 Jan 2018.

Depending on the use-case and varying needs for speed, efficiency, security and cost of transactions, consensus mechanisms on a blockchain will vary. Completely decentralised systems that are public and permissionless rely upon proof of work as it hypothetically gives every node within the network an equal opportunity to validate transactions as long as the hash rate is equal. Relatively private, permissioned chains use PoS as a mechanism to come to a consensus as it endows trust on an entity with the highest stake in the chain. These mechanisms bring scale for “trustlessness” into ecosystems that would otherwise have no means to interact in the absence of a middleman.

By providing a framework for ensuring the legitimacy of shared interactions within a network, these approaches disrupt businesses that were traditionally playing the role of “validators” and rent-seeking without substantial value addition. Consensus mechanisms can, therefore, be referred to as validators to shared facts within a network. We do not expect one consensus mechanism to ‘rule-them-all’. We expect proof-of-work, proof-of-stake, proof-of-space, and many others to evolve and new ones to emerge. We believe that different consensus mechanisms will be chosen depending on application requirements.

Identity & Reputation

While Bitcoin is pseudonymous by nature, it spurred innovation in decentralised identity by introducing a system where transactions from individuals could be validated publicly in a decentralised manner. Identity on a blockchain is an area of increasing focus due to a surge in fraud, identity theft, and increasingly sensitive

data becoming digitised. The rise of seemingly reliable, centralised players such as Equifax has not solved identity-related issues in the Internet era; instead, it has aggravated them. This stems, in part, from the fact that centralised repositories are a honeypot for hackers. Even a minor failure in the authentication systems of these centralised authorities can lead to a loss of what is most crucial to any individual - their identity.

The coming of General Data Protection Regulation (GDPR) will also introduce a richer, more nuanced landscape between anonymity and attested identifiability. There are many applications for which anonymity is not suitable there are also many for which identifiability is not suitable or necessary. Self-sovereign identity is a core piece of this new landscape. Through self-sovereign identity, an individual will be able to authenticate or verify themselves without having to pass on their documents. Instead of having siloed repositories of documents, blockchains make it possible for individuals and institutions to attest each other through a peer-to-peer mechanism. Blockchains offer a building block for better identity systems, but decentralised identity solutions need to evolve far beyond what Bitcoin and similar blockchains have offered regarding privacy and scale.

The first generation of blockchain-based identity solutions relied on centralised players to verify an individual’s identity-related data. Civic, for example, uses email and phone number as a primary source of verifying an individual’s identity. These can then be used to log in to websites through a QR-based authentication system. The project further relies upon banking entities to verify an individual’s AML/KYC related documents. Where in the past

people would share their passports or driving license with every third party they deal with and risk leaking it to unreliable entities, Civic enables individuals to have their identity attested through known, reputed central authorities such as banks. Once these attest an individual’s documents, the individual can use those attestations to comply with AML and KYC on services that integrate with Civic.

The second generation of identity solutions based on decentralised identifiers (DIDs) are emerging, giving individuals the ability to control their own identity without a registration authority having the ability to access, revoke or edit the verifiable claims they have received. The Sovrin network and uPort are the most advanced of these self-sovereign networks. Anonymity or at least pseudo-anonymity is a feature of the Bitcoin network, but for most applications, anonymity is not suitable. In industries like financial services, healthcare and education, identity is a core part of any solution.

Once self-sovereign identity becomes the norm, individuals will have the ability to track instances where a third party sells personal information and services will enable payment for sharing their details without losing control of the data. Evernym which uses the Sovrin network goes even further by incorporating zero-knowledge proofs and pairwise identifiers to further protect individual identity when sharing data. Blockchain-based identity empowers the individual while removing the need to trust third parties with personal documents through verifiable claims and tokenisation. A new era of “fragmented” authentication based solutions compatible with authentication protocols like OpenID Connect,

”

Sovrin provides a decentralised platform for creating, sharing, and verifying a wide range of identity credentials—well beyond the fixed authentication schemes of traditional identity systems. Sovrin does for trust transactions what the Internet did for packet communications.

”

Dr Phillip J. Windley
Chairman, Sovrin

//

Once self-sovereign identities are established we will see automated systems such as chatbots, companions, and AI advisors used to increase authentication and even, in some cases, verification.

These bots will need reputation just as individuals build their own reputation and the issuing entity, the owner of the bot, will also have to take responsibility for the recommendations that bots make to users. A new era of transparency will be required as bots take on ever more important tasks in our lives.

//

Mark Stephen Meadows
CEO, Botanic Technologies & SEED

OAuth, FIDO and UMA will protect the privacy of the individual while increasing the trust in interactions on a network.

Storage & Data Integrity

The most common challenge we received on our Convergence strategy is that blockchains cannot store much data; so how will they be able to support the new data economy? They won't. Blockchains are not designed to store a lot of data. They will be used as on-chain pointers to off-chain data and implement an access control lists to control and monitor data access. Today's implementations are utilising decentralised databases and distributed file storage to store data "off-chain" in a way that ensures data integrity. The link between the blockchains (on-chain) and decentralised storage (off-chain) is still to be defined. We see a world in which the minimum amount of data to ensure the required levels of data integrity will be stored on the chain, and decentralised and distributed data storages and databases store the bulk of the data in a fast, accessible and indexable way.

There are numerous requirements for decentralised databases including speed, latency, throughput, resilience, consistency guarantees, ability to structure and index data, ability to delete data and so on. As per the CAP theorem, every real distributed system must make a design choice between consistency and availability during network failures. No database or data storage is going to be ideal for every use case. BigchainDB for example, is fast and can store a lot of data, but is currently not Byzantine fault tolerant so is more suitable for private instances. A blockchain-as-a-database like Ethereum can have strong

consistency guarantees due to the inherent consensus requirement, but as coordination is required to reach consensus, it is not network partition tolerant. As with life, everything is a trade-off.

The combination of blockchains for publically-accessible immutable storage of records and decentralised and distributed data storage will be core to the Convergence Ecosystem data infrastructure. Storing data in a decentralised database has the potential for greater redundancy, speed, and censorship-resistance but as with everything it comes with trade-offs. The main one involves incentives. Why would anyone give access to their hard drives? The answer is as we surely know by now: tokens and cryptoeconomics. File sharing in the token era incentivises individuals to share resources that would otherwise go to waste. This will not only create more secure, censorship-resistant methods of data storage but also improve the efficiency of storage marketplaces while creating economic opportunities. One such project is Storj. The system incentivises individuals that provide storage with tokens while keeping the files themselves encrypted and distributed across multiple nodes. Protocol Labs, the developers of IPFS, have taken a similar approach with Filecoin. IPFS enables the network to store and exchange files in a distributed fashion.

Just as important as the storage of data is ensuring its integrity. Using blockchain timestamping, cryptographic hashing and signatures together with data structures like Merkle DAGs, decentralised systems can in most cases provide a higher level of data integrity than other types of ledgers and databases. Projects such as Factom

and Tierion have partnered with both governments and enterprises to facilitate digitisation of physical documents with timestamps to provide an audit trail for sensitive documents. DeepMind with their new Verifiable Data Audit product is using the append-only and tamper-evidence features of distributed ledgers to let hospitals check in real-time how they are processing data. Regardless of the ledger or consensus particulars, storage and data integrity benefit hugely from decentralised tools.

As data sets for AI and sensory data for IoT increase in size, decentralised and distributed storage networks with variable authentication levels will allow entities to share information that can be stored and verified.

Transport

After data has been authenticated, validated, secured and stored it will need to be transported for use.

It will need to be 'transported'. The technologies of this layer are less mature than the layers below but will become ever more critical as blockchains and DLTs proliferate if we are to avoid the same data silos that exist today in the Web 2.0 era. It is at this layer where interoperability protocols are developing for messaging, value, data and state.

Messaging

Messaging refers to networks which aim to quickly, accurately and securely send and receive information such as instructions, signals, and authentication. This technology is fundamental to many services, including money transfers, communication between applications, and data transferral in booming data markets. For international bank transfers, this is a global monopoly controlled by a single entity, SWIFT (Society for Worldwide Interbank Financial Telecommunication). SWIFT¹⁰ is currently used to connect over 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. Why is this a problem? Well, as the internet continues to develop, so do those using it and the tools they are using. Because of this,

the promise of security quickly becomes one that cannot be kept. This reality has been unravelling since the start of 2016, when the Central Bank of Bangladesh lost approximately \$81 million to a malware attack which acquired their SWIFT login details and removed their holdings from the New York Federal Reserve. It is estimated that throughout 2016 Ukraine and Russia similarly lost hundreds of millions of dollars in SWIFT-related hacks. If a single centralised system offers access to international transactions, a breach of that system's security would similarly put global cash flows at risk.

In fact, a report by Credit Suisse, 'Bitcoin: The Trust Disruptor',¹¹ warned SWIFT that blockchain technology could soon be encroaching upon their raison d'être. This principle goes not just for financial messaging networks, but for all traditional messaging networks. While xCurrent by Ripple allows banks to message each other with greater speed, transparency and efficiency than SWIFT, communication protocols like Mercury can achieve both decentralisation and tamper-evidence, ultimately removing the need for a centralised validator. By decentralising data, blockchains provide a more robust security

architecture than what was traditionally available to users. For applications building upon them, this significantly reduces the threat of compromise.

Many of these networks, however, are yet to be tested under the pressure of thousands of users per second (a capacity easily handled by current messaging systems). Nevertheless, there are a plethora of competing products improving at a rapid rate. Projects like TeleHash and Whisper¹² are working to enable more secure, trustless peer-to-peer messaging systems. Ultimately, it is the refined versions of these products and their competitors which will provide the throughput and security required in automated data and value markets.

Value Interoperability (On-chain)

Value interoperability across multiple blockchains refers to the ability of digital assets in one blockchain to interact with assets in another. The most straightforward example for an interoperable transaction would be one in which an individual transfers a cryptocurrency on one blockchain in exchange for cryptocurrency on another, for example, Bitcoin exchanged for Litecoin or XRP. Interoperability matters as it enables multiple ledgers to compound the benefits offered by each. Through limiting the flow of value in a blockchain to a single ledger, one risks creating new “decentralised” DLT-based siloes that cannot interact with each other at scale. By enabling ledgers to interact with one another with a communication protocol layer, improvements in security, speed, cost of transactions can be attained.

There are multiple approaches to obtaining interoperability, each with a focus on a specific function. One of the simplest forms is through a relay. These utilities check for transactions in one chain and “relay” that information to another. BTC Relay, for instance, allows Ethereum smart contracts to verify a Bitcoin transaction without any intermediary. This enables Ethereum DApps and smart contracts to accept Bitcoin payments. A new generation of cross-chain transaction enablers allows exchanges to occur without a centralised party. Atomic cross chain swaps use hash time locked contracts to enable two parties to interact with tokens from different ledgers with each other without the need for an intermediary.

Value interoperability will allow value that is stored in siloed blockchains to break free.

Atomic cross chain swaps will be crucial in creating a new generation of decentralised exchanges. Cosmos, Polkadot and Komodo are a handful of projects with an explicit focus on the space. Interoperability protocols also often enhance privacy through zero-knowledge proofs. They enable verifying the accuracy of a computation without knowing the variables involved. Through sending a transaction across multiple ledgers, tracking the source and recipient of a transaction can be made drastically more difficult. One could also consider decentralised exchanges such as EtherDelta¹³ as an interoperability enabler. Although restricted to ERC20 tokens, they allow individuals to trade their tokens for another one without relying on a central authority. One could trade their Storj tokens received as payments for leasing their computer’s storage space out and buy INS tokens to receive discounts at a retail outlet without having to move coins from their wallet with the help of the likes of 0x and Kyber. While decentralised exchanges come with new challenges - especially liquidity - they offer the promise of delivering significant security improvements over centralised exchanges.

Value interoperability will allow value that is stored in siloed blockchains to break free. This applies equally to value stored in both public and private blockchains. NEO is already enabling cross-chain asset agreements with NeoX. Users do not need to set up wallets for every blockchain they want to use and rely on third parties every time they have to interact on a different chain. Interoperability protocols further add value to the Convergence Ecosystem by allowing multiple industry-oriented tokens to communicate with each other. For instance, one could make payments in MIOTAs

Previous page

¹⁰ 'Discover SWIFT | SWIFT' <https://www.swift.com/about-us/discover-swift>. Accessed 9 Feb 2018.

¹¹ The Credit Suisse report can be found here <http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf>

Current page

¹² These are the Githubs and websites <https://ripple.com/solutions/process-payments/>, as well as <https://www.mercuryprotocol.com>, Telehash and <https://github.com/ethereum/wiki/wiki/Whisper>

¹³ "EtherDelta." <https://etherdelta.com/#PPT:ETH>. Accessed 9 Feb 2018.

for leasing IoT based sensors that pass on data using the Ocean Protocol OCN token. Similarly protocols would be used in connecting and incentivising functions in mobility and robotics. A machine can pay for access to a resource in the native token of one ledger and receive the resource itself through another ledger. As projects and protocols start delivering real-world utility at scale, the need for exchange infrastructure will increase. One could compare these protocols to hubs that route value without an intermediary.

In a world of seamless value interoperability one can expect a complex interplay between users holding tokens for particular service utility and others for store-of-value; the wallet or 'portfolio' balance likely optimised by a personal AI. This AI will be personalised by risk appetite, values and services; the weighting of which will lead to a new field of TPO (token portfolio optimisation) an extension of search engine optimisation (SEO) and social media optimisation (SMO). If purchasing and holding tokens is a reflection of one's values, it's interesting to think that token portfolios could become a new sort of social or political badge.

Data Interoperability

(Off-chain)

Today, incredible amounts of data are stored on the private servers of a relatively small amount of organisations. The internet's client-server architecture¹⁴ makes data-sharing inconvenient, while privacy and data protection laws¹⁵ limit the cases where it can be done legally. Even if this were not to be the case, there is no rational economic incentive for individuals to do anything other than give away their data. While strides are

being made towards increased data accessibility, such as open Application Programming Interfaces (APIs)¹⁶ and open-data regulations like PSD2,¹⁷ the benefits are one-sided. Indeed, users can now benefit from open data, but there is still no market, and data contributors remain largely unpaid. So, are blockchains the solution?

Blockchains are not databases; they are ledgers. It sounds almost flippant to say that, but the distinction is essential in understanding why data interoperability is just as important as value interoperability. Value interoperability means tokens can be moved across chains; data interoperability allows data to move across databases. Blockchains must be lightweight with limited on-chain storage so that "anyone" can download a full history of the blockchain. If blockchains become too large, fewer people will be able to participate in the network, thus reducing the decentralisation of the network and overall security. When it is said: "blockchains will enable large datasets to be shared or stored" actually it is not blockchains where the data itself will be stored. We are talking about decentralised and distributed data storages like IPFS and Swarm. Each blockchain implementation uses different data storage for "off-chain" data, and the balance between "on-chain" and "off-chain" data depends on the use case requirements. Just like the design of the Internet and the internet protocol suites, we expect blockchains to remain as light as possible to ensure speed and reliability; it will be the "off-chain" storage that will hold the majority of the data.

But what we must avoid is a world in which value is interoperable, but the underlying data is not; leading to the same monopolistic market dynamic as we have today.

But what we must avoid is a world in which value is interoperable, but the underlying data is not; leading to the same monopolistic market dynamic as we have today. Projects like OrbitDB are vital in enabling data sharing throughout the ecosystem. We need protocols that permit data to be shared seamlessly across both centralised and decentralised databases. Innovations in cryptography such as zero-knowledge proofs, differential privacy, Fully Homomorphic Encryption (FHE), and Secure Multi-party Computation (MPC) will enable data to remain private and secure but still move through public networks. Without data interoperability, the Convergence Ecosystem does not work.

¹⁴ Client-server architecture refers to networks where computers act as either a client or server. Clients use personal computers, while servers have superior computers which allows them to hoard data.

¹⁵ For examples of such laws, look at section 264 of the <https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996> <https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996> and part II of the <https://www.legislation.gov.uk/ukpga/1998/29/contents>

¹⁶ Open APIs provide services or data to third-party developers free-of-charge. For more information read Qiu, Y., 2015. How Open is 'Open API'? A Critique of the Political Economy of Openness in Programming . Pages 1-5. Link available https://ses.library.usyd.edu.au/bitstream/2123/14384/1/Qiu_Y_Thesis.pdf.

¹⁷ <https://transferwise.com/gb/blog/what-is-psd2> provides a good, brief description of PSD2.

Only when both value and data can be shared securely, can marketplaces be built that will drive the Convergence Ecosystem.

State Communication

Another barrier to mainstream adoption of blockchains is the lack of speed and increasing cost of transactions. State communication protocols provide a mechanism to limit the number of settlements a blockchain must perform by enabling off-blockchain communication channels. These 'state channels' are basically a two-way discussion channel between users, or between a user and a service (a machine), and because the blockchain doesn't need to settle the transactions they can be cheap and fast.

Consider for instance the case of CryptoKitties becoming popular overnight, clogging the Ethereum network,¹⁸ or popular token sales having the same effect.¹⁹ Blockchains like Ethereum have very low capacity limitations beyond which they become clogged, slowing down future transactions. State channels fundamentally take the process of settlement and computation out of a main network, do the necessary function and relay the final state of each individual within the channel to the main network after a preset period of time. The state can consist of payment balances, such as in a Bitcoin payment channel,²⁰ or more elaborate smart contract data, such as in a generalised Ethereum state channel. This reduces the burden on the blockchain in terms of number of transactions while ensuring that the trust, immutability and decentralisation of the blockchain itself are not compromised. State channel transactions occur entirely off a chain and

solely between the individuals involved and can be customised as per the requirement at hand. The fundamental idea behind state channel communication is to make the main network as lean as possible whilst using off-chain settlements to attain speed, cost efficiency and scale.

Bitcoin's Lightning Network,²¹ Ethereum's Raiden Network²² and IOTA's Flash Channels²³ are examples of scaling solutions that rely on state communication for efficiency and speed. Raiden achieves this through digitally-signed, hash-locked proofs called balance proofs that are collateralised through previous on-chain transactions. Where earlier an individual would make multiple transactions on the main chain, they can create a balance proof and create micro-transactions as needed. Raiden balance proofs are acquiring post individuals "signing" on the chain. This makes sure neither party can back out of the transaction as long as one of them relays information to the mainnet. These channels can also be defined to be expired between two parties on basis of time that has passed or number of transactions conducted.

State channels are core to the Convergence Ecosystem to enable the sort speed and scale needed for a global data infrastructure. For the sort of decentralised data infrastructure of the future we are anticipating, state channels as well as messaging and communication, value and data interoperability protocols are a prerequisite. Without building these transport and messaging tools we will squander the opportunity fix the Web 2.0 problem of centralised data infrastructure.

¹⁸ 'Loveable Digital Kittens Are Clogging Ethereum's ... - CoinDesk.' <https://www.coindesk.com/loveable-digital-kittens-clogging-ethereums-blockchain/>. Accessed 9 Feb 2018.

¹⁹ 'Status ICO Highlights Inherent Flaws of Ethereum's Blockchain and...' 21 Jun 2017, <https://themerple.com/status-ico-highlights-inherent-flaws-of-ethereums-blockchain-and-myetherwallet/>. Accessed 9 Feb 2018.

²⁰ 'Payment channels - Bitcoin Wiki' 26 Nov 2017, https://en.bitcoin.it/wiki/Payment_channels. Accessed 9 Feb 2018.

²¹ 'Lightning Network' <https://lightning.network/>. Accessed 9 Feb 2018.

²² "Raiden Network." <https://raiden.network/>. Accessed 9 Feb. 2018.

²³ "Instant & Feeless – Flash Channels - IOTA - IOTA blog." 24 Sep. 2017, <https://blog.iota.org/instant-feeless-flash-channels-88572d9a4385>. Accessed 9 Feb 2018.

Marketplaces

Data has been collected, validated and transported; now it needs to be used. Before it is processed, analysed and automated, marketplaces are emerging to allow the trading, buying and selling of data and digital assets.

These marketplaces are made possible because of the distributed ledgers, consensus mechanisms and interoperability protocols at the lower levels. It is only because data has been unlocked lower down that it can be traded further up the stack. We will see the emergence of a whole host of new types of marketplaces beyond just today's cryptocurrency exchanges. New marketplaces will enable the sharing of IoT data, AI data, personal data as well as other digital assets like crypto-collectables (pioneered by CryptoKitties)²⁴ and bots.

IoT Data Marketplaces

IoT data is already being collected in vast quantities, but the sprawl of devices has created a fragmented ecosystem. On the consumer side, operating system providers like Apple, Google and Amazon are attempting to leverage their dominant positions in smartphones and retail to sell more devices to collect more data. The Apple Watch and CarPlay, Google Home and Next, Amazon Echo and Dot; these are all attempts to grow their walled gardens of data. Smaller consumer IoT device makers like Fitbit, Wink, or GreenIQ struggle to collect enough data to make do meaningful machine learning to improve their products as quickly as the tech giants.

On the enterprise side, the same dynamics are at work. The internet of things (IoT) and industrial internet in the United States, Industrie 4.0 in Germany, and 物联网 (wù lián wǎng) in China all promise to use low-cost sensors and big data analytics to dramatically improve productivity and usher in a new age of data-driven manufacturing.

But the promise has not been realized for a number of reasons. Core to the failure has been the lack of data sharing. This lack of data sharing has been the case across all industries that are trying to utilise IoT technologies including aviation, agriculture, and utilities.²⁵ The problem, as we have already highlighted, is that there is no incentive to share data because it is seen as the competitive advantage to be protected. Current data infrastructure is coarse: data is either hoarded and valuable, or shared with limited commercial viability. IoT marketplaces begin to offer new business models for the monetisation of machine data. The IOTA data marketplace is a good example of the new types of marketplace that are emerging to enable the sharing of sensor and machine data.

AI Data Marketplaces

Just like IoT data, or any data for that matter, data for AI algorithms tend to be accumulated by the largest companies. Society is becoming reliant on data, and as it applied to AI algorithms, we are facing a situation in which a select group of organisations are amassing vast datasets and building unassailable AI capabilities. With the emergence of deep learning as the most useful machine learning technique for a range of AI applications like computer vision and natural language processing, data has become like digital oil. Digital monopolies like Facebook, Google and Amazon, today get data from users for free. Every like, search and purchase feeds the learning system to further improve the algorithms; in turn bringing more customers and engagement. In value chain terms, data is supply, and AI algorithms are demand. Digital monopolies are searching

“
Traditionally proprietary data and technology have been significant defensibility mechanisms for companies. In the blockchain industry this is all open source, leading to an incredibly rapid innovation cycle, but also shifting defensibility more towards the sheer size of the community and thus the distribution power. This is an industry where increasingly users decide what technologies they want to use.
”

Teemu Paivinen
Founder, Equilibrium Labs & Author
of Thin Protocols

everywhere for more and more data to feed their algorithms: Facebook buying WhatsApp and Instagram, Google with self-driving cars and Google Home, and Amazon with Alexa Echos and Dots.

Decentralised AI data marketplaces will reduce, and eventually remove, the competitive advantage of hoarding private data by enabling anybody to monetise data. Again in value chain terms, these marketplaces increase supply. An AI data marketplace will make it easy for people and increasingly agents and bots to recommend, price and therefore find value in different types of data. A market for data will lead to more efficient allocation of data, rather than giving it away for free or not using it at all. As more and more machines, individuals and organisations upload data to sell on a data marketplace, it becomes more attractive to data buyers. As this data commons grows with more datasets, it will attract more data buyers, creating powerful network effects. More than anything, decentralised AI data marketplaces are a bulwark to the rapacious AI data monopolies that have the potential to become the most powerful organisations ever built (if they aren't already), controlling ever-increasing numbers of industries and markets with their superior AI capabilities. It is, for this reason, we invested in the Ocean Protocol, whose mission is “to unlock data, for more equitable outcomes for users of data, using a thoughtful application of both technology and governance.”

We also expect to see these marketplaces become ever more automated and efficient. Another of our portfolio companies, Fetch.AI, is building a solution that uses decentralised machine

Previous page

²⁴ 'CryptoKitties, Explained ... Mostly - The New York Times' 28 Dec 2017, <https://www.nytimes.com/2017/12/28/style/cryptokitties-want-a-blockchain-snuggle.html>. Accessed 9 Feb 2018.

Current page

²⁵ HBR. The Biggest Challenges of Data-Driven Manufacturing <https://hbr.org/2016/05/the-biggest-challenges-of-data-driven-manufacturing>. Accessed 19 Jan 2018.

//

The aim of Ocean Protocol to to equalize the opportunity to access data, so that a much broader range of AI practitioners can create value from it, and in turn spread the power of data. To respect privacy needs, we must include privacy-preserving compute. Our practical goal is deploy a tokenised ecosystem that incentivizes for making AI data & services available. This network can be used as a foundational substrate to power a new ecosystem of data marketplaces, and more broadly, data sharing for the public good.

//

Trent McConaghy
Co-Founder, BigChainDB
& Ocean Protocol

learning to enable marketplaces to self-evolve around popular or valuable datasets, improving discoverability. And, as natural language and conversational interfaces continue to mature, there is value in dialogue couplets – and associated dialogue markets – which may be used to train and normalise conversations and chatbot content into increasingly relevant systems across a range of languages.

Personal Data Marketplaces

After peer-to-peer payments, control of personal data has been one of the most talked about applications for blockchains. This is related to but separate from self-sovereign identity, in the sense that once an individual controls their own identity, they can choose who can have access to it. The same principle can be applied to other personal data. This choice puts the individual in the position of the seller and the party who wants access to the data as the buyer. Personal data is an economic asset that we currently give up in return for services. Some data is handed over consciously, like entering an email address or a telephone number; other data is captured without us knowing about it: likes, tweets, our online behaviour and other forms of digital data exhaust. The value comes (albeit it is much less understood by individuals) when different datasets are aggregated, and an individual psycho-demographic profile is created and sold to all sorts of organisations like insurers, market researchers, and political organisations. A multi-billion dollar data industry exists just to trade personal data.²⁶

Individual pieces of personal data are not particularly valuable on their own. According to

the Financial Times, general information such as age, gender or location is worth just 0.0005 dollars per person. Buyers will have to fork out 26 cents per person for lists of people with specific health conditions. Genomic data would likely fetch much more. The challenge is that at an individual level, there is very little economic value. Value comes in aggregate. This is where blockchains, self-sovereign identity, and personal data wallets combine.

The key to making the economics work is pulling as much as data as possible into an individual personal wallet. Federico Zannier sold data including keystrokes, mouse movements and activity screenshots for two dollars per day on Kickstarter. An Italian university found university students would auction off their smartphone activity data for two euros. Add in other types of data such as voice, driving, health, learning, virtual reality and genomics, and the value of individual datasets will rise considerably.

In today's Web 2.0 paradigm, Google, Facebook and other data monopolists capture the profit. In the future, blockchain infrastructure, self-sovereign identity and personal data marketplaces will empower individuals. They can choose to allow Google and Facebook to use their data, or they can auction it off to get the best price. They might decide to only sell general information, but not their genomic data. Others will rent access to genomic data to cancer research charities but not insurers. New business models will emerge as buyers give sellers discounts based on aggregating family data for instance and new startups will emerge differentiating on consumer trust. Metâme is a UK-based startup working on creating a universal unit

²⁶ FT - How much is your personal data worth? <https://ft.com/how-much-is-your-personal-data-worth/>. Accessed 19 Jan 2018.

//

“Self-sovereign personal data marketplaces need to address two key hurdles before they can take off: 1) the need for a universal unit of trade that transforms personal data into assets which people can tangibly trade and own, 2) ensuring anonymity and then incentivising consented identifiability as new legislation like GDPR effectively calls for anonymity by default. Without solutions to these problems personal data marketplaces cannot scale sustainably.”

//

Dele Atanda
CEO, Metâme Labs

of trade enabling bundles of personal data to be packaged and exchanged. A data marketplace is not necessarily about making the most money. It is about giving individuals choice and control of how they want to invest their most valuable economic asset.

Digital Assets Marketplaces

The final category of marketplace we expect to evolve are digital asset marketplaces. Unlike traditional physical assets or money, distributed ledger-based crypto-tokens can be programmable. This gives them more flexibility and variety than their physical counterparts. Cryptocurrencies, or tokens designed to be a medium of exchange, are already reasonably well-defined and projects are innovating around how to create the optimal token for this use in mind with rules around supply, distribution, privacy, and other attributes being tweaked. Cryptocurrencies confer the fact that the crypto-token is a medium of exchange. Most tokens are incorrectly referred to as cryptocurrencies. This is probably because Bitcoin began life as a cryptocurrency and has over the last ten years become more of a crypto-asset, predominantly because of the programmed deflationary economics. However, currencies and assets require different economic designs. Currencies need to have a high velocity, whereas assets need to retain and ideally increase value resulting in low velocity.

Broader than cryptocurrencies, digital assets will come to include all digital assets that use distributed ledgers to create scarcity. Today there isn't a clear distinction between cryptocurrencies and crypto-assets, but as the market matures, it will

become more evident which tokens are designed to be a medium of exchange and which are designed to be a store of value. It is challenging to be both. Ether, for example, is intended to be used as a medium of exchange to redeem decentralised services from applications. But as its price rises, it becomes more of a store of value and less of a medium of exchange as holders refrain from redeeming Ether in anticipation of value appreciation. This non-fungible subclass of crypto-assets will be designed to be collectables and derive value through exclusivity and proof-of-ownership. Tooling for this is already emerging with the ERC 721 NFTs.

We expect to see a whole new ecosystem of digital assets like in-game weapons or costumes for gaming. AI bots and virtual avatar templates, such as those provided by SEED. Virtual reality land such as Decentraland; objects with real-world counterparts like digital twins; and even digital to physical assets like 3D printed items, many of which will be collaboratively made and collectively owned. With digital scarcity comes the ability to artificially limit supply which has up until now been almost impossible with existing digital and Internet technologies. The possibilities are endless and we are at the very beginning of a whole new age of digital assets created, bought, licensed, rented and sold in decentralised peer-to-peer marketplaces.

Process, Analyse & Automate

Now we get to the top layer of the stack: the process, analyse and automate layer.

This is where data is transformed into actions and insight using traditional and distributed computing techniques, as well as newer types of computing such as quantum computing. It is at this layer where blockchains and artificial intelligence blur and it becomes clear they are intertwined and interconnected. Both smart contracts and machine learning offer differing levels of automation and decentralisation depending on the type of input data and level of trust the use case demands.

Distributed Computation

Computation can be described as 'the action of mathematical calculation'. Modern methods trace their roots back to 1936 where at Cambridge University, Alan Turing described an abstract digital computing machine consisting of a limitless memory and a scanner that moves back and forth through the memory, symbol by symbol, reading what it finds and writing further symbols. In the Convergence Ecosystem, we expect to see computation just like storage and ledgers become distributed and decentralised. Over the last few years, there have been two types of computing that are regularly referred to: distributed computing and quantum computing.

Distributed computing refers to computing whereby a complex problem is broken down into more simple tasks. These simple problems are distributed out to a network of trusted computers to be solved in parallel, and then the solutions to these simple problems are combined in such a way to solve the main problem at hand. This is quite similar to how processors (CPUs and GPUs) developed from single-core to multi-core on the same circuit, and multiple cores were used to solve a problem more quickly than one core by itself. Although a simple premise, the other computers need to be trusted for the system to work. Conversely, blockchains and ledgers may be used to create networks of computers through a 'trust framework' and to incentivise these nodes to work together, rewarding those who solve these simple problems with tokens that have a financial value no matter how small. Blockchain projects including Golem and iExec are actively solving this problem. Other projects like Truebit are working towards off-chain computation in a trustless way using a prover-verifier game. Verifiable and non-verifiable distributed processing will both be needed again, depending on the level of trust between participants in the network.

Interestingly, we could finally see the realisation of the National Science Foundation Network (NSFNET) project from the 1980s, a supercomputer on-demand for any computing task. Other distributed computing projects like Nyriad are looking to achieve hyper-scale storage processing but without tokens using a concept called 'liquid data'.

Quantum computing is different to distributed computing in that it looks to solve problems that cannot be solved by existing computers (read: Turing Machines). By using quantum particles, the nascent technology has the potential to test all potential solutions to problems in one go in a single machine, rather than a network of machines. These machines pose a potential threat to blockchain technology because they are reliant on public key cryptography (also commonly used in banking for credit card security) which is made secure based on the difficulty of finding prime factors for huge numbers. These problems would typically take many hundreds or even several thousands of years to solve, but with quantum computers, this timeframe could be reduced to hours or minutes. Companies like IBM, Microsoft and D-Wave, are driving progress in the field.

Parallelisation is the core characteristic of both distributed computing and quantum computing. On the one hand, distributed computing involves networks of computers that look to solve a problem by solving smaller problems in parallel, while in quantum computing one computer is solving many complex problems simultaneously. In both cases, we can start to rely on networks of incentivised machines to solve computational challenges, rather than servers owned by

centralised entities. From an incentivisation perspective, blockchains enable these networks to work efficiently and 'trustlessly' with a token powering a marketplace of nodes with computing power. Quantum computers could also form part of these networks, solving the specific problems that the classical computers could not.

Smart Contracts

There are currently a handful of smart contracts blockchain platforms that have successfully captured the market. Ethereum dominates with over 7000 tokens launched on the ERC-20 protocol standard. Waves, NEO and Stellar, are all developing rapidly; NEO already has 30 sales scheduled to use the platform. In a nutshell, smart contracts are programmable "if this, then that" conditions attached to transactions on the blockchain. If situation 'A' occurs, the contract is coded to have an automated response 'B'. This idea isn't new, and we can find examples all around us, such as in vending machines: if button 'A' is pressed, then 'X' amount is required; if 'X' amount is paid, then snack 'B' is dispensed. By adding this simple concept to blockchains, contracts cannot be forged, changed, or destroyed without an audit trail. This is because the ledger distributes identical copies of that contract across a vast network of nodes, for verification by anyone at any time. When transparency can be guaranteed, these contracts now become possible in industries which would have previously deemed them too risky.

With correctly embedded legal frameworks, smart contracts will have the potential to replace and automate existing paper contracts.

Mattereum, a UK-based startup, is working on legally-enforceable smart contracts. The process of buying a house could become more efficient with no banks, lawyers, or estate agents. Countless hours, expenses and middle-men can be condensed into a few dozen lines of code and an automated product. This automation principle in blockchain-based smart contracts applies to any industry which requires trusted third parties to oversee agreements. Contracts are only as good as their enforcement, so decentralised dispute resolution services are necessary to make smart contracts useful. Early efforts in this direction are utilising prediction markets and reputation staking tools as with Kleros.

With the rapid development and convergence of AI and decentralised networks, we will begin to see more complex smart contracts develop, such as contracts which are connected to expansive neural networks. The development of these systems could see inconsistencies being found in legal frameworks, resulting in a more robust legal system. Smart contracts would be built upon those legal models, within which AI must comply.

It is still early in the development cycle of smart contracts and progress with require collaboration from the legal industry as well as lawmakers in Governments; smart contracts should be seen as the legal rails for the digital world. If tokens are the beginnings of digitally-native money and financial assets; smart contracts are the beginning of a digitally-native legal system. Smart contracts as with distributed computation and decentralised machine learning will automate data in the Convergence Ecosystem creating unprecedented levels of automation within auditable parameters.

//

Data and services are costly to use and can't sell themselves. It's staggering to consider all that gets lost without its value ever being realised – especially when it comes to intelligence constructed about markets and data. We simply can't let all that value be captured by a select few. Fetch has a mission to build an open, decentralised, tokenised network that self-organises and learns how to connect those with value to those who need it, or indeed may need it; creating a more equitable future for all.

//

Toby Simpson
Co-founder, Fetch

Decentralised Machine Learning

Machine learning is a field within computer science and more specifically artificial intelligence that focuses on enabling computers to learn rather than be explicitly programmed by humans. More traditional AI approaches based on rules and symbols are not capable of capturing the complex statistical patterns present in natural environments such as visual and auditory scenes, and our everyday modes of interaction such as movement and language. A relatively recent breakthrough in machine learning called deep learning is driving progress in the field. Deep learning techniques are 'deep' because they use multiple layers of information processing stages to identify patterns in data. The different layers train the system to understand structures within data. In fact, deep learning as a technique is not new but combined with big data, more computing power, and parallel computing it has become increasingly accurate in previously challenging tasks such as computer vision and natural language processing. The most recent breakthroughs in transfer learning and strategic play comes from the combination of deep learning and reinforcement learning as with DeepMind's AlphaGo.

Machine and deep learning techniques can transform raw data into actionable knowledge; converting voice input into text output in voice-to-text programs or turning LIDAR input into a driving decision. In diverse fields including image and speech recognition, medical diagnosis, and fraud detection, machine learning is equipping us with the ability to learn from large amounts of data. The current machine learning paradigm is where solutions are delivered as cloud-based APIs

by a few leading companies. But it is becoming increasingly apparent that this paradigm is not sustainable.

The Convergence Ecosystem provides global data sharing and marketplace infrastructure at the lower levels to enable AIs to collaborate and coordinate processing in a decentralised way.

As per the theme of this paper, centralised systems suffer from a few fundamental problems: inability to coordinate globally, limits on collaboration and interoperability, and the tendency toward monopoly and censorship. With machine learning becoming integral to our lives, centralised machine learning is a threat to economic competition and freedom of knowledge and speech.

The Convergence Ecosystem provides global data sharing and marketplace infrastructure at the lower levels to enable AIs to collaborate and coordinate processing in a decentralised way. This removes centralised bottlenecks for heavy computational workloads and helps address latency issues reducing the time needed to train models. On-device training like Google's Federated Learning model is a technical improvement but lacks the ability for mass coordination using marketplaces and tokens.

Decentralised machine learning not only provides a coordination mechanism for the more efficient allocation of resources, it increases access to machine learning capabilities but allowing anyone to submit models and algorithms and get paid based on quality and utility. SingularityNET, doc.ai and Fetch are examples of companies already building the type of decentralised artificial intelligence described. Decentralised machine learning will be the result but would not be possible without the development of distributed ledgers, consensus, identity, reputation, interoperability protocols and data marketplaces. This is why a holistic framework is needed to see the connectedness of all of these seemingly disparate innovations.

Conclusion

Blockchains and distributed ledgers are a core pieces of the new emerging decentralised data infrastructure.

The mistake commentators and analysts are making is approaching 'blockchain' as a new distinct market and compartmentalising: "We will make blockchain investments." Or "What is our blockchain strategy?" This way of thinking is built on old assumptions: computing takes place in an object called a 'computer'; tech companies develop products for the technology market, and industries are fixed markets with familiar competitors. The game has changed, and computing and data are everywhere. Technology firms have moved into healthcare, automotive and retail. Technologies and industries are converging. We need a new framework through which to understand this rapid change.

Blockchains are not just the technological innovation for cryptocurrencies or a new way to store digital assets; they are a foundational technology. They are a new decentralised digital infrastructure that solves technical, societal and economic problems that come from data centralisation in digital economies. As ever more data is collected by the Internet of Things and used to make decisions with artificial intelligence; data centralisation is becoming a threat to the successful functioning of markets. We cannot allow a handful of companies to have monopoly control of global data infrastructure.

The Convergence Ecosystem is the next era of economic and social activity. It will be open-source, distributed, decentralised, automated, and tokenised.

The Convergence Ecosystem

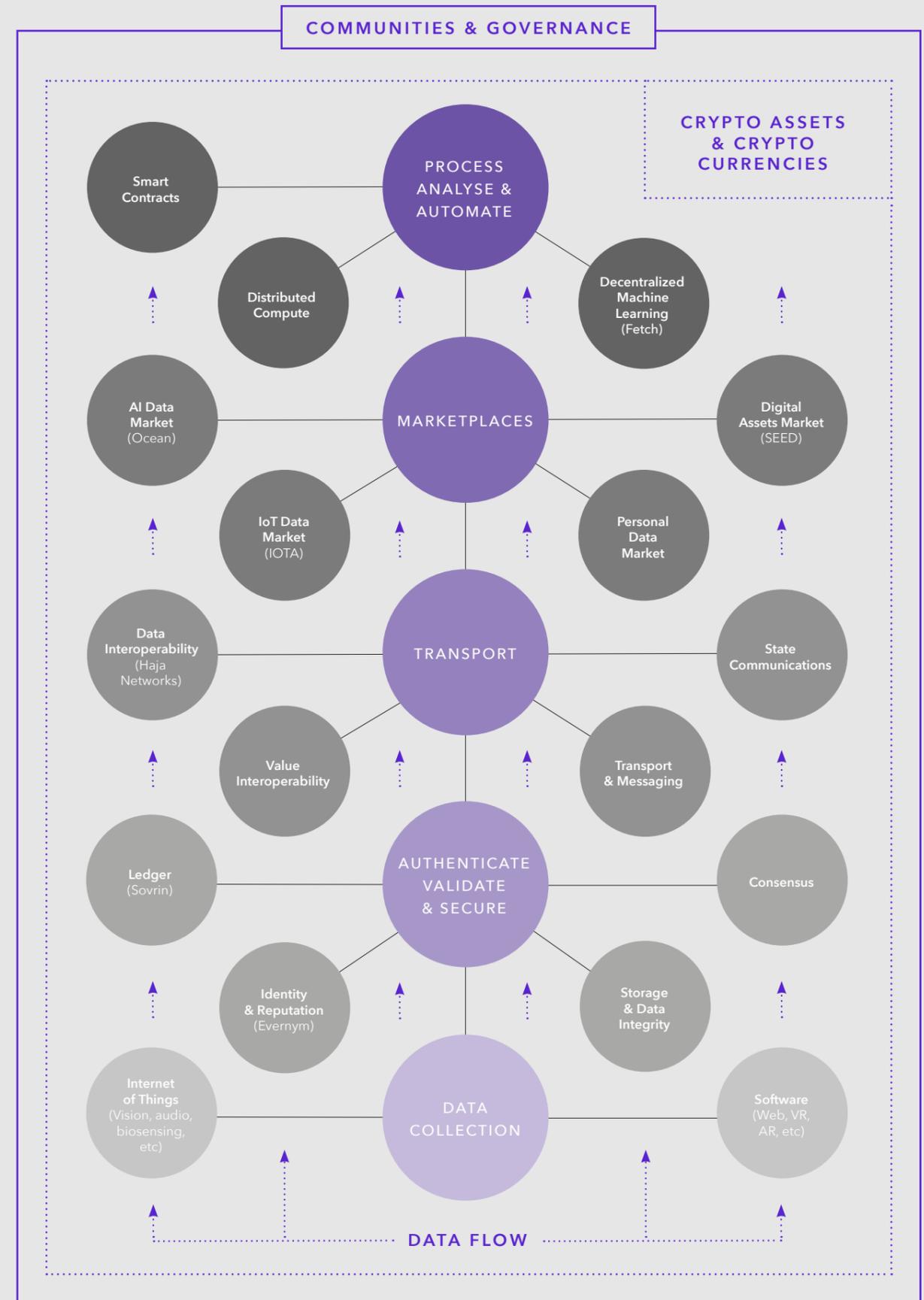


Figure 1. The Convergence Ecosystem

A decentralised data infrastructure is emerging to solve this problem. Blockchains and distributed ledgers combined with other tools like decentralised storage, consensus, and identity will authenticate, validate, secure, transport and share data collected from the physical and digital worlds. Data will then be packaged up in marketplaces to be processed, analysed and automated.

Different token designs including crypto-assets, cryptocurrencies and crypto-consumables will form an incentivisation system to allocate resources more efficiently. The entire ecosystem will be guided by governance models -- with differing levels of decentralisation and automation -- based on the values of the community. In much the same way that national governments all have their own cultural and historical nuance, token networks will develop similar subtleties. Paradoxically, the fact that the Convergence Ecosystem is driven by increasingly automated technologies means that people and communities will come to matter more than ever.

The Convergence Ecosystem is Outlier Ventures' vision of the future. The most successful networks, projects, and organisations within the Convergence Ecosystem will be those that have inclusive and aligned communities. Communities will develop around shared values and belief-systems such as censorship-resistance or self-sovereign identity. Successful projects will differentiate through values and trust. There will not be one chain to rule them all. We must change our mental models. The Convergence Ecosystem drives collaboration rather than competition.

We expect the Convergence Ecosystem to support hundreds if not thousands of communities that will over time outcompete their Web 2.0 competitors for developers and users. This shift will not occur overnight. People will continue to focus on the price of crypto-assets and worry about the regulatory implications of public token sales.

But behind the scenes, a new decentralised infrastructure is being built.

Network by network. Protocol by protocol.

The Convergence Ecosystem is the next era of economic and social activity. The revolution will not be televised - at least not over a private telecommunication network by a centralised television network - it will be open-source, distributed, decentralised, automated, and tokenised.

Successful projects will differentiate through values and trust. There will not be one chain to rule them all. We must change our mental models.

The Convergence Ecosystem drives collaboration rather than competition

Further Reading

01. Life 3.0: Being Human in the Age of Artificial Intelligence
- Max Telemark

02. The Stack: On Software and Sovereignty
- Benjamin H. Bratton

03. The Zero Marginal Cost Society
- Jeremy Rifkin

04. The Fourth Industrial Revolution
- Klaus Schwab

05. The Great Convergence
- Richard Baldwin

06. The Second Machine Age
- Andrew McAfee and Erik Brynjolfsson

07. The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World
- Pedro Domingos

08. [Money, blockchains, and social scalability](#)
- Nick Szabo

09. [Blockchain-enabled Convergence](#)
- Outlier Ventures

10. [Fundamental challenges with public blockchains](#)
- Preethi Kasireddy

11. [Disrupting Tech Monopolies & AI Tycoons – Part 1](#)
- Lawrence Lundy

12. [Disrupting Tech Monopolies & AI Tycoons – Part 2](#)
- Lawrence Lundy

13. [AI DAOs, and Three Paths to Get There](#)
- Trent McConaghy

14. [Wild, Woolly AI DAOs](#)
- Trent McConaghy

15. [The AI Existential Threat: Reflections of a Recovering Bio-Narcissist](#)
- Trent McConaghy

16. [Blockchains for Artificial Intelligence](#)
- Trent McConaghy

17. [The AI Economy & Bitcoin](#)
- Jonathan Frei

18. [The AI Hierarchy of Needs](#)
- Monica Rogati

19. [The Bitcoin Paradox](#)
- Simin Dedeo

20. [Blockchain Governance: Programming Our Future](#)
- Fred Ersham

21. [Byzantine political economy](#)
- Chris Berg, Sinclair Davidson & Jason Pott

22. [Identity and Digital Self-Sovereignty](#)
- Natalie Smolenski

23. [AI Software Juggles Probabilities to Learn from Less Data](#)
- Will Knight

24. [Is Quantum Computing an Existential Threat to Blockchain Technology?](#)
- Nathana Sharma

25. Quantum Technologies Flagship Final Report
- EU Commission Directive

For more information about the Convergence Ecosystem, or if you would like to contact us about speaking or an investment opportunity, please contact

For research or investment enquiries:

Lawrence@outlierventures.io

For marketing or event speaking enquiries

Matt@outlierventures.io

Member of



Design by www.studiobowden.com

Photography credits (in order):

Sarah Rider / Andrew Haimerl / Daniel Jensen / William Bout / Mathew Schwartz / Raj Eiamworakul / Markus Spiske

Outlier Ventures

www.outlierventures.io