

## WHITEPAPER

# The OSE Ecosystem, Backbone of the sharing economy

Romain Destenay, Conrad Lelubre, Julien Leroy

#### Abstract

## Contents

## I The Sharing Economy, Strengths and Weaknesses

## II Blockchains, Smart Contracts, Directed Acyclic Graphs:3 Milestones in Distributed Ledger Technologies

This section aims to provide background in distributed ledger technologies (DLTs). We retrace the evolution of DLTs going from Bitcoin to the most recents innovations being Directed Acyclic Graphs (DAGs).

#### 1 Bitcoin and Blockchains

From Don Tapscott's TED talk:

« For the past few decades, we've had the internet of information. And when I send you an email or a PowerPoint file or something, I'm actually not sending you the original, I'm sending you a copy. And that's great. This is democratized information. But when it comes to assets – things like money, financial assets like stocks and bonds, loyalty points, intellectual property, music, art, a vote, carbon credit and other assets – sending you a copy is a really bad idea. If I send you 100 dollars, it's really important that I don't still have the money –

and that I can't send it to you. This has been called the "double-spend" problem by cryptographers for a long time.

So today, we rely entirely on big intermediaries – middlemen like banks, government, big social media companies, credit card companies and so on – to establish trust in our economy. And these intermediaries perform all the business and transaction logic of every kind of commerce, from authentication, identification of people, through to clearing, settling and record keeping. And overall, they do a pretty good job. But there are growing problems.

To begin, they're centralized. That means they can be hacked, and increasingly are - JP Morgan, the US Federal Government, LinkedIn, Home Depot and others found that out the hard way. They exclude billions of people from the global economy, for example, people who don't have enough money to have a bank account. They slow things down. It can take a second for an email to go around the world, but it can take days or weeks for money to move through the banking system across a city. And they take a big piece of the action -10 to 20 percent just to send money to another country. They capture our data, and that means we can't monetize it or use it to better manage our lives. Our privacy is being undermined. And the biggest problem is that overall, they've appropriated the largesse of the digital age asymmetrically: we have wealth creation, but we have growing social inequality.

So what if there were not only an internet of information, what if there were an internet of value – some kind of vast, global, distributed ledger running on millions of computers and available to everybody. And where every kind of asset, from money to music, could be stored, moved, transacted, exchanged and managed, all without powerful intermediaries? What if there were a native medium for value?

Well, in 2008, the financial industry crashed and, perhaps propitiously, an anonymous person or persons named Satoshi Nakamoto created a paper where he developed a protocol for a digital cash that used an underlying cryptocurrency called Bitcoin. And this cryptocurrency enabled people to establish trust and do transactions without a third party. And this seemingly simple act set off a spark that ignited the world, that has everyone excited or terrified or otherwise interested in many places. Now, don't be confused about Bitcoin – Bitcoin is an asset; it goes up and down, and that should be of interest to you if you're a speculator. More broadly, it's a cryptocurrency. It's not a fiat currency controlled by a nation-state. And that's of greater interest. But the real pony here is the underlying technology. It's called blockchain.

So for the first time now in human history, people everywhere can trust each other and transact peer to peer. And trust is established, not by some big institution, but by collaboration, by cryptography and by some clever code. And because trust is native to the technology, I call this, "The Trust Protocol."

Now, you're probably wondering: How does this thing work? Fair enough. Assets – digital assets like money to music and everything in between – are not stored in a central place, but they're distributed across a global ledger, using the highest level of cryptography. And when a transaction is conducted, it's posted globally, across millions and millions of computers. And out there, around the world, is a group of people called "miners." These are not young people, they're Bitcoin miners. They have massive computing power at their fingertips – 10 to 100 times bigger than all of Google worldwide. These miners do a lot of work. And every 10 minutes, kind of like

the heartbeat of a network, a block gets created that has all the transactions from the previous 10 minutes. Then the miners get to work, trying to solve some tough problems.

And they compete: the first miner to find out the truth and to validate the block, is rewarded in digital currency, in the case of the Bitcoin blockchain, with Bitcoin. And then – this is the key part – that block is linked to the previous block and the previous block to create a chain of blocks. And every one is time-stamped, kind of like with a digital waxed seal. So if I wanted to go and hack a block and, say, pay you and you with the same money, I'd have to hack that block, plus all the preceding blocks, the entire history of commerce on that blockchain, not just on one computer but across millions of computers, simultaneously, all using the highest levels of encryption, in the light of the most powerful computing resource in the world that's watching me. Tough to do. This is infinitely more secure than the computer systems that we have today. Blockchain. That's how it works.

So the Bitcoin blockchain is just one. There are many. The Ethereum blockchain was developed by a Canadian named Vitalik Buterin. He's [22] years old, and this blockchain has some extraordinary capabilities. One of them is that you can build smart contracts. It's kind of what it sounds like. It's a contract that self-executes, and the contract handles the enforcement, the management, performance and payment – the contract kind of has a bank account, too, in a sense – of agreements between people. And today, on the Ethereum blockchain, there are projects underway to do everything from create a new replacement for the stock market to create a new model of democracy, where politicians are accountable to citizens.

So to understand what a radical change this is going to bring, let's look at one industry, financial services. Recognize this? Rube Goldberg machine. It's a ridiculously complicated machine that does something really simple, like crack an egg or shut a door. Well, it kind of reminds me of the financial services industry, honestly. I mean, you tap your card in the corner store, and a bitstream goes through a dozen companies, each with their own computer system, some of them being 1970s mainframes older than many of the people in this room, and three days later, a settlement occurs. Well, with a blockchain financial industry, there would be no settlement, because the payment and the settlement is the same activity, it's just a change in the ledger. So Wall Street and all around the world, the financial industry is in a big upheaval about this, wondering, can we be replaced, or how do we embrace this technology for success?

Now, why should you care? Well, let me describe some applications. Prosperity. The first era of the internet, the internet of information, brought us wealth but not shared prosperity, because social inequality is growing. And this is at the heart of all of the anger and extremism and protectionism and xenophobia and worse that we're seeing growing in the world today, Brexit being the most recent case.

So could we develop some new approaches to this problem of inequality? Because the only approach today is to redistribute wealth, tax people and spread it around more. Could we predistribute wealth? Could we change the way that wealth gets created in the first place by democratizing wealth creation, engaging more people in the economy, and then ensuring that they got fair compensation? Let me describe five ways that this can be done.

Number one: Did you know that 70 percent of the people in the world who have land have a tenuous title to it? So, you've got a little farm in Honduras, some dictator comes to power, he says, "I know you've got a piece of paper that says you own your farm, but the government computer says my friend owns your farm." This happened on a mass scale in Honduras, and this problem exists everywhere. Hernando de Soto, the great Latin American economist, says this is the number one issue in the world in terms of economic mobility, more important than having a bank account, because if you don't have a valid title to your land, you can't borrow against it, and you can't plan for the future. So today, companies are working with governments to put land titles on a blockchain. And once it's there, this is immutable. You can't hack it. This creates the conditions for prosperity for potentially billions of people.

Secondly: a lot of writers talk about Uber and Airbnb and TaskRabbit and Lyft and so on as part of the sharing economy. This is a very powerful idea, that peers can come together and create and share wealth. My view is that ... these companies are not really sharing. In fact, they're successful precisely because they don't share. They aggregate services together, and they sell them. What if, rather than Airbnb being a \$25 billion corporation, there was a distributed application on a blockchain, we'll call it B-Airbnb, and it was essentially owned by all of the people who have a room to rent. And when someone wants to rent a room, they go onto the blockchain database and all the criteria, they sift through, it helps them find the right room, and then the

blockchain helps with the contracting, it identifies the party, it handles the payments just through digital payments – they're built into the system. And it even handles reputation, because if she rates a room as a five-star room, that room is there, and it's rated, and it's immutable. So, the big sharing-economy disruptors in Silicon Valley could be disrupted, and this would be good for prosperity.

Number three: the biggest flow of funds from the developed world to the developing world is not corporate investment, and it's not even foreign aid. It's remittances. This is the global diaspora; people have left their ancestral lands, and they're sending money back to their families at home. This is 600 billion dollars a year, and it's growing, and these people are getting ripped off

Analie Domingo is a housekeeper. She lives in Toronto, and every month she goes to the Western Union office with some cash to send her remittances to her mom in Manila. It costs her around 10 percent; the money takes four to seven days to get there; her mom never knows when it's going to arrive. It takes five hours out of her week to do this.

Six months ago, Analie Domingo used a blockchain application called Abra. And from her mobile device, she sent 300 bucks. It went directly to her mom's mobile device without going through an intermediary. And then her mom looked at her mobile device — it's kind of like an Uber interface, there's Abra "tellers" moving around. She clicks on a teller that's a five-star teller, who's seven minutes away. The guy shows up at the door, gives her Filipino pesos, she puts them in her wallet. The whole thing took minutes, and it cost her two percent. This is a big opportunity for prosperity.

Number four: the most powerful asset of the digital age is data. And data is really a new asset class, maybe bigger than previous asset classes, like land under the agrarian economy, or an industrial plant, or even money. And all of you – we – create this data. We create this asset, and we leave this trail of digital crumbs behind us as we go throughout life. And these crumbs are collected into a mirror image of you, the virtual you. And the virtual you may know more about you than you do, because you can't remember what you bought a year ago, or said a year ago, or your exact location a year ago. And the virtual you is not owned by you – that's the big problem.

So today, there are companies working to create an identity in a black box, the virtual you owned by you. And this black box moves around with you as you travel throughout the world, and it's very, very stingy. It only gives away the shred of information that's required to do something. A lot of transactions, the seller doesn't even need to know who you are. They just need to know that they got paid.

And then this avatar is sweeping up all of this data and enabling you to monetize it. And this is a wonderful thing, because it can also help us protect our privacy, and privacy is the foundation of a free society. Let's get this asset that we create back under our control, where we can own our own identity and manage it responsibly.

Finally, number five: there are a whole number of creators of content who don't receive fair compensation, because the system for intellectual property is broken. It was broken by the first era of the internet. Take music. Musicians are left with crumbs at the end of the whole food chain. You know, if you were a songwriter, 25 years ago, you wrote a hit song, it got a million singles, you could get royalties of around 45,000 dollars. Today, you're a songwriter, you write a hit song, it gets a million streams, you don't get 45k, you get 36 dollars, enough to buy a nice pizza.

So Imogen Heap, the Grammy-winning singer-songwriter, is now putting music on a blockchain ecosystem. She calls it "Mycelia." And the music has a smart contract surrounding it. And the music protects her intellectual property rights. You want to listen to the song? It's free, or maybe a few micro-cents that flow into a digital account. You want to put the song in your movie, that's different, and the IP rights are all specified. You want to make a ringtone? That's different. She describes that the song becomes a business. It's out there on this platform marketing itself, protecting the rights of the author, and because the song has a payment system in the sense of bank account, all the money flows back to the artist, and they control the industry, rather than these powerful intermediaries. Now, this is —

This is not just songwriters, it's any creator of content, like art, like inventions, scientific discoveries, journalists. There are all kinds of people who don't get fair compensation, and with blockchains, they're going to be able to make it rain on the blockchain. And that's a wonderful thing.

So, these are five opportunities out of a dozen to solve one problem, prosperity, which is one of countless problems that blockchains are applicable to.

Now, technology doesn't create prosperity, of course – people do. But my case to you is that, once again, the technology genie has escaped from the bottle, and it was summoned by an unknown person or persons at this uncertain time in human history, and it's giving us another kick at the can, another opportunity to rewrite the economic power grid and the old order of things, and solve some of the world's most difficult problems, if we will it. »

#### From Ethereum Whitepaper:

« The concept of decentralized digital currency, as well as alternative applications like property registries, has been around for decades. The anonymous e-cash protocols of the 1980s and the 1990s, mostly reliant on a cryptographic primitive known as Chaumian blinding, provided a currency with a high degree of privacy, but the protocols largely failed to gain traction because of their reliance on a centralized intermediary. In 1998, Wei Dai's b-money became the first proposal to introduce the idea of creating money through solving computational puzzles as well as decentralized consensus, but the proposal was scant on details as to how decentralized consensus could actually be implemented. In 2005, Hal Finney introduced a concept of reusable proofs of work, a system which uses ideas from b-money together with Adam Back's computationally difficult Hashcash puzzles to create a concept for a cryptocurrency, but once again fell short of the ideal by relying on trusted computing as a backend. In 2009, a decentralized currency was for the first time implemented in practice by Satoshi Nakamoto, combining established primitives for managing ownership through public key cryptography with a consensus algorithm for keeping track of who owns coins, known as "proof of work".

The mechanism behind proof of work was a breakthrough in the space because it simultaneously solved two problems. First, it provided a simple and moderately effective consensus algorithm, allowing nodes in the network to collectively agree on a set of canonical updates to the state of the Bitcoin ledger. Second, it provided a mechanism for allowing free entry into the consensus process, solving the political problem of deciding who gets to influence the consensus, while simultaneously preventing sybil attacks. It does this by substituting a formal barrier to participation, such as the requirement to be registered as a unique entity on a particular list, with an economic barrier - the weight of a single node in the consensus voting process is directly proportional to the computing power that the node brings. Since then, an alternative approach has been proposed called proof of stake, calculating the weight of a node as being proportional to its currency holdings and not computational resources; the discussion of the relative merits of the two approaches is beyond the scope of this paper but it should be noted that both approaches can be used to serve as the backbone of a cryptocurrency. »

- Context: Revolution in finance after 2008 crisis
- Decentralized, distributed, no single point of failure, no unilateral decision, no government control
- Underlying tech: the blockchain. «Details»

#### 2 Ethereum and Smart Contracts

- State-transition, turing complete language + VM
- Smart contracts
- ICOs and ERC20
- Potential applications of smart contracts
- DAOs

#### 3 Limitations and Challenges with Blockchains

#### Proof of Work and the Environment

- Stats on bitcoin electricity consumption
- Failure of PoW
- Alternatives to PoW (PoS, PoA, DPoS, Master Nodes)

#### Mining, Validation Times and Fees

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### Scaling

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### 4 Directed Acyclic Graphs

As a solution to these problems, new distributed ledger structure emerged to replace blockchain, DAGs. Most notable ones bein Iota's tangle and Nano's block-lattice.

#### Iota and the Tangle

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### Nano and the Block-lattice Structure

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### III The OSE Ecosystem

#### 1 Vision

#### Becoming the backbone of the sharing economy

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### Giving the power back to the people

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### 2 Values

#### Openness, transparency

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### No centralized power

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### 3 Mission: Tools to Help the Creation of Sharing Economy Platforms

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### OSE Ledger

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### API and Modular Applications Creation

#### IV OSE Ledger in Details

#### 1 Operation

#### Nano reminder

Block-lattice, send + receive, no mining, no fees

#### **OSET**

Token transfered on our ledger

A small amount burnt at each transaction (fees, but not distributed to the miner, distributed to the holders and hedging providers = not bad for the environment)

#### Transactions with Milestones

Similar system (fork) with more possibilities than just send or receive:

- Send to many recepient / involve multiple participants
- Provide milestones in the transaction, at each milestone (usually someone's signature) some value transfer might happen between the participants and/or a hedging contract is started / transferred or ended
- When the transaction is complete the participants receive their tokens
- At any point, a participant can cancel the transaction?

#### 2 Security

#### Consensus with Delegated Proof of Activity

Activity = How much OSET burnt recently = stake transferred / time?

#### **KYC** and Privacy

#### KYC?:

- not mandatory, more services with KYC
- against sybil attack? only KYC delegate activity

Privacy achieved by ?? , necessary for example for restaurant to not learn about their competitors gross income through the ledger

#### 3 Fiat Conversion

- Decentralized exchange with JCash, USDT, TUSD?
- Solution like Request network?
- Becoming an exchange (too centralized?)
- Using centralized exchanges (Binance, Bitstamps, ?)

#### 4 Master Nodes

#### **Hedging and Future Contracts**

- Some participant can help the network by running such a node.
- It automatically «how?» accepts future contracts (cf Ethererum Whitepaper) in order to provide insurrance to the user that he'll get the same amount of value in the end. Hedge nodes are rewarded for accepting contracts (1.5%?).
- Contracts must have the ability to be chained

#### Oracles?

Oracles necessary if no DEX, otherwise just read the price on the DEX

#### Voting?

#### 5 Referer

A referer associated to each account. Possibility to change referer after KYC approval. Default = OSE Foundation.

As much token given to referer as burnt.

## V Modular Applications in Details

## VI BlockFood: A Proof of Concept

#### 1 Ethical food delivery

#### 2 Transaction example



Figure 1: This frog was uploaded via the project menu.

Item	Quantity
Widgets	42
$\operatorname{Gadgets}$	13

Table 1: An example table.

#### VII Conclusion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### Notes and Further Readings

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Use the table and tabular commands for basic tables — see Table ??, for example.

IFTEX is great at typesetting mathematics. Let  $X_1, X_2, \ldots, X_n$  be a sequence of independent and identically distributed random variables with  $E[X_i] = \mu$  and  $Var[X_i] = \sigma^2 < \infty$ , and let

$$S_n = \frac{X_1 + X_2 + \dots + X_n}{n} = \frac{1}{n} \sum_{i=1}^{n} X_i$$

denote their mean. Then as n approaches infinity, the random variables  $\sqrt{n}(S_n - \mu)$  converge in distribution to a normal  $\mathcal{N}(0, \sigma^2)$ .

Use section and subsections to organize your document. Simply use the section and subsection buttons in the toolbar to create them, and we'll handle all the formatting and numbering automatically.

You can make lists with automatic numbering ...

- 1. Like this,
- 2. and like this.

... or bullet points ...

- Like this,
- and like this.

You can upload a .bib file containing your BibTeX entries, created with JabRef; or import your Mendeley, CiteULike or Zotero library as a .bib file. You can then cite entries from it, like this: [?]. Just remember to specify a bibliography style, as well as the filename of the .bib.

You can find a video tutorial here to learn more about BibTeX.

We hope you find Overleaf useful, and please let us know if you have any feedback using the help menu above — or use the contact form at https://www.overleaf.com/contact!