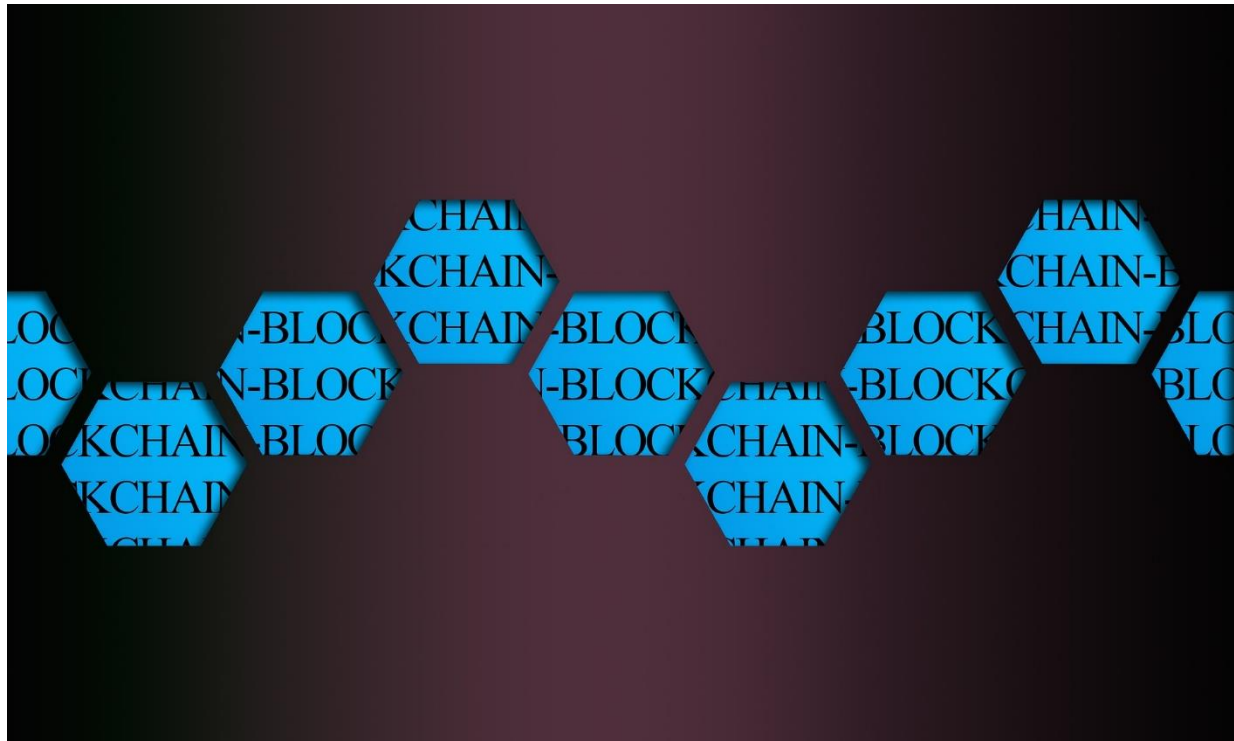# Total Record: The Blockchain Protocol Towards Post-Capitalism[1]

Guillaume Helleu & Anthony Masure

Abstract

The Bitcoin Protocol (2009) marked an extension of the utopias envisioned by the Crypto-Anarchists with the development of a secure and distributed online digital currency designed to escape the centralization of power by banks and governments. Hijacked [*récupérée*] in large part from speculative finance, these technologies, 'chains of blocks' (the blockchain), were progressive developments that widely surpassed applications in the traditional monetary field (distributed applications, smart contracts, tokens of value, etc.). Despite the persistence of certain social and technical breaking points, can the blockchain protocol work with, and even speed up, the destructive logic of contemporary finance capitalism?

Introduction

Adapted from the science fiction story, "We Can Remember It for You Wholesale" [*«Souvenirs à vendre»*] by Philip K. Dick (1966),[2] Paul Verhoeven's feature film, *Total Recall* (1990), exposes us to a tyrannical corporation that is exploiting the mineral resources of Mars. Frequently dreaming of a return to Mars, despite never having been there, Douglas Quaid (named Quail in the story) seeks the help of Rekal Inc. whom he tasks with implanting fake memories of a voyage he never had into his brain. In the story, human memory becomes a hard disk that can be rewritten (reprogrammed) from the outside without the subject being aware of any manipulation. In Verhoeven's film, Quaid wants to go to Mars to try to discover his true identity [*véitable identité*]. Inversely, in the novella, Quaid makes the choice to surrender himself to the Interplanatery Forces to save his life while having his past as a secret agent erased so as to not to succumb to any desires.[3] This story directly interrogates the fluctuating nature of the human psyche: "Had you really gone to Mars as an Interplan agent, you would by now have forgotten a great deal; our analysis […] shows that a variety of details are very quickly lost to the person. Forever. Part of the package we [Rekal Inc.] offer you is such deep implantation that nothing is forgotten."[4]

Death by Credit

The psychotic nightmare in Dick's novella worryingly prefigures the development of networks of information, in particular their ability to operate on a global scale as mechanisms of surveillance aiding in the alienation of populations. Exceeding anticipated dystopias, Chinese companies (Alipay and WeChat [Pay]) specializing in mobile payment, after 2013, began adopting and utilizing a three-digit credit score system. In parallel, after 2014, the Chinese government set in place [*a mis en place*] a social score ('social credit') designed to measure the 'reputation' of citizens, companies, or national organizations, with widespread adoption and standardization [*généralisation*] planned for 2020.[5] Since then, the GAFAM, the banks, and large Western companies began evaluating (and indeed, have been for a while) their partners and clients.[6] Further, the proliferation of data, along with companies' industrialized collection of it (via trackers, sensors, etc.), made possible the fantasy of a global,

---

[2] Philip K. Dick, "We Can Remember It for You Wholesale," in *The Philip K. Dick Reader* (Secaucus: Citadel Twilight, 1997), 305-322. [While I have the authors' original footnoted commentary, all citations have been standardized by me. Where a different version of the source text has been used, I have included my source and pagination.]
[3] The manager of Rekal Inc., McClane, concludes that fragments of memory have resisted reprogramming: "They couldn't erase that; it's not a memory but a desire." Dick, "We Can Remember It for You Wholesale," 310. [Technically, the line is uttered not by McClane, but by one of the laboratory technicians named Lowe.]
[4] Ibid., 308.
[5] Mara Hvistendahl, "Inside China's Vast New Experiment in Social Ranking," on *Wired,* published December 14, 2017. (https://www.wired.com/story/age-of-social-credit/)
[6] [GAFAM is an acronym of the web giants Google, Amazon, Facebook, Apple, and Microsoft.]

totalitarian registration system (*'total record'*) by migrating the centers of power from governments to private corporations (*data is power*). Against the *centralization* of trusted book-keeping systems [*des écritures fiduciaries*], the blockchain protocol, which appeared in 2009, allowed for the upset of saved records by the *distribution* of data via theoretically unbreakable technologies [*d'écriture théoriquement infalsifiables*]. Seen as the advancement of speculative capitalism by some,[7] such a development would represent yet another drift from neoliberal finance. Indeed, doesn't the study of the technological function of these unique architectures of information invite us to also interrogate the confidence placed in the existent (and centralized) systems of power?[8] In other words, could we ride the wave of accelerating capitalism by leaning on the technologies that have allowed for its reignition?

Crypto-Anarchism and the Beginnings of Electronic Money

Facing the widespread surveillance of the Web (and the world at large), the *cypherpunk* community born in the 1980s quickly understood that above the

alliance between States and banks was hovering a spectre: the spectre of drastic curtailments on individual liberty, a far cry from the utopias of the original information networks.[9] The recording and storing of human activities in massive, centralized databases controlled by States finally caught up [*rejoint*] with the worries pointed to in Dick's novella. Towards the end of the story, an Interplan officer addresses Quail, who is psychically incoherent due to the 'programming of artificial memories,' and threatens to reveal his past to another agent: "anything you think may be held against you [...] Not that it matters now; you've already thought and spoken yourself into oblivion."[10] In order to fight against the will [*la volonté*] of governments to restrict, or even forbid, data encryption technologies (which would, among other things, allow for the resistance to records of political opinions and mass surveillance), in 1983 computer scientist David Chaum proposed the concept of an electronic, anonymous, and untraceable system of currency.[11] This current of thought, located at the border of anarchism and libertarianism (rejection of distant power, rule, and centralization), connected with the current struggles of *post-capitalists:* to

---

[7] Pascal Ordonneau, "The Bitcoin Economy is Worse Than Subprimes," on *Les Echos,* published September 22, 2017. (https://www.lesechos.fr/idees-debats/cercle/leconomie-du-bitcoin-devient-pire-que-celle-des-subprimes-1011525) [Untranslated]

[8] Philippe Rodriguez, *The Blockchain Revolution: Algorithms or Institutions: Which Do You Trust?* (Paris: Dunod, 2017) [Untranslated]

[9] Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole*

Earth Network, and the Rise of Digital Utopianism (Chicago: University of Chicago Press, 2006)

[10] Dick, "We Can Remember It for You Wholesale," 315.

[11] David Chaum, "Blind Signatures for Untraceable Payments," in *Advances in Cryptology* (1982): 199-203. (https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF)

use the strategies of expansion intrinsic to capitalism to ultimately exceed its deleterious logic. While the crypto-anarchists wanted to use the techniques of surveillance capitalism (that is, the registration of data), they also wanted to add encryption protocols thus rendering the information 'unreadable,' thereby avoiding control. The ideal of emancipation espoused by David Chaum was furthered by computer scientist Timothy C. May who, in 1992, declared that "[j]ust as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions."[12] Later, the mathematician Eric Hughes placed more emphasis on the relation between collective emancipation and encrypted currency: "[w]e the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography [...], with digital signatures, and with electronic money."[13]

The Crisis of *Subprimes* and the Bitcoin Protocol

However, the idea of an electronic currency that could escape the banking system was not concretized until after a turning point in the mid-2000s: the *subprime* crisis of 2007 and the bank failures of 2008, events which showed the illusory nature of a dream of autophagic capitalism. *Derivatives* represented between 544 billion and 1.2 quadrillion dollars, more than the entirety of the global stock-exchange or all the currencies in circulation. Like bitcoin, the dollar is, in large part, 'digital': less than 10% of the accessible money (*narrow money*)[14] exists in a physical form – a trend that was considerably accentuated after the termination of the Bretton Woods system in 1971 (the dollar had previously been indexed by gold) [fig. 2].

The most well-known *crypto-asset* (an expression now widely employed), the Bitcoin Protocol and its eponymous currency (the bitcoin, with a small "b"), was released to the public in 2009 by the pseudonymous Satoshi Nakamoto whose identity as an individual or group remains a constant source of speculation. The relation [*la filiation*] to the crypto-anarchist movement was most clearly demonstrated in the first transaction with bitcoin (*genesis block*)[15] dated January 3rd, 2009 which occurred – probably with a hint of irony – on the same day that the *Times* wrote "Chancellor on brink of second bailout for banks."[16]

---

[12] Timothy C. May, "The Crypto Anarchist Manifesto [1988]," on *Activism.net.* Read by May at the Cypherpunk 1992 meeting. (https://www.activism.net/cypherpunk/crypto-anarchy.html)

[13] Eric Hughes, "A Cypherpunk's Manifesto," on *Activism.net,* March 9, 1993. (https://www.activism.net/cypherpunk/manifesto.html)

[14] Monetary Masses M0 and M1. See James Chen, "Narrow Money," on *Investopedia,* updated April 26, 2019. (https://www.investopedia.com/terms/n/narrowmoney.asp)

[15] [It should be noted that the "genesis block" and the first transaction are not the same thing. Indeed, the first bitcoin transaction between Satoshi Nakamoto and Hal Finney on January 12, 2009.]

[16] "Genesis Block," on *Bitcoinwiki,* n.d. (https://en.bitcoin.it/wiki/Genesis_block)
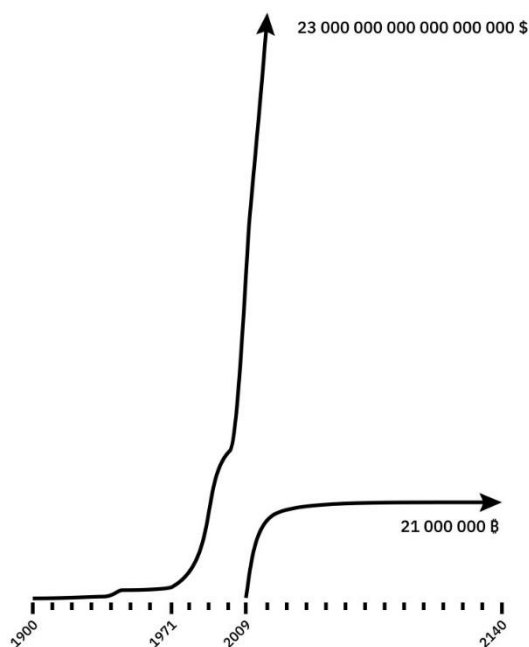
Fig. 2: Gold [and FIAT dollar]/Bitcoin Comparison
The Nixon Accords of 1971 [Nixon Shock] were followed by the hyperinflation of the dollar (issuance multiped by 57 between 1970 and 2018). In contrast to this exponential development, the issuance of bitcoins follows a logarithmic curve to ultimately reach the maximum number of 21 million bitcoins issued.

Bitcoin Today: The Triumph of Speculation?

Subsequently, bitcoin was largely captured [*récupéré*] by the forces of speculative capitalism with little concern for the anarchist ideology underpinning it. Unfortunately, the Winklevoss brothers, inventors of the ConnectU University Directory (Harvard), which was plagiarized by Mark Zuckerberg and became The Facebook, purchased massive amounts of bitcoins in 2013 via their venture capital fund.[17] Passing 0.00071 euros in 2009 to around 6,500 euros in March of 2018 after a price spike of 16,000 around Christmas of 2017,[18] bitcoin began appearing in the *mass media,* most of the time being discussed as a tool for fraudulent or nefarious economic activity (*ransomware,* drug purchasing, etc.), financial speculation, and environmental pollution by energy consumption. The study of the functional technique of bitcoin, however, provides a glimpse into other financial realities than simple returns on investments. Bitcoin is also used as a social tool by those roughly two billion people worldwide excluded from baking services.[19] These individuals on the economic margins 'could,' indeed, become their own banks.

A Public and Decentralized Registry of Transactions

At the level of technique, Bitcoin actualized the secular principle of a secure bank record in terms of cryptographic techniques (*Merkle Trees,* hash functions, asymmetric encryption, etc.) and the decentralization proper to the Internet's *client/server* architecture. Bitcoin took the form of a ledger [*un livre de compte*], analogous to a bank registry, but distributed (not centralized) and shared online. Incrementally broken up between all the nodes in the network, the

---

[17] Cameron Winklevoss, "Bitcoin: The Internet of Money," on *Winklevoss Capital,* published September 2014 [the authors have the date miscited as September 2013]. (https://winklevosscapital.com/value-investors-congress-presentation/)

[18] [I must add two things. First, these prices are not exact, rather they are relative figures. Second, for those in the U.S., the figures, respectively, are about $0.0008, $7,338, and $18,064.]

[19] Laurence Allard and Pierric Marissal, "Laurence Allard: Bitcoin Also Addresses Exclusive Banking," on *L'Humanité,* published December 13, 2017. (https://www.humanite.fr/laurence-allard-le-bitcoin-sadresse-aussi-aux-exclus-du-systeme-bancaire-647243) [Untranslated]

Bitcoin registry is shared via a *peer-to-peer* system [fig. 3]. The Bitcoin Protocol summarized a registry of all bitcoin transactions made on the network, that is to say the transfer of ownership of bitcoins from one entity to another. This mechanism, as a consequence and in contrast to the economies of debt, made it impossible to obtain a negative balance. As with most 'traditional' monies (so-called 'fiduciaries,' FIAT currencies, etc.), the 'materiality' of bitcoins resides in a registry with the key difference being that the Bitcoin registry is not a representation of value, but *is* value itself: bitcoins do not exist unless they are inscribed in the blockchain. The stories of people 'losing' their bitcoins on hard-drives or USB keys is, in fact, an abuse of language. There are, in reality, 'private keys' (access codes) which get lost and without which one cannot authenticate oneself on the network. We estimate that there are between 2.8 and 3.8 million bitcoins (about less than 20% of the available units) that cannot be recovered and are, therefore, indefinitely 'frozen' on the blockchain.
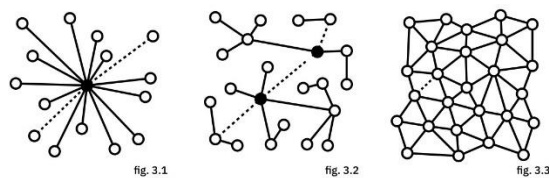

Fig. 3: Different Systems of Interrelations
Centralized [Fig. 3.1] (ex.: PayPal, Western Union), polarized [Fig. 3.2] (existent banking systems), distributed [Fig. 3.3] (bitcoin). Note that only the latter does not appeal to trusted third parties (black points) to function.

Operation of the Blockchain

Bitcoin transactions are not recorded one after another, but rather 'page by page' in blocks which hold a set of transactions that have been validated by the network at time T [fig. 1]. The workforce allowing for the validation and inscription of the 'chains of blocks' (*the blockchain*) is constituted by 'miners.' A miner (or 'node') is a person who contributes to the Bitcoin network by downloading the *open-source* registry software and allocating some of the computational power of their computer. The miners can, at any moment, submit their version of a new block (along with other miners) to insert into the registry. To write their 'page,' miners will select which other pending transactions waiting in the *memory pool* to include in their block. The most recent inclusions are sorted and classified by transaction fee, where those containing the highest fee are selected first.
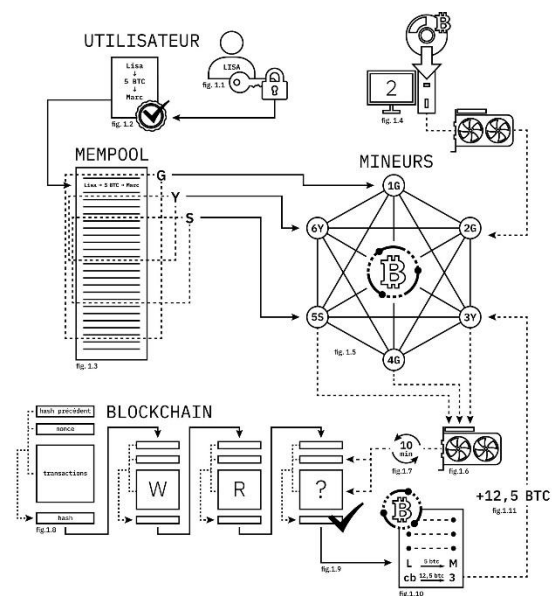
Fig. 1: Technical Operation of the Bitcoin Protocol
In order to send 5 bitcoins to Marc, Lisa must utilize her private key [Fig. 1.1] to sign the transaction [Fig. 1.2] which will be placed on hold in the mempool [Fig. 1.3]. The miners [Fig. 1.5], having previously downloaded the Bitcoin client software and allocated computing power to the protocol [Fig. 1.4], will select among the mempool the transaction to insert into their version of the block. The first miner to validate their block is able to submit it to the network and will be, among all the others (G, Y, or S), the one to have placed the new block. For this to work, the miner must 'hash' their

[6]

block by finding, with the aid of a nonce, a valid corresponding hash [Fig. 1.8]. The difficulty of the operation is calculated in relation to the total power of the network [Fig. 1.6] so that it takes, on average, 10 minutes to solve [Fig. 1.7]. Once the block is mined, it is inserted into the blockchain [Fig. 1.9] and allows Alice to see her transaction inscribed in the registry [Fig. 1.10]. The miner (3) who was able to mine the block is rewarded by a coinbase transaction [Fig. 1.10] which gives the miner, in addition to the transaction fees already won, 12.5 new bitcoins created by the protocol (a rate applied until 2020, after which it is reduced to 6.25) [Fig. 1.11].

A Consensus Algorithm

Since new versions of a block can vary from one miner to another, the protocol must make an appeal to a 'consensus.' Bitcoin rests on *Proof-of-Work* technology[20] which requires miners to 'validate' their blocks before submitting them. The miner must therefore exercise a sort of 'transformation' of their block via a '*hash* operation.' A hash function (Bitcoin uses SHA256) allows for the transformation of any set of numerical data into a product (following alphanumeric characters), called a 'hash,' which constitutes the 'footprint' (or 'cryptographic condensate') of the original data. This operation is irreversible and allows for the verification of a unique set of data corresponding to a specific *hash* (any modification would result in a *different hash*). This exercise consists of finding a new number (*nonce*) integrated into the new block such that it produces a result (*hash*) that respects certain characteristics of the network. The difficulty of this operation, which only depends upon computational power and time allocated on the network, automatically adjusts according to accumulated total power. If the work of mining is not indispensable to the functioning of the Bitcoin protocol, it is nevertheless essential [*primordial*] to ensuring the security of the system by raising the cost, both in terms of energy and in terms of capital, of fraudulent activity or an attack on the system.

Miners and Bounty Hunters

The miner who succeeds in submitting their version of the block wins all the 'transaction fees' associated with the block. The miner will also – and most importantly – be rewarded by the Bitcoin Protocol by being assigned newly created units (bitcoins). The automatic reward (*block reward*) is the only way unique bitcoins are created. This act of monetary creation (a *coinbase transaction*) has the distinction of being *disinflationary:* the reward in bitcoins decreases as the number of blocks increases. Since there are an arbitrary and finite number of 21 million bitcoins, this disinflation continues until the last one is mined around 2140. In April 2018, the date of writing this article, 17 million bitcoins have already been mined. These characteristics unique to bitcoin are why – with good reason – it is compared to gold: one can estimate current stocks, the mineral reserves still available, and annual extraction capacity.

---

[20] With the multiplication of crypto-assets, many variants of algorithmic consensus have been developed. Ethereum, for example, is working on the implementation of a Proof-of-Stake which would significantly diminish energy consumption as well as cutting down on biased retribution [*rétribution moins partiale*] for miners. The NEO Protocol, with the Delegated Byzantine Fault Tolerance (dBFT), prevents any fork in the blockchain.

Partial Anonymity and Authentication

Form the point of view of users, the Bitcoin blockchain only records transactions in the form of A → B. Contrary to existent banking institutions which authenticate a client's grace [*grâce*] and civil identity (full name, date of birth, address, etc.), Bitcoin operates by the pseudonymization of individuals. This *partial* anonymity (contrary to the popular belief of full anonymity) functions with the aid of a pair of 'keys' (*private and public*) based on a cryptographic technique called *asymmetric encryption.* These two keys, intrinsically connected to each other, are to encrypt and submit transactions to the network (private key), and to verify the authenticity of network requests (public key).

Ethereum: Distributed Applications, Smart Contracts, and Tokens of Value

While Bitcoin is the focus of media attention, it is only one of 1,500 *crypto-assets* that have been developed since its launch in 2009, some of which are particularly notable in terms of their technology. Developed by Russo-Canadian Vitalik Buterin, the Ethereum Platform (2015) proposes new protocols such as *smart-contracts* ('intelligent contracts' with automated triggering), *dApps* ('decentralized applications' not subject to capture by *app stores*), *ICOs* ('Initial Coin Offering' or participative fundraising) and tokens (generators of multi-use chips of value). If Ethereum was originally seen as an update [*mise à jour*] to Bitcoin, the difficulties associated with its implantation and governance have driven Buterin to create his own blockchain (Ethereum) with its own dedicated money (ether), primarily used to pay for the utilization of different services offered on the platform.

The Chronopolitics of *Smart-Contracts*

A concept invented by the crypto-anarchist Nick Szabo in 1993, *smart-contracts* have really only blossomed under Ethereum. By allowing for the shipment of all kinds of metadata in the blockchain, *smart-contracts* allow for the autonomization of predefined actions by the parties putting a contract into place [*mis en place*], for example, reimbursement for a ticket for a flight that has been cancelled [fig. 4]. To do this, it is sufficient that the traveler buy (with ethers) their ticket in the decentralized application (*dApp)* of the given airline. That ticket can later be materialized as a token specifically designed for this usage. The funds harvested by the application will be blocked through a *smart-contract.* This same *dApp,* by means of an 'Oracle' service (charged with entering the external data into the blockchain), connected to the airport's network will automatically trigger, via the *smart-contract,* a specific action defined by the signee(s). While these everyday cases, which are generally complicated to settle, are now solvable in minutes thanks to *smart-contracts,* other political uses are possible: payment of social aid, equal distribution and pay of and for tasks in collective projects (film, work, etc.), resale of surplus energy, etc. In addition, we have the possibility that anyone can issue tokens that represent money or any other note of unfalsifiable value (votes, concert tickets, video game items, real estate,

[8]

intellectual property, etc.).[21] If our current modes of life are driven by economic rhythms daily, weekly, and monthly, what would be the human consequences of contracts (debit or credit) executed in milliseconds (salaries, bills, etc.)? The domains of insurance, administration, energy, transport, media, etc. would be drastically transformed[22] by this form of *chronopolitics.*[23]
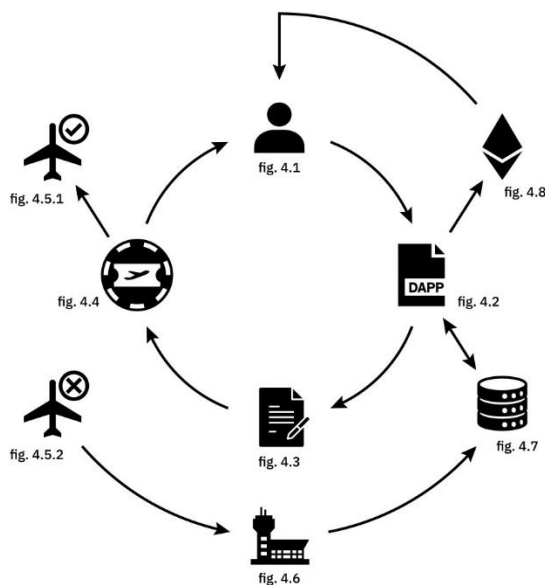
Fig. 4: The Operation of Smart-Contracts
The user [Fig. 4.1] will send ethers to the airline company's decentralized application (dApp) [Fig. 4.2] which will register the transaction with a smart-contract [Fig. 4.3] and create a token [Fig. 4.4]. This token will be spent (destroyed) during its utilization [Fig. 4.5.1]. If the flight is cancelled [Fig. 4.5.2], an oracle [Fig. 4.7] connected to the airport's network [Fig. 4.6]

triggers the smart-contract which reimburses, through the dApp [Fig. 4.2], the user in ethers [Fig. 4.9].

Hacking Protocological Capitalism

Since the possible uses of blockchains extend far beyond the narrow scope of monetary alternatives, nothing *a priori* prohibits the seizure of blockchain protocols to then be used for the rethinking of various architectures of power discussed above. It thus is yet to be known [*reste à savoir*] how to engage with the notion of *the protocol.* Researcher and media theorist Alexander R. Galloway[24] has maintained that these decentralized electronic systems do not oppose what Gilles Deleuze decried as "societies of control": disciplinary governments have been replaced by technical protocols with elusive localization and 'distributed' management.[25] A number of problems yet remain before we can render blockchain technologies humanely suitable: complete anonymity (for everyone) is not guaranteed, and the risk of a system of *global registration* where nothing could be forgotten would be socially problematic. The development of private blockchains (where the nodes in the network are limited and controlled) could undermine the original goal of

---

[21] Gonzague Grandval and Yorick de Mombynes, "Bitcoin, Totem and Taboo," on *Institut pour que l'Avenir ait Besoin des Nous Sapiens,* published February 7, 2018. (https://www.institutsapiens.fr/bitcoin-totem-et-tabou/) [Untranslated]
[22] Clément Jeanneau, Antoine Yeretzian, Alexandre Stachtchenko, and Claire Balva, "The Decrypted Blockchain: The Keys to a Revolution," white paper by *Blockchain France,* published in 2016. (https://blockchainfrance.net/decouvrir-la-

blockchain/la-blockchain-decryptee-les-clefs-dune-revolution/) [Untranslated]
[23] This idea of time-money is at the center of the dystopian film *Time Out* (Andrew Niccol, 2011) where money, replaced by life-time, forces us to work to live or accelerate death by spending.
[24] Alexander R. Galloway, *Protocol: How Control Exists After Decentralization* (Cambridge: MIT Press, 2004).
[25] [See Gilles Deleuze, "Postscript on the Societies of Control," in *October* 59 (Winter, 1992): 3-7.]

[9]

doing away with 'trusted third parties.' Another issue that remains unsolved is the energy usage associated with these protocols: nobody knows what will happen in the case of widespread adoption of blockchain protocols – the pollution already constitutive of societies of growth would be further exacerbated.[26]

Post-capitalist scenarios, first of all, necessitate a critical awareness vis-à-vis the effects and workings of blockchain technologies, and the subsequent risk of fetishization (*blockchain washing*),[27] to utilize such technologies as a necessary, but not sufficient, condition for the technological and material base underlying post-capitalist futures. This is why it is less about searching for new weapons, than deconstructing (hacking) the technological and semantic strata of the blockchain protocol in order to make them 'tactical media,' exploiting the *loopholes* of universal standardization to facilitate the emergence of a more free and democratic society. If "the technical is always political [and] network architecture is politics,"[28] the emergence of post-capitalist futures resides not in the destruction of protocols, but in the capacity to *hypertrophy*[29] their potential to invent new modes of life – or, absent that, expose the dead ends in the current system.

---

[26] Jon Stokes [listed as "partner content"], "One Day, The Stock Market Could Eat the Power Grid," on *Wired,* published December 2011. (https://www.wired.com/insights/2011/12/stock-market-power/)
[27] Ashton Kemerling, "No You Probably Don't Need a Blockchain," on *Ashton Kemerling*, published February 21, 2018.

(http://ashtonkemerling.com/posts/no-you-probably-dont-need-a-blockchain/)
[28] Galloway, *Protocol,* 245.
[29] Ibid., 176. "Techno-resistance is not outside protocol but at its center. Tactical media propel protocol into a state of hypertrophy, pushing it further, in better and more interesting ways."