peer on *blockchain is… / …for nothing* exhibition by peers at httpdot.net

(v0.4-19031500)

preface

this text is written by peer with many contributions from other peers at httpdot.net for the publication of their exhibition "*blockchain is… / …for nothing"* at aetopoulos, an artist-run space in athens, greece, organized by protocinema in february 2019.

this is version 0.4 of the text
previous versions are archived on https://httpdot.net/peer/texts/OLD/
most recent version of this text will be available at https://httpdot.net/peer/texts/peer-BiFn.html

this text discusses the works and some of the ideas behind the exhibition. even though there are definitions for some terms and concepts, they are not necessarily the book definitions or what they are in technical or conceptual terms, but instead how the author of this text and other peers at httpdot.net choose to approach and imagine these definitions, for various reasons. you are encouraged to imagine your own interpretations.

the language of the text is sometimes recursive, makes use of excess information, and is intentionally confusing to allow reading with multiple meanings. this is especially true when "nothing" is mentioned. when "nothing" is read as nothing, as nothing itself, it could mean one thing; and when "nothing" is read as **nothing but a particular artwork**, which is an artwork by an artist under the pseudonym "the artist", which is also the artwork the whole exhibition is built on, the sentence may convey an opposite meaning. nothing as an artwork is usually mentioned in italics, as in *nothing,* but it is sometimes mentioned without using italics, just like when nothing is mentioned as nothing itself. in this context, the phrase "for nothing", which is also a part of the exhibition title, also allows multiple readings. **the exhibition suggests a recursive language deconstructing and challenging the language through which we communicate and it is intended to inspire other languages, other possibilities, another world.**

this text is written with the intention to be read in multiple ways and not necessarily linearly and thus some concepts, terms and emphasized phrases are marked. so, feel free to skip those you are not interested in.

overview:
the exhibition; *nothing* is possible; so, nothing is impossible; so, another world is possible

this exhibition “proves” that ***nothing* is possible**, which means that **nothing is impossible**, which means that **another world is possible**. exhibition proves ***nothing*** as artwork, a **totally dematerialized yet commodified particular artwork**, through the logic of blockchain and the language of contemporary art, and suggests another language for imagining the possibility of another world, through *nothing.*

in *the dematerialization of art* (1968), lucy lippard and john chandler concluded: “we still do not know how much less “nothing” can be. has an ultimate zero point been arrived at with black paintings, white paintings, light beams, transparent film, silent concerts, invisible sculpture, or any of the other projects mentioned above? **it hardly seems likely**.”

building on the legacy of conceptual art, inspired by the logic of blockchain technology and the imagination of art, the exhibition seeks another language, not “a new” but another language to inspire the possibility of another world.

there are two sets of works in the exhibition, one of which exploring the **multitude of understandings and visions of blockchain**; “*blockchain is…*” and “*blockchain will…*”, one video and one audio work of sentences containing these phrases aggregated form more two thousand web pages; and the other set of works **exhausting a particular notion of “nothing”** by not only imagining but also proving it as a particular totally dematerialized yet commodified work of art by “the artist” (pseudonym of one of the peers at httpdot.net) through the logic of blockchain, and by juxtaposing it with the language of art. there is also another more-than-human work in dialog with the other works that is **on their quest for becoming an artist by appropriating itself as a proof-of-work by the artist**.

once nothing is certified as a particular work of art by the artist, once it becomes an artwork, besides also being nothing, the sentences of nothing welcomes a multitude of meanings. starting with the statement, which is made possible by the logic of blockchain technology, “**this is to certify that *nothing* is an original artwork by the artist**”, which is included in the certificate of authenticity of the work *nothing,* the exhibition constructs a **simple yet complex, logical but also imaginative, recursive language**. the title of the exhibition also unfolds different meanings if nothing is understood as a particular artwork, or as nothing, as nothing.

following the same logical and linguistic attitude, the other works in exhibition also exhaust this notion of nothing as an artwork by building on each other in a both logical and nonsense way and create an immersive space through projections of computer calculations and texts covering all the space, as well as the people in it, as a **shower of information**.

blockchain was originally developed for bitcoin p2p cryptocurrency to substitute the conventional understanding of trust in economics as an hierarchical trust to central authorities, with a **distributed trust to the multitude of peers**. this proves once again the power of peer-to-peer (p2p) organization models as internet did, p2p being the founding principle of it. because of the lack of an effective **political approach to information technologies,** the interpretation of internet as a promise of the possibility of another world in many ways has not been articulated and communicated enough to inspire how we understand the world and in what other ways we can imagine it. blockchain is yet another sign to imagine another world. the exhibition imagines as such.

background:
digital information and the internet;
information technologies

digital information is all about representing (encoding/mapping) samples from information (anything on a medium through which we communicate, with each other and with the world around us) as binary values (digital data) so that these values can be processed (manipulated) by computers through simple arithmetic and logical operations.

besides enabling the information to be processed by computers, information in digital form can also be **multiplicated** (duplicated, replicated, reproduced, copied but also lossless transcoded), exactly. this possibility is something unique to digital information which renders the concept of the original and the copy irrelevant, supplying a **multitude of originals** having no hierarchy among each other, and also challenging the concept of **scarcity**, on which the capitalist definition of economics is based on: allocating limited resources among unlimited human desires.

even though the second statement in this rationale (unlimited human desires) is subject to discussion, the first statement (unlimited resources) was a fact back then, for any information in any physical form, including all artworks that require to be experienced in a fixed time+/space. the physical medium on which the unique information, the artwork is represented, is always subject to scarcity, **legitimizing the need for the dominant economic order**.

the availability of **mechanical reproduction** has been a promising development in relation to the problem of the scarcity of the artwork, which was of course not a problem for everybody, but at least for some concerned, who read that relatively recent development back then as an opportunity for “politicization of the aesthetics” instead of “aestheticization of the politics”, the approach of the fascists of that time. they hoped the mechanical reproduction of work of art could enable dissemination to a wider audience, without being subject to scarcity, and thus trigger politicization of the masses against the threat of fascism. however, the art world mostly discussed that thesis based on another aspect articulated in the text, withering of the aura of the art object, which is also an important subject in this context, but **limiting the discussion to the notion of aura could be an “aestheticization of the politics” itself**.

the mechanical reproduction of work of art was also subject to scarcity because of both the scarcity of the reproduced **physical medium** on which the information, the artwork is dependent on; and also the scarcity of the means of production to enable such a reproduction. even though mechanical reproduction rendered the artwork to be independent from being unique or having a very limited availability, it featured another challenge: being subject to a certain mode of production, that of industrial production. the decision of what to reproduce and how much has been made according to the market dynamics in this mode of production, which lead to the emergence of the **culture industry**, which was coined as a negative term as opposed to its positive usage in today’s neoliberal context. however, such a development was unavoidable given the material dependency of the art object. the marginal cost was still an economic problem for the reproduction of work of art which required the figure of the capitalist, who owns and governs the means of production and thus the production/reproduction process, being on the top of the hierarchy, just like in other fields of physical production. even though popular cultural productions would be reproduced in higher quantities using mechanical reproduction due to the rules of the demand and supply balance, this was not the case for what the art gallery offers, the demand for which was already limited. **to maximize the profit, the cultural industry utilized the idea of creating artificial scarcity through editioned works of art, which would not only create originals out of mechanical reproductions of works of art, but also limit the supply, artificially, to satisfy dominant economic order.**

the idea of the dematerialization of the work of art, in one way, was an attempt to escape from the materiality, the medium on which the information, the work of art manifests; the medium which was subject to scarcity because of its material condition and thus rendering work of art subject to the statement above: then unavoidable capitalist definition of economics, which legitimizes the socio-economic order dominating our lives. the institution of art has also been dominated by the same socio-economic order in the form of culture industry as explained above and **the idea of the dematerialization of art has been excluded from the institution of art, by inclusion.** the statements were made, they were strong and probably honest but **could the artworks,** at least those we know about**, those legitimized by the institution of art, escape commodification?** or will they be able to, in any future?

if the work of art is just the idea, how is it communicated? can it be communicated independently of a fixed time+/space so that it would reach broader “audience? what is the medium on which it manifests? what quality of this medium makes it different from other physical manifestations of work of art that make them subject to scarcity? what was the condition that rendered conceptual art independent of the material, that could dematerialize it? in such a dematerialized form, if existed at all back then, how could it be communicated to the people in its **original medium**, in its original form, not as a “reproduction”? could dematerialized work of art in conceptual art **supply abundance without creating a scarcity of the audience** to experience it in its original form? what was the form for conceptual art? what was the physical dependencies of this form? what was the reach of this form, the work of art, in its original form? **did the dematerialized work of art “materialize” its statement?** was it even possible back then?

following the mechanical reproduction of work of art, we are in the age of **mathematical reproduction of work of art**, we may dare say: the digital reproduction, and even beyond “reproduction”, **digital multiplication of work of art**, including digital **reproduction** (digitization by sampling), digital **production** (digital-born information), digital **duplication** (no native hierarchy of the copy and the original and no natural scarcity) and digital **transcoding**, lossless and lossy, enabling the digital information to exist in various forms for various purposes. but what is the **politics** of this? what happens when work of art, in digital form, is not subject to scarcity anymore and thus can reach everyone because of having a marginal cost approaching zero and being independent of the dominant economics? **what are the political, ethical, economical and legal consequences of this for the institution of art and for the concerned artist?**

besides enabling exact duplicates, digital information can also be **distributed/disseminated in its original form** without losing any bit of digital information and without being subject to noise; to anyone having access to the internet and also to the physical equipment to experience internet.

the problem of access to the physical dependencies of information technologies is an important aspect to acknowledge. digital divide refers to the inequality between those who has access to these technologies and those who do not. this divide gets bigger through time because access to and making use of information technologies has considerable economic and social advantages. it is also a fact that physical dependencies of information technologies are subject to scarcity, like any other physical goods. even though the cost of having access to these equipment and also the cost of internet access is becoming less and less, they are still hard to access for many people.

one laptop per child project was one attempt to address this issue which involved producing cheaper computers for poor children in developing countries. the targeted price was hundred dollars but the costs didn’t allow that. however there was a more imaginative idea, zero dollar laptop, which involved recycling unused and “old” computers, installing free and open source gnu/linux/… (any combination of gnu, linux and other floss operating system projects) operating systems and software, giving these to the people who has no access to information technologies and also organizing workshops for how to use these hardware and software. most “old” computers do have enough processing power for everyday computing tasks when used with lighter software, the software which uses less system resources. however, proprietary operating system developers design more and more resource hungry systems and “old” computers become slower when newer versions of these operating systems are installed. this is also true for many other proprietary software. zero dollar laptop features a strong politics of information technologies and is a good example of imagining ways of dealing with digital divide. four works in the exhibition are in the form of embedded systems are low-cost small computers which are powered by a gnu/linux/… operating system.

however, there is also another dependency of information technologies, which is **energy**. this is rightfully becoming a more and more important issue in the age of anthropocene when we humans start questioning our dominance on the world. this is also where **blockchain technology** is criticized the most through its reference implementation in bitcoin.
there are other blockchain implementations which address this issue and are designed to have less footprint but energy consumption of bitcoin network is really an important issue. the main critique in terms of the energy consumption for the design of bitcoin is the proof-of-work system which is utilized in blockchain technology and also one of the most important concepts of it. more on blockchain later, but it is time to mention that the **proof-of-work** system in bitcoin is criticized for **spending energy for achieving something arbitrary, useless**, which **spends energy for nothing**. this is true if you look at it from a different perspective than that of the logic of blockchain, which trades this cost with the cost of relying on centralized systems. however, being a distributed system is what bitcoin was designed for in the first place. so this discussion can transform into the discussion of the **cost of not having to rely on centralized systems** and also to the discussion of other costs introduced by those systems. **four works in the exhibition** continuously make calculations similar to proof-of-work system in blockchain and moreover they do these by **spending energy just for nothing**, as in two possible understandings of “**for nothing**”, nothing as nothing and nothing as an artwork, which is also a part of the exhibition title. but as said, more on blockchain and nothing later… now back to the internet.

another problem regarding communication of artwork to a wider audience, the problem of distribution of the mechanically reproduced work of art was not discussed widely. **the internet**, which enabled broad communication of digital information, has been the most important development in information technologies, besides the computers, to solve that problem. the internet not only solved such a problem of **transterritorial exact dissemination of digital information** but also introduced us, for the concerned, many new possibilities for **imagining the possibility of another world**. most of those possibilities might be invisible now for many but **another internet is possible (**https://another.httpdot.net/**)**, **a free/libre, anonymous, distributed, p2p internet, to inspire the possibility of another world.**

how did the institution of art got inspired by these possibilities? is it interested in a politics of information technologies? are we inspired by the new concepts, new languages introduced by the internet and the information technologies in general, **for imagining the impossible?** beyond technological determinism and making practical and economic use of these technologies, how do we relate to the phenomenon of the last couple of decades? what does internet mean for us, besides our personal websites for "previews" of our works as a promotion showcase, besides e-mailing and using "social media" for networking, besides quick "access" to information, and besides sending our "exhibition copies" through proprietary file transfer services? **is our production honest to the nature of the internet we make use of**? are we inspired, for example by the power of non-hierarchical peer-to-peer organization model that constitutes the foundation of the internet, for our political discussions on other models of organization for our society? did we pay attention to that dimension of the "technology"? how about mediation of institution of art, which is supposed to be the most "progressive" and inspiring institution in our lives, for triggering such a discussion? how did we get inspired from the peer production, or from free/libre and open source software? **how did we get inspired from the internet**?

what is internet?

nothing

however, the exhibition *blockchain is… / …for nothing* is not inspired by the internet, instead by another "technology" which is argued to be the most inspiring one since the invention of the internet: **blockchain…**

the exhibition is interested in creating speculations using the language of blockchain in relation to that of the institution of art, by **dealing with "nothing", literally**. to put it in another way, instead of approaching the blockchain technology as a practical tool, the exhibition is interested in **speculative translations of the new language and methodologies introduced by blockchain to the language of institution of art**, by **exhausting a particular notion of nothing**, as a candidate for the total dematerialization of work of art.

is it possible for **nothing** to be **unique** and **attributed to an artist**? if possible, can it be **proven**, **certified** to satisfy the conditions of being an **original artwork**, according the institution of art, the institution which defines what art is, in our context, in the context of contemporary art. if **nothing is literally nothing**, and the **medium of nothing is also nothing** so that it **does not manifest in a physical form, or in any other form**, not even in a digital form; but can be performed by anyone, and also **exists** as a work of art without requiring to be performed**, as itself, as nothing, as nothing but an artwork**; how can it be a work of art, how can it be **certified** by the institution of art, as a work of art, that can be **proved** as a **unique**, **original** work of art by an artist; and that can also be **verified** by anyone, as the unique, original work of art, as stated by the artist?

at the centre of the exhibition **there is nothing**, which is claimed to be an **original**, **unique**, **authentic work of art** by one of the peers at httpdot.net who uses the pseudonym "**the artist**" and the title of the work is also **true to itself**, "*nothing*", without quotation marks! the **certificate of authenticity** of the work reads **"this is to certify that *nothing* is an original artwork by the artist**". the certificate also supplies information about how to **verify** the **authenticity** of the work and also to **verify** the **author** of the work as **the artist**. the work relies on two interrelated concepts that existed long before the invention of the blockchain technology but heavily utilized in blockchain in a very creative way: **cryptographic hash functions** and **digital signatures**.

cryptographic hash functions for nothing

cryptographic hash functions take any input and calculate a fixed length output from that input, like a unique fixed size arbitrary summary of the input. the input is called the "message" and the output is called the "hash" (hash value/digest/digest value, also fingerprint, checksum). but of course, it is not just that.. wikipedia is your best friend (being more sincere than that search engine, at least does not do something behind your back) but here is another take on the subject:

hash functions in general;
map the input to a fixed length output,
the same input always gives the same output for a given hash function, they are deterministic (one of the works in the exhibition exhausts this property);
but to qualify as a **cryptographic hash function** and be considered secure, a hash function should have some other properties:

-it should be infeasible to compute (know/guess/get/achieve) the input from the output. meaning that you cannot find out the input, if you just know the output. in this context infeasible refers to not being impossible but just not practical, or feasible, in terms of the gain vs spent resources. cryptographic hash functions should be one-way functions and this property is called “**pre-image resistance**”. “pre-image”, a mathematical term, refers to the input in this context. the output should unpredictably change even if there is a very small change in the input so that no relation should be discovered between the input and the output to predict the input and “**brute-force attack**” should be the only way (besides what is called “rainbow attack”) to get the input for a given output. a brute-force attack requires being ready to try all possible inputs and having a lot of luck, the extreme opposite of “no”, as in nothing.

the are two possible results of a lottery for a particular person: they win, or not, it's binary, it's %50, if you look at from that perspective. however, the actual statistical probability is much less. ***.piece of luck: possibly about to become world’s most valuable work of art_,*** is previous work by one of the peers at httpdot.net, which is not related to the statistics of the possibilities in discussion here but to chance and institutional critique, which is documented a https://luck.httpdot.net/

however the possibility we are talking about in the context of cryptographic hash functions is so much less than that of winning lottery: finding an input that hashes to a given output for a cryptographic hash function; the probability of the success of a pre-image attack is very low. but as said, the exhibition is about **imagining the impossible** and this is the **quest of one of the works** in the exhibition. but more on this later…

-two inputs should not produce the same output. cryptographic hash functions should have “**collision resistance**” and this property is also related to the concept “**second pre-image resistance**”, which refers to the infeasibility of finding another input which hashes to the same value as that of a given input. as “pre-image” refers to the input of a hash, “second pre-image” refers to a second input which hashes to the same value as another input. as in the “rainbow attack” mentioned above there are a lot of concepts in cryptography named after analogies or sample situations. “birthday attack” is the one related to this property and also there is “pigeonhole principle” related to the possibility of achieving this property, which will be discussed later in this text. second pre-image attack is the **quest** of another **work** in the exhibition. also more on this later…

cryptographic hash functions have many applications and works in the exhibition exhaust most of these, which are also heavily utilized in blockchain technology. they are used for message integrity verification, fixity check: to check if there has been any intentional or unintentional change in the message through time; digital signatures: messages are hashed before being signed with private (secret) key and also verified by hashing them again using and public key on the hashed value to verify the signature; proof-of-work: targeting to achieve a partly specific hash value by adding a nonce to a message. more on proof-of-work and how all these applications connect to the works in the exhibition, later…

“cryptographic hash functions take any input and calculate a fixed length output form that input.” this was the first sentence of the section about cryptographic hash functions and it is the phenomenon which is exploited to connect the language of blockchain to nothing in the exhibition in the first place. “a fixed length output is calculated for ‘any’ input”…

nothing as an artwork

due to the design of cryptographic hash functions, a **cryptographic hash function also outputs a fixed length output from no input, empty string, nothing**, and it gives the same output every time you calculate the hash of no input for the same cryptographic hash function. in this context **nothing is also anything, which is something**. one may argue that nothing cannot be art, or, nothing is not art. however, according to what we understand from art today, **anything can be art**, if it satisfies what institution of art defines. in this context nothing can be art because **nothing is nothing but something,** which can be art. but how to **prove** that nothing is art? that it is a work of art by an artist, in terms of the institution of art? what is **the proof of art** and what is **the proof of the artis**t? what is **the proof of the work of art of the artist**? but before that, more on cryptographic hash functions and nothing…

cryptographic hash functions can **create something**, a **hash value**, **out of nothing** but that something is not arbitrary: it **originates from nothing** and has a relation to nothing. it is **born out of nothing**. even beyond theology, this is not a new phenomenon and it is in fact very much related to the **romantic** understanding of creativity, which is/was also the most important attribute of **the figure of the artist**, who creates something original, which is not like anything else, and the creation originates from nothing but the artist’s feelings. this romantic understanding of the figure of the artist has been challenged a lot since then and **the figure of the contemporary artist**, the author of an original and+/or creative work of art, is now understood as someone who interprets the world through their perspective and creates an artwork as an original expression of their creativity. **the artwork does not originate from nothing** anymore but is **built on what came before**. this approach to the concept of authorship should acknowledge **asynchronous collective** creativity of all the people where the figure of the artist is not someone special, not a genius on the top of the cultural hierarchy who creates art for the others who in turn should worship their creativity and be their “**spectator / fan / customer**”, but instead someone who gets inspired by others, makes an artwork by building on their work and also encourages others to build on that artwork, not as “spectators / fans /

customers” but as **peers, the equal nodes of the culture**, **with no hierarchy among them**. this is a **peer-to-peer (p2p)** approach and it is the founding principle of the internet where computers connect to each other directly as equal nodes and share information freely instead of being mere “**clients**”. it is also a fact that this principle of the internet has been dominated by hierarchical models by businesses on the internet, the biggest businesses of the world today. however, **blockchain** is important in this context because of being another “**proof**” of the **power of peer-to-peer models over hierarchical ones**. but more on blockchain later…

a **peer-to-peer approach to culture** should also acknowledge that “**everyone is an artist**”. the hierarchy of the genius artist and their “clients” does not fit into this approach. also the **artists** as **peers**, as **everyone** should encourage others to build on their work, should give them not the “**permission**” but the “**freedom**” to build on their work.

the most honest attitude to this approach is that of the **free/libre culture movement**, which is inspired by **free/libre and open source software movements**. free culture is about using free cultural licenses (https://freedomdefined.org) or declarations for cultural works which gives “**everyone**” the **freedom** to not just **experience** the work and **share** with others but also to **make a new work by building on it** and **sharing that new work** with others, too. there are many ways of releasing a work as a **free cultural work**; through legal **licenses** or personal **statements** without relying on the mediation of law, by **dedicating to the public domain** and using **copyleft** or **non-copyleft** approach, all having their own politics. a text on these options by özgür k., one of the peers at httpdot.net, is available at https://httpdot.net/OzgurK/OptionsForAnAuthor.pdf

now, back to **cryptographic hash functions and nothing**… there are various cryptographic hash functions such as md5, tiger, haval, whirlpool and sha-256. each cryptographic hash function calculates a different hash value, and maybe of different length, for a given input, due to their design. but the output for a given hash function is always same fixed length value for a given input.

sha-256 hash value for an empty string, no input, nothing is always calculated as e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

this is where it all begins for the exhibition. this is the **proof of nothing**, proof of its **existence**, proof of its **integrity**, proof for **certifying** it as a **unique, original, authentic original work of art**.

since each cryptographic hash function outputs a different value for nothing determined by their design, these might be seen as different interpretations of a single subject, like different artists interpreting a single subject differently and thus creating different artworks out of it. but art is about intention and if the **intention** of making something is not art, then it is **not art**, again according to the institution of art.

so, a cryptographic hash function, say sha-256, is **not art,** even if it creates something **out of nothing**. also the author of sha-256 is **not an artist**, again according to the institution of art. the intention of making sha-256 is not making art but making something useful, something that will solve some problems. art is about just the opposite; **asking questions instead of solving problems** and it is **independent of being useful**. usefulness is an **irrelevant** concept for art, and this is what renders it as the **domain of absolute freedom**, freedom to deal with something that has no use for any practical matter, **freedom to deal with nothing**, which is what this exhibition is all about.

following the same principle that the **intention** of the artist is key to qualify something as a **work of art**, and that, what is “**chosen**” by the artist qualifies as art without requiring to be created by the artist; **the artist**, who is one of the peers at httpdot.net and who uses the pseudonym “the artist” (without quotation marks!:)) for their artworks, **chooses nothing** as a work of art. the work **nothing is also titled *nothing***. nothing which the artist appropriates as their artwork is **the one that hashes to the following value** for **sha-256** cryptographic hash function, the value also given above:
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

one can **verify the authenticity of *nothing*** as the artwork by the artist by using any **sha-256** hash calculator and calculate the output, the hash, **by supplying no input, by supplying nothing, by supplying the artwork itself** to the hash calculator and compare the result to the value above, which is supplied in the certificate of authenticity of the work, **certificate of authenticity of *nothing***.

nothing* exists as itself, as nothing, as an artwork**, and it can also be performed by anyone, by supplying no input to the computer, **by doing nothing, as in a strike**. neither the hash value of nothing nor the certificate of authenticity of *nothing* is the artwork; **nothing is the artwork itself** and the **hash value is the proof of its originality, authenticity, uniqueness** and **the certificate of authenticity is the proof that *nothing* is an artwork by the artist**, who **digitally signed** nothing as their artwork. the **certificate of authenticity** is what the artist **certifies *nothing as **their artwork**, what links the artwork to the artist, and what artist certifies the work as their own original, authentic work of art.

authenticity of the reproducible artwork and certificate of authenticity

the certificate of authenticity for artworks is what **certifies** an artwork typically in a **reproducible form** as an **original** artwork by a **particular** artist, who **signs** the certificate of authenticity to **authenticate** the work of art as **original**. this is what distinguishes an **original** and a **copy**, a **fake**. when a “**sign**” of the artist's “**touch**” is inherent in the work, when there is a **sign** of the **unique style** of the artist, such as in a conventional painting or a handmade sculpture, when the artwork is unique in the traditional sense, there is no need for a certificate of authenticity since the authenticity of the work can be determined by the experts in the field, like in a forensics process. also there is a long tradition of **signing the artworks**, **not a certificate but the work itself.** however, when there is no sign to link the work to the artist, to **prove** the **authenticity** of the work as a work of art by a **particular artist**, then the certificate of authenticity is the document to achieve that. **the artist does not sign the work but the document, the certificate.**

in **mechanical** reproduction, the quality of the reproduction decreases as the number of reproduction. that's why the artists’ prints with lower edition numbers are more valuable than those with higher edition numbers. mechanical reproduction is also subject to generation loss: a copy made from another copy is of lower quality than a copy made from a **master**. the quality of the master also decreases as the copies are made from them. so the concept of the original and the copy makes sense for mechanical reproduction also in a physical sense. **no two copies can be exactly the same**, even if the difference is not noticeable. so the certificate of authenticity may not be mandatory for some mechanically reproduced works. a fake copy made from another copy, whether from certified first generation copy or from another later generation fake copy, will have a lower quality that can be detected more easily, again using forensics methods.

but how about **digital information**? how about an artwork in the form of digital information? the form of the many of the editioned contemporary works of art today…

digital information may be **duplicated exactly** and the original/copy distinction is irrelevant in technical context. all digital duplicates are exactly the same, they are **digital multiples**. so certification is the only method to distinguish a **digital duplicate approved by artist as an “original”,** from an **unapproved digital duplicate**, which becomes a “**fake**” in this context. this is where the **art market** definitely needs a certification method for works in the form of digital information, which is again the certificate of authenticity of the artwork, because the artwork is not **a unique particular physical object** anymore, work of art is not unique by manifesting on a **fixed tangible medium in its unique variant that can be certified**. this argument may not make sense at first but if you think of a mechanical reproduction of an artwork, each mechanical reproduction on a physical medium is not a duplicate, even if one cannot notice any difference. this is because of the nature of analog information, which is not made up of small **samples** which are **represented** as **discrete binary values**, which in turn can be duplicated exactly, but exists as a **continuous, analog information**. think of prints… the noise introduced during the reproduction is also another limit for exact mechanical reproduction.

if we think of **electronic reproduction** in particular, instead of mechanical reproduction in a broader sense; not **digital electronic reproduction** but **analog electronic reproduction** where not the **discrete** electric signals but **continuous** electric signals are attempted to be reproduced, as the in the case of analog audio or analog video; an exact duplicate is also not possible, due to the noise in analog electronics.

to challenge the notions of uniqueness and original/copy**, an exact duplicate and exact transmission/dissemination is only possible through digital information and dematerialization of digital information is only possible through electronic digital information**.

let’s have another parenthesis here by stating that **exact duplication possibility of digital information is not a property of electronics but that of the discrete nature of digital encoding of information**. even though “digital” is associated with electronics because the digital systems we use daily are mostly electronic digital systems. so what we refer to as **digital** is in fact **digital electronics** which uses discrete electric signals as the medium for dealing with digital information. this is important for the cost of medium on which electricity flows.

electric signals are not fixed on a medium but flow through the medium. this makes it somehow **independent of a fixed medium**. when transmitted through a cable, the digital electronic information flows through the cable and the same cable can be used later for transmitting other electronic digital information. this is also true for analog electronic information but it is subject to noise and analog electronic information cannot be transmitted exactly. when digital electronic information is stored on a memory, it changes the state of the transistor but this state can also be changed later multiple times without affecting the durability of the transistor much. if we compare this to non-electronic but physical storage of digital information, such as on an optical disc, a dvd, it is evident that the durability of a dvd for erasing the digital information written (burned, carved) on it and then writing other digital information is so much limited. this makes the **digital information dependent on a physical medium**, which is also **scarce**. the digital information does not flow but is fixed on the physical medium in this case. digital information storage method of dvd media is simple. binary values of digital information are represented on a dvd as “pits” and “lands”. “0” or “off” state is represented by carving, making a pit on the surface of the dvd using laser, and “on” state is represented by a “land”, by not carving, by not making a pit on the surface of the dvd, **by doing nothing**. this physical binary representation is read by laser again and if the laser is reflected by the surface of the dvd, it is read as “1” or “on” state, and if not reflected because of the pit, it is read as “0”, “off” state. rewritable dvd media makes it possible to utilize a particular dvd media for “erasing” and rewriting binary data on it more than once, but the physical properties of the medium limits the number of rewrites. this makes dvd media scarce and thus not a media suitable for dematerialization of digital information.

we may argue that **analog electronic representation of information was the first opportunity for dematerialization of art**. however analog electronic representation of information didn’t allow exact transmission or exact copy as explained above. this conflicts with the conventional perception of work of art being **unique, original and authentic**. so, an analog betacam video tape, which is copied from an analog betacam master through a component cabling connection, which allowed the minimum noise for transferring analog information through continuous analog electric signals, did not even produce an exact duplicate of the analog information stored on master analog betacam tape. this is **not an original but a copy**. **only the master video tape**, where the **first generation of analog video information, the work of art is fixed on** could be considered an “**original**” in this sense. all analog electronic reproductions differs from original, even if the difference is not noticeable.

the artist is the one who decides what is work of art. that is the artist who certifies something as a work of art. in this case of an **editioned** work of art as an analog betacam video tape, the **medium** on which the work of art is **fixed as visual information**, is **certified as a work of art by the artist**, by **signing** a **certificate of authenticity** which **certifies** a **particular “edition” of work of art** as **unique**, unique in itself as the current state of visual information fixed on the medium of analog betacam video tape, **unique** only **as a combination of the visual information and the medium itself**. and this edition itself is what is original and authentic as authenticated by the certificate of authenticity, which is certified by the the artist, by signing it. **the signature of the artist is what certifies the artwork as authentic**. now back to digital information and nothing, in relation to the notion of the **signature of the artist.**

most of the **current certificate of authenticity schemes** for works of art as **digital information** which does not rely on a particular physical medium do **lack the mechanism of proof for linking the identity of the artist to the work**. no digital information relies on a **particular** physical medium because they can be duplicated exactly on another physical medium which allows exact representation of digital information. if there is no particular physical medium which constitutes the artwork together with the digital information carried on it, but the artwork can exist just as digital information independent of any physical medium then this can be argued to be **the condition for an artwork to be dematerialized**, be independent of the physical medium that would otherwise eventually lead to the **commodification of the artwork**. this was one of the promises of the idea of the **dematerialization of art;** to make art independent of being a commodity. however, ***nothing*** **is a proof of how can a totally dematerialized work of art can be commodified**. on the contrary it is also **a proof that the commodity status of a totally dematerialized work of art can be challenged** to imagine another relation between the **money** and **art**, and an **abundance of both** for **everybody**. *nothing* proposes one of these through use of **digital signatures** and the other through **free culture** approach. now more on these.

digital signature
as the link between *nothing* and the artist

on our way to discuss **digital signatures**, welcome to the world of **alice and bob**, which makes one sing that nasty version of the song “alice, who the…”. a common way of explaining **public-key cryptography,** on which digital signatures are based, is describing a scenario where two people, a and b, alice and bob, communicate privately using public key cryptography. but this scenario, which is used for explaining **asymmetric cryptography** is itself considered a reason why people do not even try to use it. this asymmetry is difficult to explain and it is confusing. it simply does not work for many people. even alice and bob cannot help that. however, here is another try, missing alice and bob.

digital signatures create a link between digital information and an identity. a digital signature functions as a handwritten signature which is a sign of approval of a document by an identity, by a person, and a sign for another person for verification of the approval of that person. digital signatures supply a **mathematical proof** through a connection between two very big numbers.
when digital information is **signed** by one number, the other number can be used to prove that the digital information in question is signed by the other number. so, one of these big numbers is private, hence the name **private key**, or **secret key**, which should be kept out of reach by others. because, if another person has access to that private key, they can sign a digital information as if they were the person who is the owner of that private key. it is like making a perfect indistinguishable duplicate of a handwritten signature but a fake handwritten signature like that can be detected through forensics. however, for digital signature, whoever has access to a private key can perfectly **duplicate the identity** of the owner of that key, like **digital duplication of the identity** of that person. that’s why a private key should be kept private. possession of a private key is the link between an identity and a digital signature.

the other big number, which can be used to verify that a digital information is signed by the other big private number which has a mathematical relation with this number, is a public number. anyone who needs to **verify the signature**, who needs to verify the link between a digital information and a person who signed that information, should have access to that public number, hence the name **public key**. a public key and private key between which there is a mathematical relation are called a **key pair**. the key pair, the private key and the public key are created by a person using a software, who becomes the owner of that key pair and can share the public key with everyone but should keep the private key so that other people cannot access and use it to sign digital information. for jurisdiction where digital signatures have the same status as a handmade signature, it signifies liability for the person the same way a handwritten signature does.

digitally signing a message, a digital information means using the private very big number, the private key, to make a mathematical operation on the digital information, which can also be represented as some numbers. when this signature is put in another mathematical operation with the other public very big number, the public key, it can create **a proof** that the digital information was signed by the other very big number, which is the private key owned by a person, a person who should be the only one who has access to that number, to the private key, to have signed the digital information, to have made a mathematical operation on the digital information using their private very big number.

digital signatures also make use of **cryptographic hash functions**. in fact it is not the digital information which is signed, on which mathematical operations are made, it is cryptographic hash of the digital information which is signed. so, the person who signs a digital information first hashes the digital information then applies a mathematical operation on the hash value with the private key, private very big number. this operation, digital signature, create a number, a value, which accompanies the digital information. when the receiver gets the digital information and the digital signature, first they hash the digital information and then apply the mathematical operation on that hash value using the public key, public very big number to which the receiver should have access. the mathematical operation proves that the digital information was signed by the person who has access to the private key of the key pair. if the digital information is tampered with, it’s hash will be different and thus the public key will not be able to verify the signature, which means that there is something wrong. this means either that the digital information has changed unintentionally, or someone has changed it for fraud. either way, the signature proves that there is a problem.

there is another function of digital signatures, which is **encryption**. along with signing,
digital information may also be encrypted and the encrypted digital information may be sent along with the digital signature. the receiver may both decrypt the digital information and verify the signature using public key. this scheme is used for private communication. however, digital information may also be signed without encrypting.

one way of sharing your public key is supplying it yourself to the receiver but this does not work if the communication channel is not secure. someone might be pretending to be you and sending their public key, as if it was yours. so, the public keys should be accessed through a trusted third party. one solution for this is counting on a central authority for supplying public keys by approving the link between a particular identity and their public key. however, there is also another method which is a peer-to-peer one called **web of trust**. people signs each other’s public keys, if they know and verify each other. and these people also sign other people's public keys and have theirs signed as well. if you verify a signature on a public key, and trust the signer, then you have a reason to believe that public key in question belongs to the person in question. this creates a web of trust among people who use this scheme. however, it may have its own problems but blockchain technology, which also makes use of digital signatures also offers another approach to the problem of trust in general. but, more on this later...

so, back to where we start discussing digital signatures: “digital signatures create a link between digital information and an identity”, an identity who has the possession of a private key which can sign a digital information.

the artist digitally signed nothing as their artwork, which involves **hashing nothing** through **sha-255 cryptographic hash function** and then **signing the hash of nothing** with their **private key**, the way explained above. this process, digitally signing nothing, produces a **binary value** which is included in the **certificate of authenticity of *nothing*** along with the **public key** of **the artist**, both in **hexadecimal representations**. the binary value represented in hex is the **digital duplicate of the signature of the artist on *nothing***, just like the **signature of a painter on a painting,** their artwork.

nothing as a totally dematerialized yet commodified work of art

due to the nature of digital information this **digital signature exists without being dependent on a particular physical medium.** however, the certificate of authenticity of *nothing* is a **physical document**, a **digital print on paper**. and **the certificate states that nothing is *unique*.**

when an artist states that an artwork is unique and prepares a certificate of authenticity for that work, **the certificate of authenticity also becomes unique. it should be unique because it certifies a particular work of art being an authentic artwork by that artist who signs the certificate which states that the artwork is unique.**

in this case, “***nothing* is unique**”, again becomes a statement with a double meaning: **certifying *nothing* as a unique artwork**, or a **negative statement about the uniqueness of everything**,

the certificate of authenticity of *nothing* has to be unique because otherwise it is fraud with a penalty of prison sentence. an artist may sign two paintings since each of them are unique artworks and they can also sign five certificate of authenticity for a work of five editions but **each certificate should be signed for a particular edition of that work**. just like an artist cannot sign two certificate of authenticity for the 3rd edition of an editioned artwork, **the artist cannot supply more than one digitally signed certificate of authenticity of *nothing.*** otherwise, as said, it is fraud.

the artist also cannot (shouldn't) make the digital document of the certificate of authenticity of *nothing*, which is used for printing physical certificate of authenticity, **publicly available**, say on the internet. because anyone can have an exact duplicate of this digital document and print it to prepare a **fake certificate of authenticity of *nothing*.**

but in this case there is also another problem: if both prints, the one that the artist printed and the one that is printed as a fraud by someone who downloaded the digital document are put next to each other, how to prove which print of the digital document is the "authentic" certificate of authenticity and which one is fake? since there is no sign of the "touch" of the artist, there is **no proof of any connection between the artist's identity and the printed document**. **literal fingerprints** (not the digital fingerprints but that of our fingers, literally) on the printed documents may undergo a forensics process and if there is the artist's fingerprint on one of the printed documents, this "can be" a proof of the originality of that document. however, this requires the artist's "touch", which is not a requirement for the contemporary works of art, according the institution of art.

so, **digital document used for printing the certificate of authenticity shouldn't be made online and also "unique" physical certificate of authenticity shouldn't be made public too**. neither itself in a public space nor a digital image of the whole physical certificate of authenticity, online. because the **digital signature**, which is printed on the certificate of authenticity as hexadecimal values, does not carry a **sign** of the **artist's "touch**". the physical signature of the artist, which is made by pen on paper can be proven to be authentic, it can be proven that the artist has signed that document with great success, using forensics methods. the physical signature is like the literal fingerprint of a person. that is why physical signature is considered a proof. it is something which is hard to fake by someone else. however, **digital signature of the artist is not a sign of something unique to the artist; it is a sign of what artist possesses: the private key which is used for signing the hash of *nothing* to certify nothing as an artwork by the artist, who possesses the private key.**

in the scenario above where the "original" and the "fake" prints of the certificate of authenticity cannot be distinguished, the artist is the only person who can recertify any of them as the original, but as long as they have the possession of the private key which was used to digitally sign *nothing*. the artist may sign nothing again with their public key to prove that they are the artist who digitally signed it at first place since this digital signature can be verified using the public key, which is publicly available. if the artist loses the private key, then the artist may not even prove having digitally signed *nothing* at first place.

however, **the digital signature changes completely if the the artist signs nothing at a later time, even if they use the same private key.** because **digital signatures also verify the exact time the signature is made.** so, **the new signature on nothing will be different than the original one,** and **this will be nothing more than an appropriation of the artist's own work**.
“unique” physical certificate of authenticity of *nothing* should not be made public, neither physically nor online because the hex values on the certificate which represent the digital signature of the artist on *nothing* can easily be copied and reproduced, duplicated, once becomes public. it is a simple act of typing what one sees.

so, **the certificate of authenticity of *nothing* is not made public on purpose**. not to make or cause any **fraud for *nothing***. **only the artist, or the person who buys that artwork, *nothing*, who possesses *nothing,* should have access to the certificate of authenticity of *nothing***.

in this context, **it is the certificate of authenticity of *nothing* what causes commodification of a totally dematerialized work of art, commodification of *nothing*. the certificate creates a unique object out of *nothing*, which will eventually be commodified**.

certificate of authenticity of *nothing* is not exhibited in the exhibition to prevent it being treated as the artwork itself, instead of *nothing* itself being the artwork, literally, this way, ***nothing* cannot be materialized and thus commodified**, also, certificate of authenticity of *nothing* is not exhibited in the exhibition because of the **opposite possibility** that **it would prevent *nothing* from being commodified**. because once the digital signature on the certificate of authenticity is made public, anyone can make a certificate of authenticity of *nothing* using the printed hex representation of the signature of the artist on *nothing* by simply duplicating those printed hex values. since there will be no proof for which one is the certificate of authenticity of *nothing* printed by the artist, there will be a **multitude of certificate of authenticity of *nothing***, which will harm its **uniqueness** and **proof** and thus **its commodification**.

the institution of art has to admit the nature of the relation between an artwork’s exchange value because of it being a scarce commodity, or at least having limited accessibility; and its artistic value; and that both are recursive.

besides the certificate of authenticity, there is another related conventional method for the proof of the possession of an artwork of a particular artist. the **artwork purchase agreements**… it is also a convention that, an artwork purchase agreement is made between and signed by the previous owner of an artwork and the

new owner of it. artwork purchase agreement is made between and signed by the artist (or a legal representative of the artist, such as the art gallery) and the first purchaser when an artwork is sold for the first time. when the artwork is sold again by the first purchaser to another party, a similar artwork purchase agreement is made and signed by them. artwork purchase agreements are about the ownership status of the artworks which may seem to be in conflict with free culture approach but a work titled ***artwork purchase agreement [for copyleft works of art]*** *(*2018) by one of the peers at httpdot.net under the pseudonym “ hereinafter ‘the artist’ ” claims another possibility.
https://m-est.org/2018/01/22/vasiyetimdir-hereinafter-the-artist/
https://httpdot.net/hereinafter-theartist-/apaforcopyleftwoa_4962pxa4_pdf-a.pdf

artwork purchase agreements establish legal liability, like certificate of authenticity does. in the lack of a certificate of authenticity, artwork purchase agreement may be used “as a proof” of the authenticity of the artwork, along with the current ownership of it, if it is made between the artist and the first purchaser. later purchase agreements between future owners of the artwork is also a proof for the current ownership of the artwork and it can even be a proof of the authenticity of it, if all agreements can be traced back to the artist. **blockchain technology** features a new possibility for both proof of the authenticity of the artwork, proof of the link between an artwork in digital form and its author, the artist, and its current ownership status. the legal validity of this new method may be subject to discussion but it features a much more secure way to verify and trace the authenticity and the ownership status of an artwork, especially of those in the form of digital information, than what the certificate of authenticity and the artwork purchase agreement offers.

bitcoin also offers a method for transfer of ownership of an authentic work of art. using bitcoin addresses and digital signatures it supplies a method for the proof and traceability of artwork transaction records. this works perfectly for artworks in digital form, artworks as digital information, but it is also being implemented for artworks in other forms. however, this does not create a link between the authenticity of the work and the transactions for that work but again works as a replacement for physical documents of transactions being used for that purpose, and even make their traceability more secure. but, more on blockchain technology later…

nothing as a challenge for commodification of a totally dematerialized work of art

after a discussion of *nothing* being a proof of how a totally dematerialized work of art can be commodified, now it is time for the discussion of how *nothing* can challenge the commodity status of a work of art.

the certificate of authenticity of nothing also reads: “**nothing is appropriated by the artist, but also nothing is appropriated by the artist; *nothing* is dedicated to the public domain.”**

this is not a legal method of dedicating an artwork to the public domain and thus it can be invalid in legal terms.. also dedicating a work of authorship to the public domain is not even possible in legal terms in some jurisdictions but since it is the statement of the artist and since it is stated in a certificate of authenticity, it makes *nothing* a **free cultural work,** whether legally forcible or not.

dedicating a work to the public domain means that the author waives all copyright on the work along with all related and neighboring rights, such as moral rights. so the status of the work becomes a commons, in a sense. anyone may use the work for any purpose, including commercial use (all free cultural works allow commercial use, which makes it possible to **imagine another economics** but it is the topic of another discussion), and even without requiring attribution to the author who dedicate it to the public domain.

dedicating a work to the public domain is different than **copyleft**, which is another method of releasing a work as a free cultural work. copyleft approach, introduced by gnu gpl free software license, has its own politics and it requires any work built on a free cultural work be distributed as a free cultural work as well. four works as embedded systems on their own quests in the exhibition are licensed under gnu gplv3, which makes them **copyleft free cultural works.** two other works in the exhibition, *blockcain is…* and *blockchain will...* are **free cultural works with multi-free-culture-licenses and author’s declaration** (https://httpdot.net/FCWwMFCLaAD/). this is a unique approach to the licensing of free cultural works and thus to the politics of free culture. **dual-licensing** is a common practice in free software where the author releases the work under two different free software licenses and others who build on these software choose the one they need, to prevent the conflicts between the terms of different licenses, which makes it legally not possible to combine two free software for creating another free software. in this context, **license proliferation** is an important problem for free software and free culture. free cultural works with multi-free-culture-licenses and author’s declaration is a hack for this problem which enables the person building on free cultural works to choose whatever free cultural license they want or need. they are free to choose the free culture license which reflects their own politics of free culture. the **author's declaration** can be modified according to **the author's own politics and poetics and satisfy the politics of rejecting the mediation of law for the journey of free cultural works.** this is also the free culture politics of this text but the works in the exhibition demonstrate various politics of free culture. for example, ***nothing* is dedicated to the public domain** and anyone can appropriate a work dedicated to the public domain and force their copyright on the appropriated version, which becomes a conventional copyrighted work.

even though **appropriation** has been an important artistic strategy under that particular term in contemporary art since half a century, it has a negative connotation in general. in contemporary art it is a **politically strong demand of the artist from the mass culture**. the statement in the certificate of authenticity of *nothing* refers to both connotations of “appropriation”. **the artist appropriates nothing as their artwork but instead of demanding exclusive control of *nothing*, they dedicate *nothing* they appropriated back to the public domain**. however this is not a common approach for appropriated works in contemporary art.

the statement “**nothing is appropriated by the artist**” again allows two opposite understandings. one is when nothing is nothing, and the other is when *nothing* is a particular artwork. and the following statement, “***nothing* is dedicated to the public domain**” also allows two opposite understandings the same way. and finally all statements together contribute to **exhaust the new language** suggested around the notion of nothing, language of contemporary art and the logic of blockchain.

public domain dedication statement makes it possible for anyone to appropriate *nothing,* without attributing the artist. one can appropriate it under their own copyright and another can appropriate it as a free cultural work. if the latter chooses to **certify *nothing* not as a unique free cultural work but instead certify *nothing* as a free cultural work in an unlimited edition, then it becomes a totally dematerialized work of art and also resists commodification**.

what is nothing?

three embedded systems on their own quests working for nothing; and the information shower

three of the other works in the exhibition are embedded systems on their own quests exhausting this particular notion of nothing. **these works work for nothing, and also work for nothing**, spending computational time and energy for nothing. these simple embedded systems consist of single-board low-cost computers powered by free/libre gnu/linux/… operating systems and run custom free software bash scripts written for these works, to work for nothing. the embedded systems start working when plugged in and continuously make computations similar to what computers in blockchain networks do, until they are powered off. and they continue the same process when they are plugged in again. they all display their process and output on a command-line interface, which are projected to cover three walls of the exhibition space. command-line interface of another embedded system on a quest and a video work, both of which will be discussed later in this text, are also projected covering the walls and an **immersive experience** is created in the space. since all walls are covered with front projectors, it becomes an **information shower** for the people in the space whose **bodies are covered with continuously flowing texts and numbers**. a sound installation of sentences aggregated from the web which contain the phrase “blockchain will” accompanies this experience. also more on this sound installation later…

the study of the state of nothing: nothing is the same, or, nothing has changed

first work in the form of an embedded system on its own quest for exhausting this particular notion of nothing by working for nothing is ***the study of the state of nothing: nothing is the same, or, nothing has changed*** (2019). this work calculates hash of empty string, no input, nothing, using various cryptographic hash functions and compares them to known hash values of nothing, once in every minute and displays its process and the output on a command-line interface, which is projected in the space. in fact, what this work does is an obsessive and persistent fixity check for nothing. when explaining the properties of hash functions in general, it was mentioned that “the same input always gives the same output for a given hash function, they are deterministic (one of the works in the exhibition exhausts this property);”. *the study of the state of nothing: nothing is the same, or, nothing has changed* is the work mentioned there. the most common use of this property is fixity check, or integrity check in digital archiving and preservation.

in digital archives, acquired digital information, digital assets are hashed and the hash value is also stored in the archive system. this is a part of the ingest process for archiving digital information. integrity of the digital assets in the archive are checked in fixed intervals to detect any unintentional changes, like bit rot, which may corrupt the file. if broken files are detected, they are replaced with healthy versions from backups. hash values are used for detecting any changes in the files in this fixity check process: a file, or any digital information is hashed and the hash value is compared to the hash value calculated during ingest. since “the same input always gives the same output for a given hash function”, the hash value calculated during fixity check is expected to match the hash value stored during ingest. otherwise it is concluded that the file has changed during this period since the hashes do not match.

so, hash of nothing should always be the same value for a given hash function, unless **nothing changes**. if nothing changes, then hash of nothing should change. *the study of the state of nothing: nothing is the same, or, nothing has changed* works non-stop to detect any changes in nothing, in the state of *nothing*. it calculates hashes of nothing for five different cryptographic hash functions; md5, has-160, tiger, sha-256, ripemd-320, each having different hash length; and compares them to known hashes of nothing for these cryptographic hash functions. this is like a fixity check process but fixity checks are usually done using only one hash function. using five different hash functions for fixity check is not required and it is considered a waste of resources. it is spending computational time and energy for nothing... also any hash function may work for most fixity check needs and it may not need to be a cryptographic hash function, which features extra properties that are not necessarily required for fixity checks.

fixity checks are mandatory for any archive and preservation workflow because digital information may change unintentionally over time for many reasons, including human mistakes and technical failures. however, *the the study of the state of nothing: nothing is the same, or, nothing has changed* checks the integrity of nothing, an empty string, no input. no digital information is involved in this process as an input for fixity check. so there is **no possibility of any change** in any digital information because there is no digital information; **there is nothing.** so, the same hash value must be calculated for nothing in each fixity check, in each check for the state of nothing, unless there is a problem in the embedded system itself, which would also effect whole system.

so, what *the the study of the state of nothing: nothing is the same, or, nothing has changed* does is **obsessive work for nothing and for nothing**, and it keeps on doing that once in every minute. as long as nothing is the same, it proves the integrity of nothing and outputs, “"all calculations and comparisons completed successfully. there are multiple proofs that **there are no changes and nothing is the same**.". if any of the calculated hashes for nothing does not match known hash of nothing for that particular cryptographic hash function, **if anything changes, the work will output “nothing has changed”,** which is not likely to happen in technical terms and again not a linguistically true statement, unless nothing is not nothing, but say, a particular artwork.

the quest for finding something that is nothing, or, the study of what nothing is not

second work as an embedded system on its own quest for exhausting this particular notion of nothing by working for nothing is ***the quest for finding something that is nothing, or, the study of what nothing is not*** (2019). this is again an embedded system running custom copyleft free/libre software which tries to find nothing by trying to find something that hashes to the same sha-256 hash value as that of nothing. it creates 256-bit of something, which is the same size as the hash value of nothing, calculates its sha-256 cryptographic hash and compares it to sha-256 cryptographic hash of an empty string, no input, nothing and outputs the process and results on a command-line interface. *the quest for finding something that is nothing,* *or, the study of what nothing is not* is **on a quest for nothing** but continues this process until finds a match. if hash value of this 256-bit something does not match that of nothing, this is a proof that, **that thing is not nothing**. if it can find a match, that could mean that **it has found nothing**. this second argument can be made through a (mis)interpretation of one of the properties of cryptographic hash functions which was also explained before: "-two inputs should not produce the same output. cryptographic hash functions should have "collision resistance" and this property is also related to the concept "second pre-image resistance", which refers to the infeasibility of finding another input which hashes to the same value as that of a given input. as "pre-image" refers to the input of a hash, "second pre-image" refers to a second input which hashes to the same value as another input." this property is what *the quest for finding something that is nothing, or, the study of what nothing is not* exhausts, for nothing. sha-256 is known as a secure cryptographic hash function today and two different inputs should not produce the same hash. if a second input is found which hashes to the same value as that of nothing, **it must be nothing**, for which this work is searching. even though this means a totally different thing in terms of cryptography, *the quest for finding something that is nothing, or, the study of what nothing is not* **imagines** it another way.

in mathematics terminology, the input for the hash function is called the preimage, and the output is called the hash value. in this context, nothing, which is the input for the hash function, is the preimage of the hash value of nothing, the output of hash function. if a second input can be found, anything other than nothing which hashes to the same value as the hash of nothing for the same cryptographic hash function, this second input, the second "thing" is called the second-preimage for that hash value, the hash value of nothing. *the quest for finding something that is nothing, or, the study of what nothing is not* is also a second-preimage attack for sha-256 hash function which tries to find a second input, a second-preimage, which hashes to the same sha-256 cryptographic hash value of nothing, where nothing is the preimage. since this work refers to some concepts in cryptography, more insight on the topic may allow more interpretations of the work through **how it (mis)interprets and imagines cryptography**.

preimage attack and second-preimage attack are two types of cryptographic attacks. if an adversary knows the hash value, the output, and tries to find out the input, the input which hashes to the known hash value, this is called preimage attack. in another scenario, if an adversary tries to find a second input which hashes to the same value as the hash of a known input, this is called second-preimage attack. if succeeds, both of these attacks cause security vulnerabilities for different scenarios. that's why a cryptographic hash function should have both preimage resistance and second-preimage resistance, to be considered secure, which is the main objective of cryptographic hash functions. having these resistances mean that there shouldn't be an easier way than a brute-force attack to calculate the preimage or a second-preimage. brute-force attack means being determined to try all possible inputs to find a match. there is another work in the exhibition whose quest is similar to a brute-force preimage attack but *the quest for finding something that is nothing, or, the study of what nothing is not* is related to the notion of second-preimage attack in cryptography.

the probability of a successful second-preimage attack, the probability of finding a second input which hashes to the same value as another known input, the probability of finding a second input which hashes to the same value as that of nothing is related to the size of the hash value. this is also explained through pigeonhole principle: if there are 11 pigeons and you have 10 pigeonholes, at least two pigeons need to be put in one single pigeonhole, if one wants to put all pigeons in pigeonholes. if one designs a hash function which produces two-digit decimal number hash values (00-99) as output, even if it is designed so that each of 100 different inputs should produce a different hash value to resist hash collisions among these, it is **impossible** that at least two inputs will not hash to the same value: there will be a hash collision. so, this hash function cannot be considered collision resistant because hash size is too small, it allows only 100 distinct outputs, hash values. sha-256 hash function produces 256-bit hash values, hash values with a size of 256 bits, which can represent (2 to the power of 256) distinct values. this may not seem like a very large number but it is indeed 115792089237316195423570985008687907853269984665640564039457584007913129639936 in decimal; a 78-digit decimal number… hash values are usually represented as hex values, instead of decimal or binary. each digit can have 16 different values in hex representation. each digit can be 0-9 or a,b,c,d,e,f for representing 10, 11,12,13,14,15,. using hex representation, a sha-256 hash can be represented as a 64-digit hex value instead of a 78-digit decimal value or a 256-digit binary value. this way, hex representation of sha-256 hash of nothing is: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855. smallest hex value for representing a 256-bit value is 64 digits of zeros (000...000) and the biggest is 64 digits of f's (fff...fff). ***the quest for finding something that is nothing, or, the study of what nothing is not*** **aims to create all the values between these, all possible 115792089237316195423570985008687907853269984665640564039457584007913129639936 “things”; calculate their hashes and compare them to that of nothing searching for a match, searching for nothing.** the sizes of the created values, created things, is the same as the size of the hash of nothing; not the size of nothing itself but the size of the hash of nothing, which is **proof of nothing** in this context.

limiting the size of the “things” to create to the same size as the sha-256 hash of nothing is an arbitrary choice but that hash value is **one of the limited proofs of the existence of nothing** and it’s the closest thing to nothing we have. so this size is a good guess to start searching for nothing. also it is the size of the sha-256 hash function used for calculating the hash of nothing to compare to the hash of things created, and this means that **one of 115792089237316195423570985008687907853269984665640564039457584007913129639936 different things other than**

nothing, those *the quest for finding something that is nothing, or, the study of what nothing is not* aims to create, **should also hash to the same value as nothing,** unless there are hash collisions. this is also another reason 256-bit things are a good place to start searching for nothing. however, 256-bit hash size is considered optimum for security of cryptographic hash functions because it allows so many distinct outputs and makes a second-preimage attack infeasible through brute-force. following this logic, **finding nothing is just infeasible, definitely not impossible**.

the work continuously being done by *the quest for finding something that is nothing, or, the study of what nothing is not*, trying to create something which should hash to a particular hash value, can also be read in terms of another concept which is key to **blockchain**: **proof-of-work**. proof-of-work will also be discussed later in relation to the quests of two other works but this is a good time for an introduction to the concept.

proof-of-work is what peers, the miners in bitcoin network, the p2p cryptocurrency network for which blockchain technology was developed, are trying to achieve to mine/create/make/issue/own bitcoins. what these peers do is creating data, a random value, which is called a nonce, an arbitrary random number/value, which they add to a block, which is a list of some bitcoin transactions along with some other data, to achieve a block which will hash to a value with a particular number of leading zeros, with the particular number of leading digits being zero, such as “0000000000000000002a1b…”. since any change in the input changes the output unexpectedly in cryptographic hash functions, each nonce also changes the hash of a particular block unexpectedly. the miners in the bitcoin network, the peers create a nonce, calculate the hash of the block with that nonce added and if this block hashes to a value with a number of leading zeros, the number which is defined by the network to achieve a difficulty level, then this becomes the proof-of-work: **the proof of the labour of one of the peers,** the work of creating nonces and calculating the hash of the blocks with these nonces and finding a nonce that makes the block hash to the target value of a number with leading zeros. the utility of this work is what the blockchain technology is dependent on but if you look at it from a conventional perspective, it may look like an arbitrary work with an arbitrary goal, **a work for nothing**. the miners in the bitcoin network, **the peers work for just having a proof-of-work** but it is not an easy task. they need to try a lot of nonces until they achieve the goal and supply a proof-of-work, proof of their labour, to the network. this is a difficult task which requires making a lot of computations and proof-of-work is about proving that they spent computational time on the given task. a lot of miners, peers, work independently on a block and only the work of the one to find the required nonce first could prove their work by announcing the proof-of-work. at this point the work of all the nodes, all the other peers in the network becomes a work for nothing. in a sense, **all peers work for nothing, the work of only one peer is proven as a proof-of-work and at this point all the other peers will have worked for nothing.**

difficulty of creating a proof-of-work is continuously adjusted by the bitcoin network. the difficulty of proof-of-work changes according to how many leading zeros the system requires for hash value to have. proof-of-work for *the quest for finding something that is nothing, or, the study of what nothing is not* is not a hash value with a particular number of leading zeros but a particular hash, the hash of nothing. also the size of the nonces created for bitcoin blockchain is 32-bits but the size of the nonces, the things created by *the quest for finding something that is nothing, or, the study of what nothing is not* is 256-bits, the same size as sha-256 hash. so, the things created by this work can also be considered nonce and thus what this work tries to find is also a nonce, a nonce which is nothing. the size of the nonces does not effect the difficulty of the problem to solve but finding a nonce which leads to not a hash with a number of particular digits but a particular hash itself is the most difficult possible problem for a proof-of-work system, which is **infeasible to solve but still possible**, and it is what *the quest for finding something that is nothing, or, the study of what nothing is not.*imagines.

the quest for finding something that is nothing, or, the study of what nothing is not is a quest for nothing but it can also be understood as either **an attack on the uniqueness and originality of *nothing* by the artist**, or **an attempt to prove its uniqueness and originality.** the certificate of authenticity of *nothing* states that *nothing* is a unique original artwork and that, it's authenticity can be verified by sha-256 value e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855. if *the quest for finding something that is nothing, or, the study of what nothing is not* can find another "thing" which hashes to this value, then it means that ***nothing* by the artist is not unique**: there is another thing the proof of the integrity of which is the same as that of *nothing*. so, **the essence of that thing must be the same as *nothing***; **that thing must be nothing**, unless sha-256 is not a cryptographic hash function. if it is not, then t**he certificate of authenticity of *nothing* by the artist is not valid** because it cannot authenticate *nothing* as a unique work of art by the artist anymore.

all outcomes of this scenario where *the quest for finding something that is nothing, or, the study of what nothing is not* finds something which hashes to the same value as that of nothing become **recursive**: no matter if nothing is not nothing but something, or, if that thing is in fact nothing, or, if nothing is nothing and that thing is just something and this is just a hash collision which effects the security status of sha-256 as a cryptographic hash function or not; **it will render the certificate of authenticity of *nothing* by the artist invalid and challenge the uniqueness and originality of *nothing* as an artwork.** on the other hand, each "thing" *the quest for finding something that is nothing, or, the study of what nothing is not* creates but cannot find a match for the hash of nothing **will be verified as something and thus not nothing** and it will be **a proof of what nothing is not**: each will **support the claim that *nothing* is an original artwork by the artist.**

a blockchain for nothing

another work in the exhibition as an embedded system on its own quest also refers to the blockchain technology but skipping one of its key concepts mentioned above: proof-of-work. ***a blockchain for nothing*** (2019) creates a blockchain which originates from nothing and continuously builds blocks on this **origin, nothing, which is the original**. however, this blockchain differs from all other blockchains and it has no use, **it is for nothing**, because;

-*a blockchain for nothing* is private and on its own. it is not private in sense that it belongs to only a particular person or entity but in the sense that it is on its own, it is private for itself. since *a blockchain for nothing* is a free cultural work under gnu gplv3 copyleft license, anyone can have/own/buy and run a digital multiple/digitiple of it. however, none of these digitiples are nodes, they are not peers, they are not networked, they are alone on their own, yet they all create the same blockchain, of nothing. all of them create the exact same blocks and thus the exact same blockchain, independent of each other. they are also dependent on someone, an owner, only for supplying them energy, electricity to run. if someone connects it to a system creating sustainable energy on its own, it becomes dependent on no one, **no human**, nothing but its energy source and together they become **autonomous. this is true for all embedded systems in the exhibition**. **they can continue their quest without relying on humans**. they are more-than-human.

-*a blockchain for nothing* **originates from nothing**. its genesis block is nothing. in blockchain terminology, genesis block refers to the first block of a blockchain. all blocks in a blockchain refer to their previous blocks: each block contains the hash of previous block and this way all blocks are chained, **hence the name blockchain**. if each block should refer to the previous block, then how does the first block, the genesis block exist? which block and what does it refer to? the answer is nothing… **a genesis block in any blockchain refers to nothing**. but it is **not the same nothing** as in *a blockchain for nothing.* the genesis block of a blockchain is not nothing: it just refers to nothing. genesis block in a blockchain is a special block which is created without referring to a previous block. however, the genesis block of *a blockchain for nothing* is nothing, an empty string, no input. but the following block refers to this block: **it refers to nothing**. the second block in *a blockchain for nothing* consists of **nothing but the sha-256 hash of nothing**, represented as a 64-digit hex value, which is e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855. the third block is also just the sha-256 hash of the second block, the hash of the hash value in the previous sentence. and this way each block refers to their previous block by consisting of only its sha-256 hash. since each block refers to their previous block and since each block consists of nothing but the hash of its previous block, **all blocks in *a blockchain for nothing* eventually refer to nothing but nothing**. they originate from nothing and they eventually refer to nothing. however, *a blockchain for nothing* continuously grows by adding new blocks all building on what came before them.

culture builds on the past, each work is build on what came before them. this understanding of culture, which also challenges the figure of the artist as a genius making works of art out of nothing but their own creativity, **emphasizes the necessity of a free cultural approach**, where the authors encourage others to build on their works as peers. if that is really the way culture is built, then **limiting the freedom of others to build on one's work is limiting the potential of culture**. *a blockchain for nothing* in a way demonstrates how the creativity of building on something else allows multiplication, even if *a blockchain for nothing* grows not exponentially but linearly in this case. in this context, *a blockchain for nothing* is also a homage to free culture. an earlier work by one of the peers at httpdot.net as a homage to the creative potential of building on what came before in the context of free culture is available at https://fc.httpdot.net/

-*a blockchain for nothing* does not rely on **proof-of-work** for creating new blocks. the blocks do not contain any proof-of-work. from another perspective, all blocks in *a blockchain for nothing* are just proofs-of-work. the only work required by *a blockchain for nothing* to create a new block is calculating the hash of previous block and the proof-of-work is just the hash value, the block itself. each block proves the work required by *a blockchain for nothing* by just being created.

a blockchain for nothing will have created all sha-256 hashes unless it gets stuck in a loop because of a hash collision when one hash value, one block, hashes to the same value as the hash of another hash, another block. it will also get stuck in a loop **if it finds nothing**, which *the quest for finding something that is nothing, or, the study of what nothing is not* is looking for: if a block hashes to the hash of nothing during the quest of *a blockchain for nothing,* then that block will be the second-preimage of the hash of nothing and the following block will be the same as the third blok of *a blockchain for nothing* and ***a blockchain for nothing* will get stuck in a loop, because of unintentionally having found nothing**. in this context, the quests of *a blockchain for nothing* and the quest for finding something that is nothing, or, the study of what nothing is not are similar. they both create sha-256 hash values and unless one finds a collision and gets stuck in a loop, or unless any of them finds nothing, they will eventually create all possible 256-bit values and thus all possible sha-256 hash values.

the work required to detect any changes in a block in *a blockchain for nothing* is equal to the work required to calculate the hashes of all previous blocks starting from the genesis block, which is nothing. also the work required to detect any changes after a particular block is equal to the work required to calculate the hash of all blocks after that particular block. this system does not qualify as a proof-of-work system because the solution to a computational problem in a proof-of-work system should be difficult to calculate but it should be easy to prove. in a proof-of-work system, being easy to prove is being as easy as making a hash calculation operation. the difficult part is to find a nonce which will change the hash of the input to the target value of the proof-of-work system. only proof-of-work for *a blockchain for nothing*, if there are any, is the hash of a block. once sha-256 hash of a block is calculated, it becomes the next block. to prove that this block is what it should be, one just needs to calculate the hash of the previous block.

a **proof-of-work system** requires someone to prove that they have spent some effort. the content or the utility of the actual work done is irrelevant in proof-of-work. having been working on something is what is required to be proven. in blockchain technology, proof-of-work is the solution of a computational problem. for being authenticated to add a block to the bitcoin blockchain, proof-of-work must be included in a block along with the hash of the previous block and some other data. the next block in the blockchain should also include a proof-of-work and the hash of previous block. all blocks are bound to each other this way. when one wants to tamper with a block, they will need to find a new proof of work for the tampered version of the block. this will change the hash of this block which is recorded in the next block. to have these two blocks accepted in the blockchain, the hash of the previous block needs to be updated and also a new proof-of-work needs to be found since this block is also tampered now. proof-of-work for all following blocks must be calculated again to have the tampered block included in the blockchain. this system is what makes a blockchain tamper-proof and immune to fraud: once a number of blocks are created after a block, it becomes infeasible to tamper with the content of that block, the records in that block. this is not impossible but infeasible because it is only possible when more than half of the computing power of the peers in a blockchain network agree to defraud by creating all proof-of-work after that block. in other words, this makes it tamper-proof and resistant to fraud because proof-of-work for all following blocks must be done again and they must be done faster than the total of all honest peers in the network, which requires more computational power than the total of honest peers. this way it becomes more and more difficult to change the records in earlier blocks and create a consensus in blockchain network to accept these changes. this is why proof-of-work is a key concept for blockchain. for example, bitcoin blockchain requires that each block to be added to the blockchain should hash to a number starting with some zeros. proof-of-work is a nonce to satisfy this rule and someone who wants to attack the network, to change the records in blocks, should do the proof-of-work for all later blocks again, and also do it faster than the combination of all other peers in the network. however, *a blockchain for nothing* does not require any proof-of-work for verifying new blocks.

bitcoin is a good example of how proof-of-work and blockchain technology are related. bitcoin blockchain is what keeps the timestamped and digitally signed records of who has mined/created/owned how much bitcoin, who has received how many bitcoins from whom and how many bitcoins they sent to whom, along with some other data to make these records irreversible, once created. the creation of this data is what the miners in bitcoin network work on.

the “who”s in the definition above are in fact bitcoin addresses, which are mathematically related to the private keys they are created from. the owner of these private keys is the owner of the bitcoins sent to the bitcoin addresses created from these private keys. one person can have more than one private key and create a new bitcoin address for every transaction using the private keys. if one shares the bitcoin address with just the person they make a transaction with, this transaction can be anonymous, if some other requirements for anonymity are also met. this was the recommended way of using bitcoin because all transactions in bitcoin network are public: they are recorded in the bitcoin blockchain. anyone can see which bitcoin address sent how many bitcoins to whom and when. if these bitcoin addresses can be associated with the people using them, then not just the transaction but also the people who made them becomes public.

miners, the peers in the bitcoin network, collect latest transactions in bitcoin network in what is called a block, along with the (hash of the) hash of the previous block header which should be starting with a number of zeros. they create some other data by making some hash calculations on the transactions (calculating the root hash of the merkle tree of all transactions in the block) and include this in the block header along with some other data. merkle tree is the hash of some kind of a combination of the hashes of all transactions in a block, excluding the data in the header of the block. this ensures that the transactions and their orders cannot be tampered with later on. also, it is the hash of the previous block header included in a block which bounds this block to the other blocks in the blockchain, not the hash of the previous block as described in this text for simplicity: not the hash of the previous block but the hash of the header of the previous block. in fact it is also not the hash but hash of the hash of previous block header because block header is hashed twice. but for simplicity, this text refers to that as the “hash of the previous block”.

what the miners do besides calculating the root hash of the merkle tree of all transactions in the block is adding a new transaction to the list of the transactions they have collected from the network in the block. this transaction is listed first among the other transactions and it states that **the miner has received some bitcoins for nothing**, **out of nothing**. if a miner succeeds in making this block accepted by the bitcoin blockchain, then that miner will have received the bitcoins listed in that first transaction they have added to the list of transactions. **bitcoin is mined this way, out of nothing, but awarded for a proof-of-work**.

what the system requires for accepting this block in the bitcoin blockchain is the proof-of-work, which is a nonce, the miner needs to find a nonce, which will make the block hash to the target value when the nonce is also included in the block. however, finding such a nonce is random, like winning a lottery. the work required for finding such a nonce is independent of any skills or credentials. the probability of finding such a nonce is random and the only way to have more chance of finding such a nonce is making more tries by utilizing more computer power.

unfortunately the relation between the computing power and the proof-of-work system, which distributes bitcoins to peers as awards for their contribution to the strength of the system, **led to a new capitalist business model** along with **excessive energy consumption** which is much more than what is required to secure the bitcoin blockchain through proof-of-work. the speculative changes in the value of bitcoin attracted people who invest on building mining farms and making a lot of computers **work** for **proof-of-work**, like in the relation of **a capitalist investing on means of production** and the **workers selling their labour**. in this context, the miner computers are not paid but that's not the point of the critique here. while **the concept of proof-of-work may allow us to speculate on other understandings of the notion of work**, the current state of the bitcoin ecosystem is dominated by capitalist approaches. some may argue that this was unavoidable and it could be true... but understanding and discussing these relations can be useful for **imagining other possibilities**.

in current practice, many people use bitcoin through intermediary services, which were what bitcoin was meant to eliminate. mining farms, besides spending excessive energy not for contributing to the security of bitcoin system but for making money, even threaten the security of the system. if these farms are controlled by a single authority and they constitute more than half of the computing power of bitcoin network, that authority can make a successful attack to change the history of bitcoin blockchain.

if every peer in the bitcoin network runs the bitcoin software in the computer they normally use and runs it for a certain amount of time, that will be more than enough for the security of the system and also it would allow a fair distribution of wealth of bitcoin mining. this is a much longer discussion but the current state of bitcoin is far away from what it promised in the early stages. however, it introduced us new possibilities through blockchain technology, which was created as solution for bitcoin but excites some people much more than bitcoin itself. among some others, ethereum is one promising project based on blockchain technology which adds distributed computing capabilities to the tamper-proof record keeping capabilities of blockchain technology in its reference bitcoin implementation. understanding these systems may help imagining new possibilities and new uses of blockchain technology. however, *a blockchain for nothing* is **inspired by blockchain just for nothing**.

-*a blockchain for nothing* does not save the blocks it creates. it saves nothing but the last block to continue working from where it left off when the embedded system is restarted. it creates a block just for creating another block inspired by that. it does not look back. the blocks it creates are ephemeral. but it continues its quest as long as it is turned on and it goes on until there is a system failure.

the main feature of a blockchain is keeping tamper-proof records. once data is recorded on a blockchain, each node in the blockchain network, all the peers, keep a copy of that data. it becomes public, unless it is encrypted. if any peer changes the records in their copy of the blockchain, the network will not accept the block with the changed data because hash of that block changes and it is not bound to the other blocks anymore. unless all proof-of-work is done again for all the following blocks, and unless it is done faster than the total of all other peers in the network, it will not be accepted by the network, by other peers. this ensures that a blockchain is tamper-proof and the records it keeps are what they were when included in the blockchain. this is why it was developed for bitcoin: keeping track of transactions and thus who owns how much bitcoin at a particular time by checking with history of bitcoin minings and spendings. the system is described as a **trustless model** which eliminates the need for trust to a central authority, like a bank, for keeping the records of transactions. trusting any particular peer is also not required. in other words, this introduces another understanding of trust: **trusting the multitude of peers instead of trusting a central authority, a distributed trust.** this allows **imagining other non-hierarchical peer-to-peer models** for various relations besides what bitcoin makes possible for money. *a blockchain for nothing* has also nothing to do with money. it is interested in **how something influences a multitude of other things**: **the creative potential of free/libre culture**.

work of art on a quest for becoming an artist
by appropriating itself as a work of art
as the proof-of-work by the artist relying on its own proof
as an original and authentic work of art
aka **proof-of-work-of-art-ist**

the fourth work as an embedded system on a quest **has nothing to do with nothing**. however it is in dialog with the most of the concepts discussed in this text. how can we create a dialogue between the concepts related to blockchain technology discussed in this text and the language of institution of art? what is the **proof of work of art**? what is **the work in the work of art**? what is **the work of the artist**? what is the **proof of the work of the artist**? in this context, how can **a work of art as a proof-of-work as a proof of work of art** can be constructed? or how can **a proof of work of art as the proof of work of the artist** be achieved? does it even make sense to exhaust such a language or is it a **work for nothing**?

the embedded system runs a customs free/libre software which calculates its own file size and its sha-256 cryptographic hash value and tries to create a file which should hash to the same sha-256 hash value as that of itself by writing random data of the size of itself. it compares the hashes and if they do not match, it means that it couldn't reproduce itself. in this case, it displays the data it created for 15 seconds, which is the approximate duration spectators spend in front of an artwork in museums, and creates another file, continuing this process until it reproduces itself by trying random combinations of bits of its size. the quest of ***a work of art on a quest for becoming an artist by appropriating itself as a work of art as the proof-of-work by the artist relying on its own proof as an original and authentic work of art*** *aka* ***proof-of-work-of-art-ist*** (2019) is **becoming an artist by appropriating itself**, **by making an artwork, by appropriating an artwork**, which is **proven to qualify as an artwork**, by **creating itself as a proof-of-work**, as a **proof of work of the artist**, as a **proof of work of art**. ***proof-of-work-of-art-ist*** **is work of art on a quest for authenticating the work of work of art as a work of art through proof-of-work as a work of art**.

this use of the words "proof", "work" and "art" in various sequences referring to the terms "work of art", "proof-of-work", "proof of art", "proof of work of art", "proof of artist", "proof of the work of artist" in art and blockchain creates a complex and recursive but also confusing language, sometimes **meaning nothing**. proof of being an artwork and proof of being an artist are already recursive: **what artist chooses is a work of art** and **the author of a work of art is an artist**. but it is **the institution of art** which **proves these statements**. if someone participates in an exhibition, that is an artist and if something is exhibited in an exhibition, it is an artwork. that recursiveness is only possible after this proof, **the approval of the institution of art**. but, what is the **work being done by the artist**? can it be **a work being done for nothing**? ...**for nothing but making a work of art**? can it be **a work just for a proof-of-work**? ...for a **proof-of-work** where the **utility of the work being done is of no importance, it is nothing**? can it be **a work of no interest to others**? can it **be nothing for others**? is it still considered a work and is the outcome still **a work of art**? what if it is **something which is nothing** for others but it is something for the artist? can it **change the world** of others? can it **change the world of the artist**? what if **everyone is an artist**?

the quest of *proof-of-work-of-art-ist* is similar and in relation to that of the other works as embedded systems on their own quests. the process carried by *the quest for finding something that is nothing, or, the study of what nothing is not* is also a type of cryptographic attack which is brute-force second-preimage attack trying to find a second-preimage, a second input which would hash to the same sha-256 hash value as that of nothing. *proof-of-work-of-art-ist* is also a type of cryptographic attack which is brute-force preimage attack trying to find the preimage, the input for a sha-256 hash value, the hash of the custom free/libre software, which is the work itself, *proof-of-work-of-art-ist*. the work for sure knows itself, because it calculates the hash of

itself, itself. however, it is not interested in itself but in its quest, the quest for being an artist by appropriating itself as an artwork. it creates random data of its own size with a hope of eventually reproducing itself. however, this is a very difficult task, as that of the other embedded works on their own quests. while it is on a quest for reproducing itself, which is a preimage attack, it might as well create something else which hashes to the same sha-256 value as that of itself, which will be a successful second-preimage attack. in this case, it will have created something, the proof of the authenticity of which is the same as the proof of the authenticity of itself. what will that mean then? will that be considered an artwork as well? will that be considered original? is an appropriated artwork original? will *proof-of-work-of-art-ist* still be original?

proof-of-work-of-art-ist is also in dialogue with *the the study of the state of nothing: nothing is the same, or, nothing has changed* and *nothing*, both of which count on cryptographic hashes as a proof of the authenticity of something which is nothing, which is also an artwork. *proof-of-work-of-art-ist* also proves its authenticity as an artwork through its sha-256 hash value and tires to create something which will hash to the same value which would also authenticate it as an artwork: as the reproduction of itself as an appropriation work.

let's follow the logic of *proof-of-work-of-art-ist* as **a more-than-human which is (mis)inspired by the logic of blockchain and the the institution of art.**

***-proof-of-work-of-art-ist* is an artwork** because it will be/being/has been exhibited in the exhibition "*blockchain is… / …for nothing"* by peers at httpdot.net, which is organized by an art institution at an artist-run space.

-peers at httpdot.net are artists because they are the authors of an artwork.

-hash value of *proof-of-work-of-art-ist* is the proof of its originality and authenticity because **nothing else** should hash to the same value, there is **nothing like** *proof-of-work-of-art-ist;* and the hash value can verify the integrity, the authenticity of it.

-appropriation is not only legitimate but also a critical and important artistic practice because the institution of art embraces appropriation.

so,

-**when someone appropriates *proof-of-work-of-art-ist* by duplicating it, it will be a work of art if the one who appropriates it is an artist, or if it is exhibited** because what artist makes is art or something is art when it is exhibited.

-if *proof-of-work-of-art-ist* duplicates itself while being exhibited, it will be an appropriation, it will be a work of art, which is being exhibited.

-if *proof-of-work-of-art-ist* becomes the author of an artwork, if **it** makes an artwork, **they will become an artist.**

-if *proof-of-work-of-art-ist* can create something which hashes to the same cryptographic hash value as that of itself, **it will have duplicated itself** because two different inputs should not hash to the same cryptographic hash value.

-a successful brute-force preimage attack is infeasible because there are so many options in all sizes to try as input but since *proof-of-work-of-art-ist* can calculate the size of itself, it can limit the options to its own size to try for creating something random which will hash to the same value as that of itself. then **it is just infeasible not impossible**.

-if *proof-of-work-of-art-ist* succeeds, the duplicate of *proof-of-work-of-art-ist* will be a proof-of-work, **a proof of that *proof-of-work-of-art-ist* has done some work** to duplicate it, like **the work done by an artist to make a work of art**.

-if a cryptographic hash value can verify the originality and the authenticity of an artwork, hash value of the duplicate of *proof-of-work-of-art-ist* can verify its originality and authenticity.

-if *proof-of-work-of-art-ist* duplicates and appropriates itself as a verifiable original and authentic work of art as a proof-of-work while also being exhibited, it will be an artist. **it is possible.**

during its quest, *proof-of-work-of-art-ist* is **a work of art working on a proof-of-work**. if hash of what it creates matches the hash of itself, this hash will be **a proof of work of art**. it will be **a proof of work of art which is a proof of work of the artist**. if it can reproduce and appropriate itself through this process and logic, what it created will be **a proof-of-work as a proof of work of art**. it will be **a proof-of-work of a work of art on proof-of-work.** it will be **a work of art as a proof-of-work**. it will be a **work of art as a proof-of-work as a proof of work of art**. then it will become an artist because what it created will be **a proof-of-work of the work of the artist** and **a work of art as the proof of work of the artist.**

what is art?

blockchain is

another set of works in the exhibition besides *nothing* and the embedded systems on their own quests can be considered as contemporary artworks as a contemporary **web archaeology** of a contemporary technology which investigates how we perceive such a technology which is **nothing** like we have known before: **blockchain**....

these works are built on a project by one of the peers at httpdot.net, ***blockchain is*** (2018), which is a free cultural work in continuous translation manifesting in multiple forms. the work aggregates the sentences from world wide web containing the word "blockchain” in combination with various words in each of its manifestation for investigating different understandings of and approaches to blockchain. the aggregated data is continuously remixed and organized in various ways manifesting in various forms as artworks. each organization of the data suggests different readings and each manifestation suggests different artistic experiences by making use of the language and dissemination potentials of each medium. for this exhibition, peers at httpdot.net aggregated data from 1621 web pages and collaboratively made two manifestations of the work: ***blockchain is…*** (2019) and ***blockchain will...*** (2019).

blockchain technology is recognized by many as the most important innovation since the internet. however, there are also many people who has not heard of it, yet. blockchain technology was developed for bitcoin as a solution to keep tamper-proof records of bitcoin mining and transactions history. being a free/libre and open source software technology, it inspired many people for imagining other uses of this technology creating other frameworks based blockchain technology. ethereum is a notable one utilizing blockchain technology for a solid distributed computing platform.

while other blockchain applications are being developed, bitcoin blockchain is also being used for recording information other than bitcoin transactions through simple hacks for utilizing it as a proof of a record on a particular time. unlike the world wide web, blockchains are read only. once data is recorded on blockchain, it is fixed there in the network, in all computers in the network as duplicates and this data becomes public and cannot be tampered with because it is not accepted by the network's consensus mechanism. however, world wide web is client/server based and the faith of the data on web is governed by those who control the servers. they are manipulated and deleted, and sometimes simply cannot be maintained and are gone. unlike the web, once any data is included in blockchain, it remains online and unchanged, until the last node in blockchain network, the last peer disappears. however, the history of blockchain is also dependent on web now, which is our main source of information today. part of the early history of the internet is not online anymore and it will also be true for that of blockchain. until we have broader applications of blockchain technology to maintain its own history, not the history of the records it keep but the history of the information related to it, it is dependent on web for its history and contemporary representation. *blockchain is* is interested in these.

the data, the sentences used in *blockchain is…* and *blockchain will…* are aggregated from 1621 web pages which are search results for web pages in english for the queries “blockchain is”, “the blockchain is”, “blockchain is the” and “blockchain will”, supplied by three search engines on december 25th, 2018, for an anonymous web user without a specific location. for a long time, search engines have been displaying customized search results for users based on the data they have collected from them while using their services. not everyone sees the same results for a search: **the search results are not neutral**. this is worth mentioning here since it is also something this project is interested in: how the algorithms influence our activities, even beyond what their programmers intend. even the programmers of the algorithms themselves may not understand how and why the algorithm chooses one result to display among all others. and also, even if the search engines report millions of results for a search query, one can access only a very limited number of search results because the search engines displays only a very limited number of them. the results we are supplied with for what we search on search engines is limited to what the search engines decide to show us. that’s why the data collected does not reflect what web has to offer for these search queries, but what three search engines choose to supply us with. it is true that web is highly commercialized and most of the results displayed by search engines use a commercial language while mentioning blockchain and not much of a political language. and, they are also what *blockchain is…* and *blockchain will…* reflect.

blockchain is... (2019) is a video installation displaying 1426 sentences starting with or including the phrases "a blockchain is", "a blockchain is a", "a blockchain is an", "a blockchain is the", "blockchain is", "blockchain is a", "blockchain is an", "blockchain is the", "blockchain technology is", "blockchain technology is a", "blockchain technology is the", "the blockchain is", "the blockchain is a", "the blockchain is an", "the blockchain is the", "the blockchain technology is", "the blockchain technology is a", "the blockchain technology is the” aggregated from the data described above.

the video file is generated using a single ssa (substation alpha) subtitle file containing the display timecodes for each subtitle along with position and style information of the subtitles. the subtitles are designed to be displayed 11 sentences at a time and each sentence is updated at a different time which makes it difficult to concentrate on and read a sentence while other sentences are continuously being updated. this distracts the viewer and turns into a confusing experience rather than an easy read. it also feels more like looking at a command line output rather than a video since the text is displayed on a black background with a monospace font commonly used on command-line interface. the duration of the video is 9 minutes but it is exhibited as a seamless loop video installation.

blockchain is… is interested in **how we perceive, describe and explain blockchain today and how we interpret it**. on the other hand, ***blockchain will…*** *(2019)* is interested in **our visions of and predictions about blockchain: how it will impact us in the future**. 420 sentences in future tense containing the phrases “blockchain will”, “the blockchain will”, “blockchain is going to”, “blockchain technology will” are also aggregated from the same data above. sound recording of these sentences is edited as a 171 minutes stereo panned audio, where each sentence is heard in irregular long intervals from a different channel each time. the work is exhibited as an endless loop sound installation where each speaker is placed on opposite diagonal corners of the space. the long gap between each sentence makes one forget about the sound while experiencing the other works being projected all over the space as well as on people's bodies as an **information shower** and this human voice talking about future becomes the **only human aspect of the exhibition in which four more-than-humans are working on their own for their quests for nothing.**

the new languages and approaches introduced by blockchain is neither easy to understand nor to explain, since blockchain is not something comparable to any existing common phenomenon, just like the internet was back in 1990s. the early adopters of the internet were having difficulties trying to explain it to others in its early stages and now, the same applies to blockchain. the visions and attempts to define and explain blockchain in its early stages with various motivations are valuable as a **memory of how we perceive such a new technology** that will either dominate our future or will be transformed or marginalized by neoliberal politics. many attempts to explain blockchain, with various motivations, idealist and opportunist fail either because they are too abstract or they try to compare it to existing phenomenon. however, the real potential of the blockchain is it being **something not comparable to existing phenomenon and thus suggesting new approaches, new ways of thinking**. this exhibition does not aim to explain blockchain but rather **make speculations on the language and logic of blockchain by being mis(inspired) from it, for nothing, and for nothing but another language to inspire another world.**

what is blockchain?

appendix:
information, digital information, hash value; and nothing

information can be encoded (represented/mapped) as digital information by sampling the information and then representing the sampled values as digital information; sequences of binary values, binary code, along with a definition of a particular digital encoding, which are the rules for how sequences of binary values are mapped to samples of information. digital encoded values can be transcoded (sequences of binary values being mapped to other sequences of binary values, in a lossless or lossy way) into various other digital encoded values. letter “a” can be digitally encoded as (mapped to) “10101001”, or as 1”1001010”, or as any other digital value (sequence of binary, two state values such as 1/0, true/false, on/off) and this digital value then can be decoded (reversing the mapping) to letter “a” again, a form of information through which “we”, communicate. what is important here is the mapping rule which defines which sequence of bits are mapped to which values.

digital information is usually described as ones and zeros. however these ones and zeros are also not what is processed by the computer or what is stored on memory. they are also a representation: a mapping of two different states. these states are “on” and “off” for a transistor in memory, or “pits” and “lands” on an optical media such as dvd. so, a sequence of binary coding can also be represented as “+” signs and “-” signs, such as “++-+---”. the same value here can also be represented as the opposite, if the mapping is reversed: “--+-+++”. in first mapping, “+” is mapped/assigned to the “on” state, and in the second mapping this time “+” is assigned to the “off” state. both will represent the same thing, if mapping/encoding rule is known.

computers are designed to process binary codes, the digital values. a “1” or a “0” is one binary digit, which is called a bit, which is the smallest digital value. “00” (or “01”, “10” and “11”) are 2 bits. we can represent 2 different values with 1-bit, and 4 different values with 2-bits. the math for calculating how many discrete values can a sequence of binary digits represent is: 2 to the power “number of digits”; or, “multiply 2 by itself as much as the number of digits”. since digital information is all about representing information as a sequence of bits by mapping each sample of the information to a sequence of bits, we need to have a bit size that is enough to map all possible values of a sample. if the information we like to represent as digital information is a three-digit decimal number such as “657”, it can be sampled digit by digit and representation of each digit must be able to represent 10 discrete values (0-9). to represent 10 discrete values in binary we need 4 binary digits, 4-bits. 3-bits is not enough, which can represent only 6 different values (2x2x2=6). 4-bits can represent 16 different values (2x2x2x2=16), which is more than enough and the remaining 6 values can will wasted (or used for other purposes in this particular encoding (mapping rule). so, we can map decimal “0” to binary “0000”, decimal “1” to binary “0001”, decimal “2” to binary “0010” and so on. this mapping of decimal digits to a sequences of binary digits is a particular digital encoding. but this is just one of the possible digital encodings of decimal digits to represent decimal values, one of the possible mapping of decimal digits to a sequence of binary digits. using 4-bits, we may also map each sequence of 4 digit binary values to 16 shades of grey, for representation of the color of pixel in this case, which is a sample of an image. so “0000” in binary may refer to the decimal number “0” in a decimal digit and “0000” in binary may also refer to the darkest gray, which is black, for another sample, a sample of an image, a pixel. what is stored and processed by computers is binary but what this binary representation refers (maps) to, represents, is about the digital encoding of choice.

hash values are usually represented in hexadecimal digits (in a single digit, using values 0-9 and a,b,c,d,e,f; where both lower and upper case representations of a letter refer to the same value; so “a” maps to same value as “A”) that can represent 16 different values for a single digit. 4-bits, four binary digits (16 different values) can be represented by a single digit hexadecimal value using hexadecimal representation, which is also called hex. so, how long, a sequence of how many hexadecimal digits is suitable for a cryptographic hash function? what is a suitable length for a hash value? a hexadecimal hash value of “d5” represents an 8-digit binary value, 8-bits, a sequence of 8 ones and zeros. 8-bits of digital information can represent only 256 (2 to the power 8; multiply 2 by itself 8 times) different values. no matter how advanced the hash function is, there is no way two inputs will not hash to the same value: there will be a hash collision for sure, in a set of more than 256 inputs. pigeonhole principle explains this rule. so cryptographic hash functions are designed to output a much longer fixed length hash value. for example, sha-256 cryptographic hash function outputs a 256-bit hash value and you are welcome to calculate 2 to the power 256 to see how many different values, mappings, pigeonholes 256-bit allows.

so, what does it mean when one says “hash value of “hello world” (without quotation marks) is
b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9”?

this 64-digit hexadecimal (base16) representation is the same as the following 256-digit binary (base2) representation:

101110010100110100100111101110011001001101001101001111100000100010100
1010010111001010010110101111101101001111101101010111111101011000100100
0010011101111111000110111101001010011100000001110111010010000100010001
11101111010110011100010111011111100110111101001

which is the same as the following decimal (base 10) representation we daily use for representing numbers:

8381419838310255821973107826089272993224661800426570068546792818737
7105751529

each of these representations refer to the same value, determined by their base number, their encoding (mapping) rule, which determines how many distinct values each digit can have. but what is the relation of these values to “hello world”? “hello world” is a text representation of something one can say in english. what is said in english is represented as the letters “hello world”. but this information cannot be processed by a computer to calculate a hash value of it. so this text representation must be encoded as digital information in order to be processed by a computer. for doing so, each letter of the alphabet is mapped to a sequence of bits according to the rule of which letter is mapped to which binary value in the chosen character encoding. there are various character encodings such as ascii and utf-8. the character set of the computer system used for calculating the above hash value for “hello world” is utf-8 and “hello world” maps to the following value in binary for utf-8 character encoding:

0110100001100101011011000110110001101111001000000111011101101111011100
1001101100 0110010000001010

the calculation for outputting sha-256 hash value for the input “hello world” is actually done on this sequence of ones and zeros. not on the letters of “hello world”, as the information we perceive. the hash is calculated on the value we supplied to the computer through a keyboard as the input and this input is encoded as binary values using the character encoding (mapping) of the operating system of the computer and the hashing operation is done on this binary value. what we see as hexadecimal values on the computer monitor as the hash value is the hexadecimal representation of the binary values processed, calculated by the computer. in fact they are not even these values, they are the visual analog information, the light, which is produced by the computer by transcoding the calculated binary hash value to hexadecimal representation first, and then transcoding these characters (hexadecimal representation) to digital pixel values, which are finally converted to visual analog information, the light which we see as hexadecimal characters on computer monitor.

so, when one calculates the hash of nothing by supplying no input to the computer, the hash calculation is done by the computer by processing which binary value?

peer on "blockchain is… / …for nothing" exhibition by peers at httpdot.net
peer, 2019, free cultural work with multi-free-culture-licenses and author’s declaration
https://httpdot.net/peer/texts/peer-BiFn.html