RAID

by Sam Porter

Foreword

I have decrypted Finney' will, deciphered the very essence of it and translated it into a completely different kind of software. I dedicate all the time I have left to the development of this software. It allows to transform money into the purest form of power. As it was said in the Bible:

> "In the beginning was The Word"

It allows to engineer society. Name and the symbol in the contract are not constants. First name, "RAID" is a call to action to prevent the establishment of upcoming centralized multi-millennial tyranny and decrease chances of conventional World War 3 becoming a reality. Every dying programmer is a potential existential threat for tyrants. We must act fast, before surveillance reaches unimaginable levels.

Only a madman could even attempt to build something like this, somebody who does not value his own life or/and somebody who is very-very naive. My English could be bad, since I am Russian. Take this paper with a grain of salt, because I am probably insane. Also, my education could be lacking on certain matters, and it could all be just conspiracy theories. And, after all, I just wanted to shitpost. Forever.

Page of contents

Part 1. Philosophy

Part 2. Design overview

Part 1. Philosophy

Innovation pace

Modern politicians are still having trouble catching up with the times. They still struggle to understand the fundamental significance of the internet, they struggle to understand how to regulate it and what are the potential benefits, problems, threats. Today, as blockchain became a thing, they are even more clueless, you could even say they are funny, naive.

The thing is, they are as naive in the face of innovation as we are. All their experience means absolutely nothing when an innovative technology turns upside down everything what they knew about. For presumably good reason, they see innovation as a potential existential threat, so what they do is stall the innovation pace at all costs, specifically all the innovation which is out of their control. They impose sanctions on each other, slowing down economies development, even destroying economies, sometimes more than just economies, the very essence of nations. They sabotage each other all the time. Piece is a lie, cake is a lie, they all lie. International Affairs is a doggie dog world like business but without any sense of integrity at all. It’s all rotten with hypocrisy. Trustless to begin with, international affairs have to be settled on a decentralized blockchain.

Humanity could already land on Mars, many diseases could be defeated, VR technology could be much more advanced, food could be much cheaper for everyone, overall quality of life and longevity could be much higher. There are so many underdeveloped technologies already present waiting for investments, but the thing is, the very most of these are concentrated in US, everything is very expensive to develop. The world scientific progress while advancing everyday is actually close to stagnation in comparison of how fast it could be.

Everything is inefficient. The direction these medieval savages are taking us is the dystopian surveillance nightmare with ever increasing taxes and government spending, even more bloated governments, more departments to control everything, every step, breath, thought. They are taking us into the world so full of lies, with so much lies on top of lies, that it will eventually be completely impossible to hide the truth without tyrannical measures, which they won’t hesitate to use, if things start to go out of their control. This is the price they want us to pay to prevent existential threats. We are all Sam, just delivery guys. A mere joy division of our generation. Trapped in the Matrix of our own imagination with our only friend being a literal Frankenstein monster, who might not even exist. We are holding this weight. We are holding this responsibility. The world is one step away from Greatness, from it’s True Potential. We just need to accept our responsibility and take necessary steps to deliver efficiency to the world.

They will introduce more and more inefficiency only to delay the inevitable progress, to maybe save humanity from a potential calamity, but maybe from something that takes away their power over us, as they believe their power is a sacred guardian of the very civilization, which is true, until it isn’t. In a way they are right, hierarchy must be present for order to exist. But, if the system becomes inefficient and fails to keep up with the times, especially when it so badly fails, a change must also happen.

Today, science is just smoke and mirrors, it's a joke. Statistical information contradicts statistical information. And why can't I access ResearchGate from a VPN to read these lies? Why do they need my real IP address? This medieval presentation is very dangerous for Homo Sapiens. We have World Wide Web, and the truth will always surface somewhere, trying to hide it is plain stupid.

Expressing your concern is like shouting at a wall – they will allow you to talk, but capture audience attention with something completely made up, in other words, they will censor you. Modern censorship gets more and more sophisticated. And you can’t even vote with your feet against this tyranny, because choices are either a bigger shithole, or a place completely alien to you.

Inevitably, they will start paying special attention to the lives of high IQ individuals. Since these people are more likely capable of innovation, and therefore of producing a new existential threat to this tyranny. The probability of a new innovative technology appearing increases exponentially with each passing year. The probability of a new existential threat appearing increases exponentially with each passing year. Humanity either evolves or goes extinct.

Politicians are frightened of what humans are capable of, they can't even imagine that evolution is possible. It's possible to make this world better, decrease crime rates, suicide rates, eliminate depression, but politicians can't see that. They are simply incapable, because they are not busy understanding anything further other than influence and power. They can control but they can't genuinely help. All their help to third-world countries or a certain social group is an expression of dominance, it's shallow simple politics, nothing good. Next year they can just destroy the very country they helped today, leaving millions in poverty, disease and crime. They do not really fix things.

They are frightened with the realization of that they can never predict what kind of software and at what point in time comes out of which third world shithole. It is impossible to control the whole world by only one jurisdiction, therefore it’s impossible to control all innovation. It’s time for those old farts to step aside, they are as naive in the face of innovation as we are, but we learn and adapt faster. These old farts can take positions of advisors, not the rulers.

The governments are running out of options facing increasing pace of innovation. For example, GitHub was acquired by Microsoft, and what they did is they banned some countries IPs. A useless measure, more of a statement, that the government is inclined to break software licenses openly even if everybody will know, basically break the law out in the open without any fear of being condemned. So, apparently, they are incapable of stopping it right now by democratic measures and only submitting to tyrannical ones is what's left for them. They are the existential threat.

Richest governments spend billions on medical research paying full salaries in their inefficient bloated jurisdiction. While they can outsource a half of the studies to countries in which scientists would be happy working on those studies for 2x less, 5x less, 10x less. We could have so many treatments and cures already, so many people would not die, live longer, would be happier, would be way less irritating. To be fair, they do outsource medical research sometimes. But only if it means establishing influence. Certain place. certain time, certain research. Far from efficient.

Or at least if these governments weren’t so against multi-polar capitalism, then we could also have way more advanced medicine. Sanctions delay development of certain economies, Russian economy in particular is being completely suffocated by sanctions as USSR was. Consequently sanctions delay the innovation and medical research. The world has so much more brain power than ever, and the most of this brain power is unable to innovate. If you live in first-world country – you need to somehow cut through all rigged competition and somehow pay taxes if you are a EU citizen. If you live in third-world country – you are probably just broke. What we do is we build biggest factories in Minecraft, then we die.

Historically most smart people were failing to achieve power, because they were always busy with concepts nobody understands. And as power today is more social than purely evolutionary concept, the most important thing a politician has to master is nothing but smooth talking, which could be an impossible challenge for some smart people. I believe RAID probably tackles this issue. RAID could potentially become the smartest political force in the world.

If we support increasing innovation pace, then we will take away the power from tyrants step-by-step, inevitably. We need a world in which anybody who is too busy lying to own people will be always too late. To make it happen we need multi-polar capitalism.

US creates circumstances to keep the wealthy around, to keep innovation and cult of personality concentrated in US. They keep billionaires hostages, so they won't leave. So the inequality in US will continue to become more and more pronounced until they will commit to Chinese tyrannical rule to keep the order. If two leading economies will be so tyrannical, what will happen is that other economies will submit to their ways and will inevitably follow their ways. And at that point the freedom of the individual will be lost potentially forever.

The aim is to put tyrants into a stalemate position, so that they will have to compromise. No, we are not seeking to overthrow the governments, we are a sanity check. We will be watching over them. Be aware of that the probability of success for this project approaches 0(zero). Even if it complies with all possible regulations, even if we lie about the purpose of the project, even if it will use a rainbow logo, and the thing is, it's basically futile to hide for what it is. It could be obvious to CIA of what it's potentially capable of in it's final form, even long before that, maybe even from the start, because it will be impossible to stop forks from doing something really stupid. I tried to word it differently, to present it as just a marketing tool, a revolution in marketing industry – didn't work for me, I have to be sincere. RAID could fail and with it become a funeral to democracy. Hopefully, it will be at least fun. Can probably be like Free Software movement, talking one thing and witnessing completely the opposite happening.

However, soulless greed of these control freaks faces an elaborate ideology. If they want to trap so much money on the blockchain – then maybe, just maybe RAID has a real chance. And if not – then it will attempt to leave the Legacy for generations to come.

Fundamental value of centralized governance

It approaches zero. History has proven it countless times. A monarch can lose his mind or just commit a terrible mistake, having only one man in power is unwise. That's why we have advisors, forums, parliaments, senates, unions. Decisions must not be unilateral.

This is why I very often use "we" instead of "I", but not to speak for everyone, it's because this whitepaper is v0.1, essentially a draft, and I believe that it requires way more brain power than I have. I am looking to start a discussion on details defining how the project should operate, so I refer to "we should/must" often as a means to speak to anybody who feels like RAID is something they want to participate in. This is also the reason why RAID starts with only minimum functionality, because I have realized that I am probably missing variables, probably will commit a mistake in the design and it’s best to bring it to discussion. This paper is essentially a governance proposal, you could call it like this, because I won’t be actually in charge of RAID, I do not own the contracts.

Politicians use the term “Power Vacuum” as a means of justification for starting wars and interfering international affairs. Power Vacuum is a legit concern in some situations, however the longer I look at their actions, the more it seems to me now that in their eyes Power Vacuum is the situation in which there is no dominating force in a given area, which is supposed to lead to cumbersome disagreements and civilized diplomacy. As it seems, the point is to avoid Power Vacuum at all costs, even if it means destroying a country’ economy and ruining people’ lives. Even if it means directly killing people. So what we have now is exactly centralized governance. Bloodthirsty, incapable of reason. It really is a doggie dog world, completely savage. It’s understandable that humans could not find better ways of creating order in times before the internet, but today as it’s all out in the open, absolutely inhuman hypocrisy of these ethical “saviors” makes me puke. They try to hide their ways now, and it’s still all obvious. Tyrants’ ratings are dropping, trust in the government decreases worldwide because of the internet. Because of that, they might use force easily, wipe any signs of democracy from the face of your nations. All states could become police states, and if a nation tries to stay democratic it will only result in more pressure on that country.

Empires of the past didn’t have the surveillance technology empires of today have. The upcoming suffocating tyranny of modern empires could be multi-millennial. And we can’t possibly know how bad things really are. It could be that we are already too late. If there is a strict regulation being introduced in one country, in the world of internet if we won’t express our disagreement, it eventually can spread to other countries, until the individual will become completely stripped of the freedom we knew about.

So many government officials are trying so hard to be useful, it's dangerous. Anybody young who was browsing the internet before the creation of Twitter and Instagram, when it was still 1% boring and 99% porn, is smarter than a typical government official. Because it's a different breed, with a different brain, capable of grasping concepts quicker. Yes, he does lack years of experience, but his experience is condensed, 1 year of his life is like 2 years of those who are currently in power. A 40 years old tech guy could be a real sage and it's simply normal. A 20 years old tech guy could already know so much more than today' politicians when they were in their forties. The superiority is clear. We have to act accordingly. They have proven themselves to be absolutely incapable of catching up with innovation(it's not just a decade of bitcoin, it's 2 decades of the internet being mainstream and them still not being able to understand it), so they will likely be too late to understand what RAID is about, however we have to act quickly anyway, regardless of our chances. Let it be an overkill, but ensure it will work.

Centralized governance is an existential threat in itself, the very thing it tries to prevent. It stalls the scientific progress which could in turn prevent so many more existential threats. So it’s the choice between certainty and uncertainty. We either have predictable piece full of rotten lies and inefficiency, or, we abandon medieval ways and embrace the progress, since there is no way to stop it anyway. Satoshi has shown to us, that one programmer can change the world. It’s real, observe: this is Digital Era.

Significance of the internet

With the internet, at least several values turned upside down on a fundamental level, most important one is how it redefines Power Vacuum. For politicians to actually start a war again like savages they are, they have to make worldwide national firewalls a thing. As long as we keep open borders for the internet, devastating conventional warfare or even World War 3 won't happen regardless of Power Vacuum. As long as the internet watches over politicians the only way is small conflicts and civilized diplomacy. The internet is the watch, clearly a virtuous invention. And we have to keep it open, or else we won't even know what is happening in the world. However, as conventional warfare loses it’s popularity as a means of settling international affairs, economic and ideological warfare becomes the driving force behind negotiation. Economic warfare specifically should not be taken lightly by a blockchain enthusiast. The more economic significance Bitcoin and Ethereum gain, the higher is the chance of PC’s of some countries’ residents being hacked. Whoever controls Windows OS can potentially define blockchain development. Keep in mind, that in situation considered critical, extreme tyrannical measures are possible: even confiscating cryptocurrency from centralized exchanges, not just users’ funds, but also the very holdings of the exchange.

Another one is free speech. Romans were using free speech to turn son against father and wife against husband, they ruined authorities, so nobody would follow anyone, in other words free speech was making revolt the least possibility, as nobody could unite. Free speech was a weapon of control for empires before the internet. With the internet however, when people were able to become influencers and exchange information between each other freely, it occurred to the politicians, that influencers create a following and unite people. While with the internet free speech is a force holding back conventional warfare and is clearly a virtue for the world to have now, free speech became the enemy of governments.

Now they regulate the internet. It’s impossible to get rid of free speech completely, but it can always be overhyped with some made up bullshit, and it can be restricted to unpopular resources. Lies now mounting on top lies, exponentially more to come, if it won’t be stopped. With so much lies, the fundamental value of truth also increases exponentially with time. Basic logic now is not just an important subject to master, basic logic now becomes the hidden knowledge, an autistic super-weapon.

Crime rates decrease as the internet comes to a third-world shithole. For the most desperate and cornered with life it enforces escapism, makes video games popular. The internet creates an existential crisis, it makes the most of the population humble, makes people think about their place in the world. The internet saves more lives than all world governments with their tyrannical laws combined.

When the internet was available only to middle class, to scientists and researchers, 95% of it was consisting out of porn, maybe more. We are definitely still human. The place now becomes even less and less informative as it becomes available to even broader audience. 99,99% of blogs today are simply unreadable providing absolutely no value to a sensible individual. The audience lacks education. It’s impossible to even speak to them. So the internet adapts, dumbs itself down. New generation now explores a much dumber internet we were exploring. It’s now all images and videos, and if it’s a blog, then it’s just dumb. An internet this retarded stalls the innovation. It’s an utter disaster of a civilization, the audience needs to learn how to think.

Logic against lies

Only because individuals now capable of exchanging information freely between each other all over the world and everybody are allowed to speak, the fundamental value of logic is at all time high. The first nation(even if it’s a shithole) to make logic a mandatory subject in school will gain immensely in the long run.

Stalin once noticed that his people are too dumb. He then asked: “how can they even go to war being this dumb?” What he did is he made logic a subject in schools. Naturally, he regretted it and banned it completely a few years later. This is how the generation of innovators in Soviet Union was born. The downside (for the empire) is that it was also the most rebellious generation and was one of the reasons of why USSR fell.

Modern humans' views are made of plasticine. They can't even elaborate on their stance about any particular subject, you can change their lives forever with an argument, or simply by rhetorics. This has to end. Homo Sapiens will be able to think efficiently for themselves and their beliefs will be made out of granite, so you could shape their minds with only valid arguments. Logic was always the hidden knowledge, as well as philosophy. Obviously, the benefits of introducing it to the masses were perceived as useless if these people will become capable of overthrowing the government. Now, however, as governments didn’t realize it yet as it seems, the people who are more likely to overthrow the government are those who have no ability of reasoning whatsoever. As cyberwarfare and destabilization with the help of world wide web became a thing this is the case.

Information and art were always weapons, it was known by the governments well before the internet. So destabilization through internet has gained incredible popularity in no time. It’s only a couple of decades of internet mass adoption, and the examples are already countless. The richest countries can afford to fight wars on the internet on all fronts. And, with the help of AI, it will only get worse. Logic is the only solution to save a nation under attack in the world of misinformation. Just take a look at completely brainwashed Ukraine. They truly believe that Russia would want to destabilize neighbors of all options, to have trouble right at their border with people who also can speak Russian. What Ukraine now attempts to do is to decrease informational dominance of Russian language in worldwide field of information, decrease economic activity at Russian border, basically weaken Russia. Ukraine became even poorer and it’s even easier now to buy Ukrainian government, they can’t even pay proper salaries to officials. The agenda is obvious to any sensible individual.

What could potentially happen if all Ukrainians were studying logic in school? Logical people are more predictable, since they think alike, rationally, they are safer, and they are worthy of genuine trust. First, even more Ukrainians would immigrate to other countries with higher standards of living. Sounds like bad news for a politician, unacceptable. Well actually, these immigrants would create an authority in the eyes of the world as very intelligent individuals, it would help Ukrainian people’ patriotism and improve their morals. The economy would not be as bad. There would be less crime, more integrity and more overall happiness, less bad habits, better health, better productivity, more patience. In the long run brain drain would eventually decrease. Average IQ would significantly rise. And most importantly, Ukrainians would not become victims of brainwashing and so much less people would die. While logic could also lead to more disagreements with the government, nowadays, logic is clearly a virtue for a nation to master. Whoever says otherwise is a liar. We do not need equality, we need to make humanity Sapiens.

Surveillance nightmare

They will say, it’s because of terrorism and child trafficking. This is true and noble, until it isn’t. It’s now against wrong-think too. When we stand before potentially multi-millennial tyrannical empires, we have all the reasons for wrong-think. While we still have rights for it.

To understand what US surveillance has to offer what’s required is to know that China has bought surveillance technology from US. Obviously US does it in a more democratic way, still stays nearly as tyrannical as far as their actions go. History shows it pretty well: richest empires always have the most blood on their hands.

Tracking suspiciousness level of users’ traffic is “democratic enough”. Basically, if you actively use google for cryptocurrency research, you are probably more suspicious than average user. It’s nothing until it isn’t. For now most crimes are being overlooked even if reported I guess, because if it was used against everyone, then it will be too obvious and it could easily become a scandal. It is used only to track terrorists or people who acquired wealth or fame. A way could be is to share your PC with a woman, or to use a very sophisticated bot.

The problem with US surveillance and informational dominance is actually on a whole another level than China. Google and Microsoft always have to comply. All billionaires have to comply, basically if you see a billionaire in good health, it means that he is basically a government official. If you think that riches will give you freedom in an empire – you are naive. Steve Jobs was attempting to protect users’ privacy, his views on privacy were “old fashioned”. He could be poisoned.

If a billionaire disagrees with the government – he dies. Happens everywhere, all the time. The governments do not like any competing power even if this power is reasonable and civilized, they crush billionaires as they crush disobedient third-world countries, without any sense of integrity or dignity. I am not saying that wealth working with the government is a bad thing, I am saying that when most of the wealth concentrated in a couple of countries – that’s a point of failure for humanity. So to think of it, if you become a billionaire because of cryptocurrency, after you will be identified you will have to fuel this surveillance nightmare like a good dog, and when the time comes, you will have to donate 90% of all your wealth to charity like Bill Gates did, because your money are not considered yours to begin with, it appears that your money were allowed to be yours. They really don’t like power out of their control, as soon as you reach a certain limit, your business world becomes a world of politics, and, in your life, integrity becomes a sham. And, if you will be a good dog, who can guarantee that a competing government won’t kill you someday?

So basically Google and Microsoft are government corporations. And they have access to information of billions of people. More than that, CIA can push updates dedicated to special concerns. Say, you want to take out some Bitcoin out of your cold wallet on a Windows PC. You launch wallet software and next minute what happens is that the system freezes completely with a notice of urgent security update being pushed, a minute later you see that your wallet is empty, this security update transferred everything to an unknown wallet. And it was an official Windows update.

A week later you find out in the news, that Russian hackers exploited Windows update servers in your country. Maybe you just born in a country which CIA does not like, maybe Russian hackers actually never use a VPN, what gives now anyway. Basically, as economies become increasingly digital, CIA can severely damage these economies with a click of a button. As EU becomes more and more distant from USA, it can happen in EU, as long as EU citizens continue to use USA spyware. There are so many ways to spy on you, for example modern GPUs. They are so powerful, taking screenshots every second would not produce noise on performance diagram. Better use only open-source drivers. US is well aware of the power they hold in worldwide informational field, it’s very interesting that they attempt to make fetching from their social networks as hard as possible, they want to keep all the information about a half of the world to themselves. They value this dominance badly.

How can they prepare a stable tested meaningful update ready to be pushed live in one day on a consistent basis? They just don’t, it’s not really an update of the software, it’s just an update of tracking headers/info.

All this spyware will quickly become a thing of the past, as people will stop using closed source programs. So how will governments fight terrorism and child trafficking? If they won’t simply enforce using approved spyware by collaborating with hardware manufacturers, they could move surveillance out of citizens’ private life at least partly, out of their homes. Street surveillance could become much more advanced, the problem though, it’s expensive to research, develop and even much-much-much more expensive to bring it on the streets everywhere. Do they have a choice? As long as we are silent, yes.

Allowing privacy at home is certainly a must. Maybe mobile phones have to remain surveillance devices? Personally, I do not believe so. The government should track only immigrants and tourists(with their consent), and former prisoners, but not lawful citizens who were born in the country. Russia has bought surveillance tech from China, if cybergulag expands to Russia now too, the probability of conventional wars increases.

History however shows that privacy of the individual was never respected. We have to demand it as a right, establish it as a right. The internet is the bastion of freedom, and they want to take that from us. And as we speak, they develop a powerful super-weapon to leave us no chances.

Centralized AI tyranny

Needs some general computer science knowledge and common sense to understand that they now have a mass brainwashing machine and an effective surveillance data analysis. Twitter was an AI playground for years now, it's the most suitable environment with very short posts. That's easier to compute. The bots probably never need to enter any captcha or add a phone number to an account, they are probably trusted. These bots can help plenty with psy-ops. They can push any chosen lies or/and agenda. How advanced/effective are they? Can't possibly know how bad things really are. What we can estimate though is potential scale, these bots can probably flood the whole Twitter/Youtube 24/7 if required. And these bots are learning, in certain circumstances they probably can mimic not very intelligent humans already.

Surveillance can become very sophisticated with AI, it is probably already capable of identifying potential terrorists in no time, which is good. What's bad is that this surveillance can be used against any sort of wrong-think. Somebody could commit a crime, his internet browsing history is digested by AI, now the AI knows how to quickly find people attempting to do the same. Even if it means mixing them with people who would never do the same.

They try to hide it all the time, they use absolutely shocking headlines to shift masses' attention from real issues. I firmly believe that a convenient democratic solution is to track only immigrants, tourists and former prisoners. If there is no freedom for the individual in his home – there is no future for humanity. It won't be humanity anymore. It will become an army of mindless drones, incapable of even thinking against the system which takes away their freedoms one by one slowly, through generations, so that it will never be noticeable.

What a bloated government usually does, when it's power already solves everything like terrorism and child trafficking? It start to abuse the power, as it has to act on something, a department has to deliver the results of their work to superiors even if there is nothing to work on. Nobody wants to lose a job. So they will spy on wrong-think closer, will spy even on completely innocent citizens and if there is nothing else to do – will pressure them in one way or another.

What's good about AI surveillance technologies? It is capable of protecting national internet borders against destabilization and cyberwarfare attacks. So with AI, if it was available to every country it is possible to keep open borders for the internet forever, it is even possible to drop Chinese firewall.

As long as I am alive, I will develop fully open-source text-generation AI, so that anybody could use it to broadcast his opinion on the internet, and every country could use it to protect internet borders. Participating in this project for other developers could be too risky depending on their country of residence. Hopefully, we will not experience lack of support. I believe that any country except US and China can potentially support it. Will be interesting to see what the governments will do with this technology, as they will have a choice to stop lying to their own people.

If cybergulag becomes a thing, it could lead humanity to extinction easily, the probability of nuclear weapons being used again increases. China and United States are pretty much ready for an enormous amount of casualties and deaths if required. While China has an increasingly huge population, United States is the Land of the Free many dream to live in. If United States population will shrink for whatever reason, they can just ease immigration rules at any time, get more fresh blood.

All they need is to make sure that no citizen knows about what is actually going on. With deep fakes it can become even worse, people won't even know who is dead and who is alive. AI can make the internet polymorphic, show different content to different users on the same resource. We must prevent it by any means.

Blockchain as possibly the last chance

Decentralized blockchain gives real power to wrong-think. One billionaire can easily be observed and *influenced,* but 10 multimillionaires are a lot harder to track, find and change their mind, more than that, their collective brain power can do a lot more. It's possibly the last sanity check humanity has as of now before multi-millennial surveillance nightmare is established, and humanity just wastes it. Soulless scammers sincerely believe that taking away others' money is good. The thing is, this is a completely new space, new paradigm that waits for more and more innovation. Why would you scam people, if you can innovate? Really as we speak, it's possible to find yet another solution to a real world problem, fix an inefficiency, but still, what people do is lie to each other. You won't be able to fight what comes alone, it's just stupid, you forgot the way. You forgot about what Szabo was talking about. You forgot why Bitcoin was created. While probably it was an attempt to cover medical expenses first and foremost, the creator inevitably, willingly or not, left a fingerprint of his beliefs in his creation. And it's not hard to see that Finney followed Szabo beliefs. They have shown us the way, we must not forget it. US and China own Bitcoin and can pretty much choose the course of blockchain development. No centralized entity on Earth should ever hold so much power. This is just inhuman and will likely lead to more and more tyranny. With RAID now, the power Satoshi gave us will not be wasted regardless of cryptocurrency bans. If they trap us on the blockchain – they will only regret it.

Free open-source software

As we are barely ever aware how much the society needs free software, I would like to expand on free open-source software philosophy as much as I am able. Broken Windows Theory suggests that if there is a window broken in the neighborhood, and for some reason the budget to fix it is lacking, people around become more and more anxious with time. Some teens can start gathering around seeing that the place lacks supervision. Them partying disturbs the neighborhood, making it more subject to anger and poor decision making. After teens come actual criminals. Depression and fear slowly, barely noticeably spread around the broken window, a possibility of a crime occurring increases dramatically, drugs abuse, murders, suicides. It is also called Butterfly Effect.

Anything that makes our lives more comfortable does exactly the opposite. Any new technology which increases quality of life and any great free software indirectly prevent crime. It positively influences the lives of those who can barely afford any nice things. It's almost like free software developers are modern Saints. I'd fight for them. Supporting free software is supporting Good.

While it’s not as much related, however torrents allow low-income individuals to relax and forget about the misfortunes of their lives, avoid doing anything really desperate and stupid. Is it bad to prevent crime?

Free software increases innovation pace in software development, advances multi-polar capitalism and therefore increases overall innovation pace. Also, it gives more power in the hands of individual programmer or user. A world full of high quality free software is much harder to obsessively control.

The governments keep software closed source, especially US. Naturally, if Windows OS were to become open source, any government could easily create a copy of it and adapt it for own needs, which would limit US surveillance power. Surveillance agenda is always against open source. Free software could decrease the costs of development dramatically, for example AAA+ video games would certainly cost a lot cheaper to develop, therefore would probably contain less bugs and the developers will focus on more and more innovative game design which will stimulate kids' brains to develop faster. Many industries would be thriving with richer free open source availability. RAID will support free software as much as it will be able.

Immortality

Modern humans are potentially immortal and all of us should have the right for cryopreservation before dying. We don't need a spit in the face in a form of elders' care. We can use our retirement money for cryopreservation. We can have, even if weak, real hope of returning youth back. We can stop dying in regret of forever lost years. If only we choose. We will supervise cryopreserved humans' rights to be fulfilled until the very time they will get revived and they will be able to claim everything they have, not wake up to slavery.

Humanity will always remain an existential threat to itself. This is why in the future many absolutely unimaginable technologies will be researched to prevent extinction. Even if better ways of life prolongation would exist, revival of cryopreserved humans is a technology which will eventually be researched. This technology is another way to increase survivability of out kind, so while, depending on circumstances, it could be forgotten for centuries, it will have it's time.

Immortality won't devalue life. For a time being emotional response becomes less intense, but it will all come back inevitably. If everybody will stay healthy for eternity, they would strive for new experience for eternity, and the amount of new experience present in the world increases exponentially with innovation. We already have plenty! Do you have enough years to read every book, watch every movie? Immortal humans' lives won't be an eternal decadence, all immortal humans will inevitably find something very important, will obtain soul, sooner or later. Immortality will actually increase the value of life(at least in the eyes of the individual). Immortal human has genuine hope for the future, immortal human sooner or later loses any reasons to lie. Nobody would go to war, nobody would kill, or at least it will be very rare. Immortal human will be extremely intelligent and incredibly experienced, forever young and healthy he will discover and learn. Immortal human can enjoy existing only in exchange of the ability to quietly think and explore imagination freely. Even if the science and philosophy achieve absolute understanding of every single thing in the universe, immortal humans will still find Meaning, they will build It for each other out of sheer Need. There will be no reason for the government to lie to immortal human as he will be wise and educated. Immortal human won’t sin as the main driving force behind sin is probably fear and greed. And immortal human will not fear, will not envy, will not crave. Eternally beautiful woman will be virtuous and truthful.

My personal goal is to bring next-level efficiency to medical science, cryopreservation, and anything related to life extension. Could be a grave mistake, because it’s basically interfering with international politics. Could not care less about that. I am supposed to be dead already. I was on the other side, I know what it means to be a moment away from death, what dying people feel, when the immune system fails, when dopamine and serotonin drop. They just stop wanting to live, that's it. That's how we die. Because we don't see a reason to continue. Old people do not seek cryopreservation, because they just give up on life altogether. Slowly with aging it seem to happen to everybody or almost everybody as systems start to fail.

Well, so far time goes, I am still lucky. Maybe the only reason I am still alive is because I have something very Important, something Unfinished, Meaning. I have RAID. While I will attempt to survive and probably will get cryopreserved, in no way I want to wake up to a dystopia. I am simply incapable of closing my eyes on truth, immortality with surveillance will probably turn out to be Hell. This system is a real tragedy. So I came to the terms. If something happens to me – so be it. One thing for certain: I am not going down without a say. And I want anyone who is dying to have a possibility to let the world know. I want to make all dying people an existential threat to tyranny.

Bottom line

Many things you read in this draft will become just rumors, I am going to deny everything. In fact, I have found this draft somewhere on the torrents, it's not even mine, and I condemn it, I merely use it as a reference point to the design of marketing token, and certainly, this paper has to be rewritten.

RAID doesn't care who you are, what’s your age, gender, ethnicity or skin color. It’s here to preserve the freedom of your opinion. Hopefully, your opinion does not oppose your government, but if it is: you need to understand that when national agency of your country will find you, they will break your resolve, your willpower, regardless of how fearless you are. In some cases it will just take more time, in few cases it can take years, but eventually you will forget who you are, they will reshape you. Even if your aspiration is noble and inherently good – be prepared.

I hope, I believe that RAID will spark a lot of awareness in humans, a lot of thinking, reevaluanting, paradigm shifts, possibly teaching them to think critically, to see the world differently, be closer to reality, become smarter, wiser. Better humanity is actually possible. We can do it. Expose everybody to the very truth, painful truth instead of lies, and witness enlightenment. If we let painful truth to be everywhere, involve everybody, then it is possible. If we only have a few exposed to this truth, while others are still living in lies - it only brings more pain to those few.

Let’s fight each other on the internet until total exhaustion. And after exhaustion we will become friends. And after that we will turn against governments' lies. Together. No country will be able to brainwash it's citizens ever again, their lies will become worthless, futile, as it should be. This is war for truth. Without guns and casualties.

With every innovation comes good and bad, and we can't change that. Can we ever? It's probably normal to be afraid. Hopefully, RAID won't be a mistake. I sincerely believe that decentralized monarchy with no central figure like a king could help to solve many issues the world currently faces. Or maybe not solve, but at least take necessary steps towards the solution. We could also expect that RAID technology won't be the only solution to preserve the dignity of humankind, the ability to look at the truth right in the face.

I am not in charge of RAID and won’t be able to stop the direction it’s taking. I can only hope that RAID won’t be a group of politicians, but a group of Philosophers. And as modern situation is such, that mostly conservative views are being censored, I sincerely hope that RAID won’t be a group of nationalists who are ready to push the button, but a group of Patriots who would never push the button, because they want their country to thrive, not to be in ruins. Good luck, gentlemen.

Part 2. Design overview

Decentralized word-of-mouth marketing service

As of today internet personality bubble reaches absurd levels, a mere mention by an internet celebrity can a very significant amount of money. It is generally believed that buying internet personalities' time or creating an ad-trailer should be expensive and it’s worth it, however it appears than a new more effective alternative to this already exists and actively being used. And it appears that it is certainly possible to achieve this in a decentralized manner when the employer and the poster don't need to know anything about each other except the stake, eliminating the need of assembling a marketing team or trying to apply to real-life jobs.

What ad trailers and internet personalities attempt to do is not just to sell, but to start a *discussion* to increase awareness, to pump up the popularity of the product. Word-of-mouth marketing, proof-of-discussion, whether it's praising or sick burning, FUD or optimistic insights, blind cult following or elaborate arguments, - the discussion behind the product is what really promotes the product. Celebrities and ads are just a third-party and it is certainly possible to eliminate this third-party and pay directly for discussion and mentions instead. A mass discussion by nobodies for nobodies. RAID attempts to provide income to socially inept, traumatized, schizophrenic, mentally challenged and physically disabled people, so that they will never be kicked out of their homes for being unable to adapt to life.

The primary utility of the token is being a sovereign currency for exchange between employers and posters. Employers buy RAID token, setup and fund campaigns with that token in Raid Market contract with chosen key strings or topics on chosen websites, posters commit to these campaigns by discussing certain posts or anything eligible(matching keyword) for paid discussion. By default, posters are allowed to express any opinion on every topic, and, depending on the resource, posters by default have the right to completely derail the discussion, talk about weather, discuss investments, etc. Posters will get paid for unrelated discussion as long as it for example bumps the thread, or adds another comment to discussion making it look more heated and popular. RAID default marketing paradigm promotes critical thinking. Again, it mostly depends on the resource and a forum could simply ban/remove unrelated posts. Posts need to be witnessed by oracles, so a poster has to ensure that his post satisfies the rules of a website. Campaign settings are flexible:

1.Ppp – pay-per-post. Defines how much posters get paid for a post in USD value. As RAID token price decreases, the amount of RAID being paid to posters increases. USD index is monthly and is average price of RAID token last month. Therefore if a campaign lasts more than one month, amount of RAID paid per post adjusted automatically to ppp. Ppp can only be increased by the employer if edited.

2.Array of key strings. A key string can be a word or a phrase, a sentence, a text of any length. If employer sets more than one key string, then these key strings become options to make the posting more natural, if a poster mentions just one of those key strings or posts below an op post with one of those key strings, he is eligible for a reward, and there is no point for him to mention all key strings.

3.Mandatory key string can be left blank. Requires to use mandatory key string in every post regardless whether the post is related to key string discussion or not.

4.Array of target urls. The campaign works only on the websites with these urls. If none set – it means everywhere, dapp interface will help to easily choose most popular resources.

5.minStaked. Minimum requirement of locked RAID tokens for a poster to have to join the campaign. It can potentially help with moderation or eliminate the need of moderation completely, depending on the chosen route of marketing campaign.

6.nonEditable, a boolean. Can be set to true in it's inception or at any point in time, to allow the employer to first set it up looking at results. If a campaign is non-editable, it can attract funding from other employers, basically allows to make it last longer potentially.

7.noFiring, a boolean. If set to true, posters can't be fired at all, so that posters will more likely join the campaign.

8.onlyManualApproval, a boolean. If set to true, posters can't join the campaign without employer' approval, when this is set, then minStaked is ignored completely, even posters with 0 RAID tokens locked can join as long as approved.

9.KeyStringPerWords. As an example, in a job which requires 1 key string per 1000 words, if a poster writes 4 posts 250 words each, he has to mention the key string in those 4 posts at least once, and he will get paid for those 4 posts.

10.MinPostLength. If the requirement isn't met by the poster in a post, he is not eligible for a reward for the post.

11.ModsPay. Needed if the employer does not feel confident and wants to moderate the campaign, but has no time for that. RAID mods are not obliged to follow the rules he wants to enforce, however they are assumed to follow the rules he wants to enforce, since mods salary(independent from ModsPay) is not fully tied up to RAID to USD index and because the governance can fire them prematurely.

12.rulesLink. A link to a post explaining the rules for posting in detail and ban rules. In the spirit of default RAID campaign can be left blank.

13.expirationDate. By default it's 3 months from creation, can be set only longer. If the budget of the campaign is not exhausted, and non-editable set to false, the remaining budget is being refunded to the employer.

14.minCreativity. Decentralized moderation evaluates some posters' creativity, emotions and sense of humor and increases it with time.

15.postRate. Currently in Polygon blocks. Determines how often a poster can post eligible for payout posts in this particular campaign. Default is ~1 minute, if poster posts more often he is not punished, just not getting paid for more.

16.maxPosters. A limit to make small budgets viable. If not set, might be computed automatically, considering that posters have to cover expenses of rewards claiming.

17.startTime-endTime. By default 0 to 0, which means 24 hours per day. Specifies time of day, when the campaign is active.

18.An array of campaign languages. Left blank if any language. RAID can probably support at least up to 256 languages. If not left blank, then only posters who can join are those who stated their language. A poster can't alter his language, he can only choose to set one or not to set at all. From the start, posters of different languages will have same pay-per-post for default campaigns for fair distribution.

-Some of the most expensive commercials ever made cost around $30 millions. This amount of money in RAID could produce 300 millions of posts, if the compensation is 10 cents per post, and an absolute overkill campaign of 3 billions of posts if the compensation would be set to 1 cent. The most commented videos on Youtube have less than 15m posts, so a campaign of this scale could be used to promote brand commercials on Youtube and potentially create unprecedented so far public interest. This campaign could also build the community around official accounts and to set given keywords trending for a prolonged period of time on different social networks.

-Twitter influencers can mention default RAID campaign, so that the posters will more likely discuss that post, helping to promote that Twitter influencer profile.

-On websites which support nicknames posters will eventually be able to talk about anything with nearly anyone anywhere as long as they have keyword in their nicknames.

General technical principles

1.Accuracy is expensive.

- Stone Age math whenever worth it, minimum Solidity store loads and writes.

- Packed structs if more than one value of a struct is altered by a method.

- Store numbers with less decimals where possible and convenient. Restrict accuracy where possible and convenient

- Hardcoded addresses and values whenever possible to, again, reduce store calls.

- Queue Transfer Contract will be introduced later, briefly it's a bulk sender which allows to perform certain actions in a collective queue. The cost of Queue Transfer for the end user can be potentially reduced to 1 store write as trustless version and to 1 emitted event as a trusted/trustless version at the expense of waiting until the queue gets filled and executed.

2. Decentralization is the most valuable concept of our times.

- Bitcoin forks are more centralized than Bitcoin. If it will be required then top holders of Litecoin could be found and influenced in a way that allows the government of a nation where top holders reside to acquire a lot of control over Litecoin. BCH and BSV wealth distributions are considerably better than Litecoin, still worse than Bitcoin. A huge dump has the potential to weaken the security of the network, and after that it can be reorged in any way required. Today, cryptocurrency is potentially regulatable and mutable as is. There are ways to change this.

- RAID attempts to revive old concepts of decentralization, and aims to be decentralized in any possible way. There won't be a CEO, there won't be a Lead Developer, there won't be unilateral decisions, no wealth concentration hopefully.

- RAID solves blockchain wealth distribution problem by implementing old like the world CeFi feature - active income(salaries). With it, RAID can expect Gini coefficient closer to real world CeFi levels than any other blockchain project. This pushes decentralization security standards on another level.

3. No mandatory auto-updates. No hidden tracking.

- RAID dares not only to support this standard, but to promote it and make it the only acceptable standard. Auto-updates will be always disabled by default(if possible, Chrome browser does not allow that)

4. Free open source.

- If it wasn't for free open source, if no free libraries would exist, the development of minimum RAID functionality could take years. And RAID could be a puzzle for something greater.

Base contracts

Ethereum is the blockchain of choice as the most popular and robust censorship resistant chain, and with an assumption in mind that blockchain industry is fundamentally monopolistic in a sense, since the biggest network is always the most secure, which attracts even bigger capital and in turn makes it even more secure. And in case of Ethereum even more censorship resistant. Base contracts will not be owned by the deployer or governance and won't be upgradeable.

https://github.com/SamPorter1984/RAID/blob/main/contracts/VSRERC20.sol

1.First and main contract is "Very slow ERC-20" implementation(VSR ERC-20). The implementation utilizes standard ERC-20 function _beforeTokenTransfer() in such a way that prevents treasury fund from dumping on the market. The function checks how many blocks passed from rewards genesis block and allows to claim only a certain amount per every passed block. Basically developers and all other participants of RAID can only claim rewards within constant emission limits and this hard limit can't be avoided. Even if treasury happen to be upgradeable, no matter what kind of logic will be present, even if the contract will happen to have a bug, the bug in no way will be as devastating as it could be without _beforeTokenTransfer() guard.

Allowances in this ERC-20 implementation are made booleans instead of integers. As it seems so far, allowances computation is wasteful in very most cases, since nearly all protocols ask for infinity-1 allowance. RAID token has the cheapest transferFrom() of all ERC-20 at the time of writing.

Another feature is bulkTransfer() and bulkTransferFrom() methods. These methods require an array of addresses and amounts as arguments and compute balances of an array and only after that compute the balance of msg.sender, instead of how regular transfer would compute the balance of msg.sender after every transfer to an address, which makes bulk transfer twice cheaper. BulkTransfer() can be used by treasury to distribute rewards and bulkTransferFrom() will be used by Queue Transfer contract.

https://github.com/SamPorter1984/RAID/blob/main/contracts/FoundingEvent.sol

2.Second base contract is Founding Event Contract. This is a liquidity generation event(LGE) proposed by CORE token team with certain differences which I believe most suitable for RAID. Founders Contract is a trust minimized LGE. It automatically creates liquidity on first transaction after last LGE block. I can't transfer Ether from it, nobody can. To ensure critically required in case of RAID decentralization, the LGE will last for 2 months. Liquidity is not locked at all, instead an incentive to keep liquidity is introduced. Rewards for Founders and liquidity providers in general depend not on the amount of liquidity shares they stake, but on the amount of RAID tokens present in their liquidity shares at the time of staking. And this number won't change as long as a given provider does not unstake the tokens. So, for liquidity providers the incentive to provide liquidity and stake increases if the price is going down. While RAID is not expected to give any returns or any kind of guarantees, if the price increases - founders have the least incentive to unstake. As soon as they unstake, they lose the advantage. Founders also lose Founder status as soon as they unstake their liquidity from Founders Contract and become a liquidity provider.

Founder status gives Founders ~150% higher rewards than a normal liquidity provider, which is done in an attempt to mitigate potential losses. Becoming a Founder is an even greater risk than participating in the ecosystem after Founding Event concludes, therefore their rewards are higher just in case. To learn more about risks, you absolutely need to read the last page. Founders, as well as liquidity providers, are able to switch addresses if they feel the need to, which allows them to claim their stake and rewards from a different address.

Every Ether deposit is being subtracted by 0,5%, and this 0,5% will be used for audits, bug bounties and development like oracles, servers, RPC, ddos protection(as it starts with centralized oracle and only after moves to completely trustless architecture) and any other expenses required by RAID during LGE.

https://github.com/SamPorter1984/RAID/blob/main/contracts/TrustMinimizedProxy.sol

3.Raid Market which was already explained.

4.Trust minimized proxy. It's an altered OpenZeppelin upgradeability contract with some features that allow to remove trust to developers and/or governance. New logic implementation is not being set suddenly, instead it is being stored in NEXT_LOGIC_SLOT up to NEXT_LOGIC_BLOCK_SLOT, or for a month or so. The period allows participants to identify if the deployer or the governance is malicious and therefore to exit safely. Next logic can be canceled in case of a bug discovered or upgraded to after month passes. It is impossible to cancel next logic and immediately propose another next logic, because there is also PROPOSE_BLOCK_SLOT which disallows proposing next logic more often than once a month. It is also possible to add a value to PROPOSE_BLOCK_SLOT if for example a situation arises in which there are no plans to upgrade a particular contract for year maybe, so that it keeps participants piece of mind for that period, because no upgrades are possible during that period. This variable also can be set to infinity-1 to essentially.

Additionally there is DEADLINE_SLOT, the block after which it becomes impossible to upgrade the contract at all. Admin keys are burnable and just in case DEADLINE_SLOT stays. I would like to encourage DeFi developers community to use this proxy as soon as it gets an audit, so that the amount of scam could potentially decrease at least a little bit. However, there is no warranty even after audits.

Public temporary database

RAID will use fast centralized public blockchains as temporary databases or optimistic roll-ups which are incapable of any censorship, one of such roll-ups is Arbitrum. First, RAID can start from Polygon Network. The database should be blockchain agnostic, because fees on a particular network can become unacceptably high for posters.

Database contract is a simple event emitter with settings variables for oracles to act upon. Posters emit events in database contract with the information about their posts. Oracles then verify if those posts exist. Commit-reveal scheme nearly eliminates front-running as well as disallows oracles to alter the transactions and allows this system to scale to any number of posters and websites. Emitting an event ideally has to be a lot cheaper than 1 cent. After and if all fast blockchains become more expensive than RAID requires, there are at least 2 solutions to resolve it:

1. Add oracles between posters and the blockchain on which they emit events. This solution could also allow to use slow chains like Ethereum Classic.

2. Create super lightweight restricted to certain functionality second layer only for oracles to act upon. Could use Autistic roll-ups(an even lighter version of optimistic roll-ups, specifically dedicated to support oracles with events being wiped regularly).

Or both. Ideally, RAID will have to give a poster a choice: broadcast through an oracle aggregator, or broadcast on his own.

Raid Wallet

RAID wallet is a browser extension. As of yet, no ability to connect to any website, no ability to transact either, it’s a brick. Extension was supposed to be a Metamask fork from the start, however, Metamask has committed heresy against free software license. RAID wallet does not connect to any website as of yet, so the probability of it being fished is reduced. It’s very insecure nonetheless as of yet.

The extension fetches specified form data, stores the post and sends a hash of current post and previous post to the blockchain. It can operate on nearly every website on the internet, any social network or html-js chat, from Twitter to Twitch. Functionality of this extension is restricted during beta-test to certain imageboards and Twitter by centralized oracle. It will probably be restricted for a lot longer than that, and different relevant websites support will be added gradually over time.

Planned functionality:

1.Custom encoding for languages which could require that, as UTF-8 is inefficient by blockchain standards. Every community dedicated to specific language can submit an efficient encoding scheme if they feel like it’s needed.

2.Everything that a modern wallet has, including encrypted keys being stored on the user device only.

3.Limit orders and any other orders useful for dex trading.

4.Queue Transfer contract interface for cheaper but slower transactions.

During beta-test posters will be able to specify any secure address which to receive beta-test salary, the extension itself is not supposed to hold any funds as of yet. After extension will be secure enough, the posters will lock a certain amount of tokens in poster wallet to be able to work. Different jobs could require different lock amounts. Posters can also participate in governance with their locked amounts.

Decentralized moderation

Sense of humor is the only way to prove that you are human. It's the last frontier of humanness in AI' world. Moderators of different language communities have to be not only Patriots, but also Comedians. Good sense of humor could be promoted and given a higher pay(but the difference should not be too high, so it won't discourage anybody). There are probably other ways to recognize genuine humanness at least as of today' AI development. Creativity, emotions. Promoted posters can help with moderation. Moderators can potentially be unfair so it's required that they will be reelected frequently, probably once a year, and have a high enough pay to care. To become a candidate defining language is required and it will be set in stone. To vote for or against candidates, it's also important to define the language, so voters have to not only lock their voting power, but also they have to set their language(or they can leave it blank, anonymous, except they won't be able to vote for mods and anything else related to specific languages).

How can we be sure that moderators of a language community we don't understand at all actually does the job correctly? Simply test that community. First we try to spam in our languages and get banned eventually, then we go to other languages community and try to spam random text after translator or fetched posts from all over the internet, maybe from previous threads, and see if we get banned. If we don't get banned – we just add more bots and get more tokens. Either way, bad moderators' job will be revealed regardless of language. All moderators' job should be public and shown on the website with history of addresses they have banned, so that independent reviewers could point out to censorship. No moderator should be able to ban anybody single-handedly but instead a group of moderators vote, and only most voted addresses will be banned. We can add a second layer of moderation to this to make it nearly trustless: most voted addresses by moderators cannot receive any pay for posting until DAO decision. The DAO can take from locked stake as much as the account posted or revoke punishment.

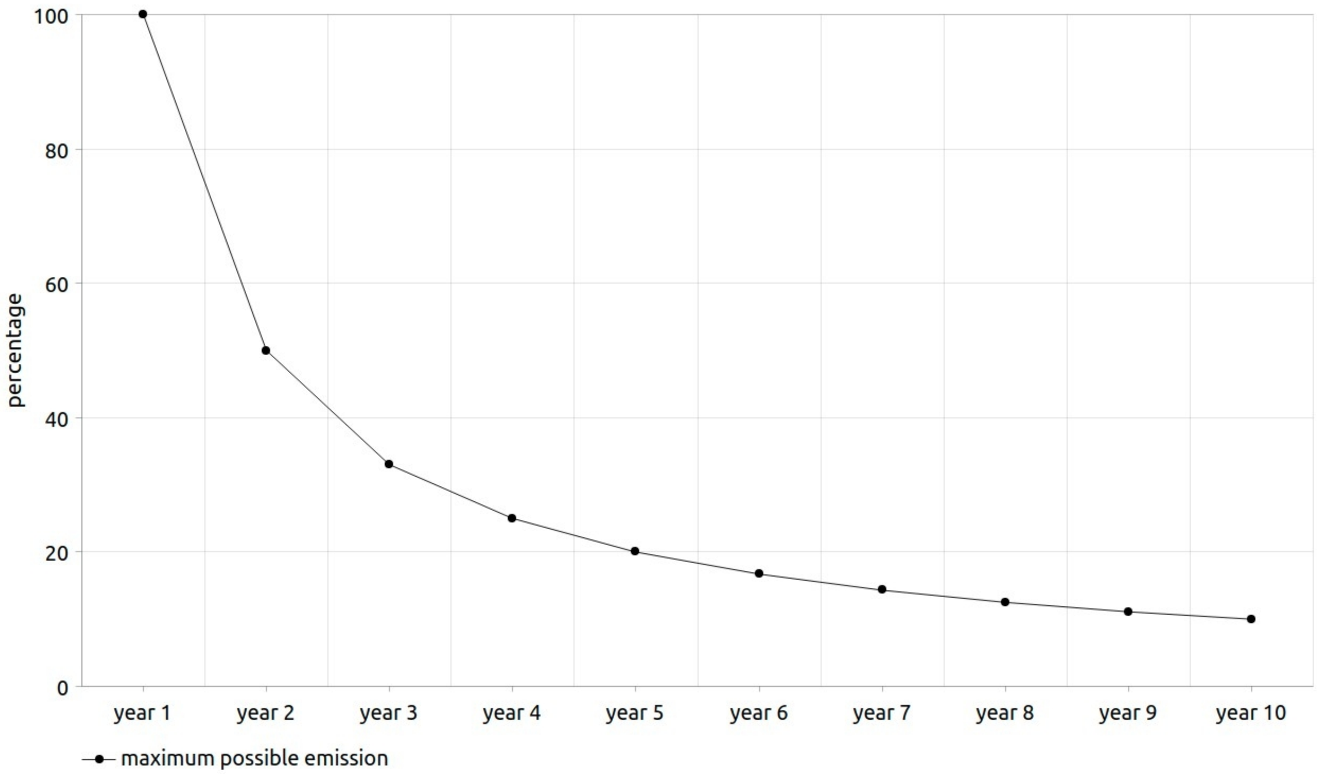
Moderators salaries have a base salary which is not dependent on monthly RAID to USD index, and also they will have a small bonus depending on the amount of active posters in their language. The bonus is small, because a big one can further the disparity of adoption between popular and less popular language communities. RAID moderators are also community managers and tech supports, and they decide between each other how and what and who will do, the governance will be able to fire lazy or unfair elected officials prematurely. First year officials could be elected by Telegram polls. Officials can define how they will run the community, they decide if they need to run a blog, a Twitter account, or whatever else. For second year elections governance contract will most probably be ready, so that the community decides upon if they want to reelect former officials or to introduce new ones in a trust minimized way. A Telegram bot, and probably more than just Telegram bot, will be required to grant mod status to elected mods.

Tokenomics and Treasury

Token utility and multi-year token locks require high inflation in order to support decentralization progress.

Starting supply: 1 million.

Total supply: 1 billion.



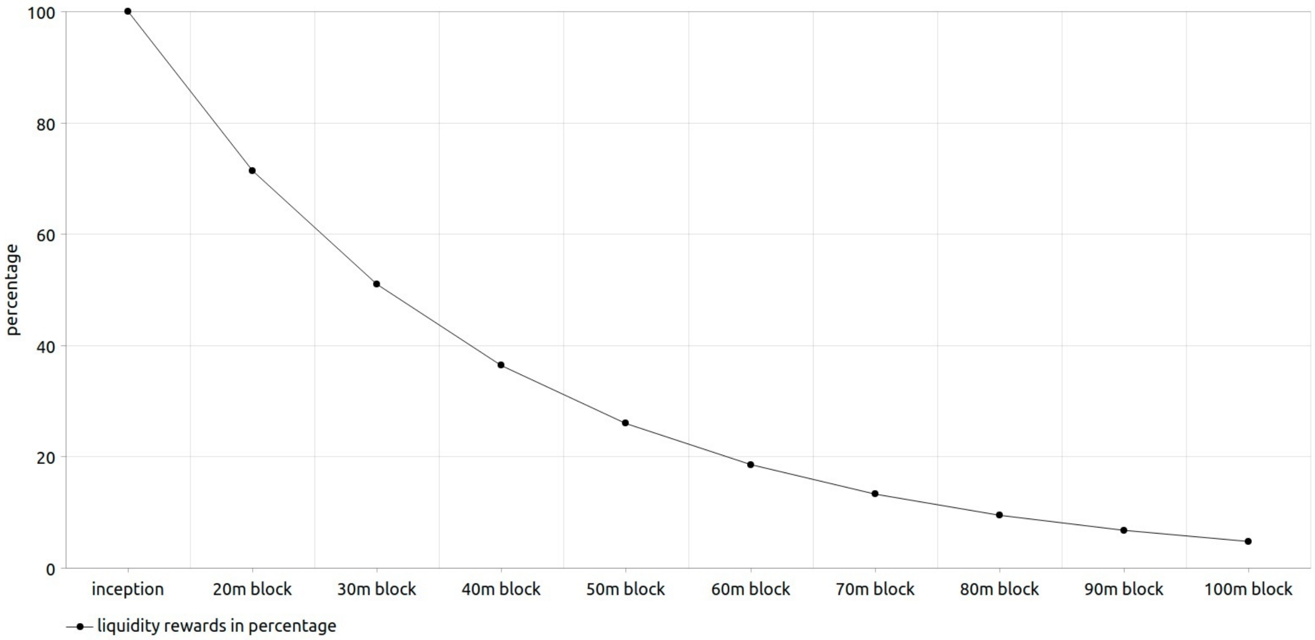
Emission: maximum emission is approximately 1 million each year. First year includes testnet rewards, 0.001 token per post. Note: while some funds' tokens are being unlocked on fixed schedule, it does not mean that all unlocked tokens are being claimed, so it's better perceive these numbers as maximum possible inflation, not actual inflation. The reason behind these numbers is mainly an attempt to make 1 token always affordable to the residents of poorest countries, assuming that Pareto distribution in cryptocurrency is extreme, as the main income in cryptocurrency space is passive. It's important for numbers to be comprehensible to not only economists. Another reason is that if RAID uses mint function with upgradeable contracts which could potentially have a critical bug, it could destroy the project completely, so there is no minting at all and _beforeTokenTransfer() used instead.

Treasury is an upgradeable contract until finalized, the reason for this is that it's still a challenge on how to implement trust minimized management of the treasury. A deadline of 2 years for finalization is hardcoded in upgradeable proxy, if the contract won't be finalized at that point in time, it will be set in stone as is.

Treasury will support:

1. Default RAID promotion campaigns. Posters will receive salary for default campaigns from treasury. _beforeTokenTransfer() fixed emission ensures that too many posters will be unable to consistently claim salaries. It does not mean however, that a poster who was unable to claim loses his salary, he will be able to claim *eventually*. This will allow to properly setup and scale oracle network to prepare the network for more posters. This could also create an incentive to FUD RAID in case when there will be too many posters, which will result in mostly smart posters getting on board(while Founders would more likely rather shill RAID after Founding Event is over). Default jobs will have least requirement for tokensLocked, and probably least pays.

2. Founders and generic liquidity providers. Founders have starting rewards equal to 5% yearly for their ether contribution assuming that the price of ether and raid token stays constant. Founders will have 150% higher rewards for same tokenAmount than generic liquidity providers. Rewards for both groups of beneficiaries decrease by ~28.571428571% every 10 million blocks. TokenAmount is a variable that represents the amount of RAID tokens in liquidity shares at the time of staking these liquidity shares. Founders' liquidity shares are being staked from the very start, and their total tokenAmount equals to starting supply, 1 million. As a founder unstakes, his share of rewards is being redistributed among all remaining founders. Liquidity providers collectively get 150% lower rewards than founder rewards, and share their rewards together without accounting for founders rewards at all. If a liquidity provider stakes the minimum amount of liquidity shares to get at least 1 wei of tokenAmount, as long as he is the only one staking, he receives all rewards from generic liquidity providers pool. This solution could potentially eliminate third parties like Unicrypt.



3. Monthly meme contests. Governance will vote for best memes monthly and a top third of winning memes each month will receive rewards from treasury. To prevent too much spam in meme contest while at the same time not causing stagnation, only addresses with at least 1 RAID token will be able to submit memes to the community as NFT. Winning memes are being resubmitted for the next month, therefore best memes can receive rewards for several months.

4. Oracles. RAID is heavily reliant on oracles. The oracle network around RAID might become massive. Especially if we attempt to fulfill the idea of pseudo-anonymous oracles network. You can read more on this in the next chapter.

5. Decentralized development of RAID network and software, as well as support of established free open-source software.

It’s important to emphasize that RAID development starts decentralized from it’s inception. I have invited Odilitime as a second developer. Two first developers chosen by the community which will join RAID decentralized development each will have fixed 30k of RAID tokens from the treasury, since the very-very inception situation is rather hard to decide upon in truly decentralized way, even RAID strives for it the most. Absolutely anybody can optimistically contribute to the development even before the governance contract is finalized, assuming that after the governance goes live it has a strong incentive not to forget great contributors. Therefore after those two developers with fixed allocations any other developer can join and contribute so much, that the governance can decide to give that developer a bigger allocation than two first developers. All other developers can be hired by the governance when the governance contract will be ready, and they will not have a specific fixed allocation but a salary instead based on the monthly index of RAID to USD or one time grants for contributions. Their salary can vary from $30k to $500k per year, depending on the governance decision evaluating the amount of work and responsibility for a particular developer, and the grants can be of a lesser amount. In it's final form the governance will create verifiable by oracles tasks and find developers to execute them. Emission for developers funds release is very slow, assuming that there are only two developers and they claim their grants immediately as they are released

Many will probably agree that small but dedicated teams can easily turn out to be more efficient, than bloated corporations. The treasury can enable developing free open-source alternatives of any closed source proprietary software. So it will be a lot of small teams up to 5 people maximum maybe. They can create an alternative to Photoshop, Sony Vegas, Google search engine, car driving AI, etc. Including Windows, GPU drivers, any sort of software, including even game engines, we can develop free open source games with all assets being completely free to reuse, which will decrease the cost of game development. If Linux Mint becomes compromised, and it is highly likely as soon as it gets really popular, we can build on top of their legacy and call it Linux Tall Hat, I guess. There are plenty of things not only to bring open-source but also to develop. The fund will also pay (hopefully the most generous) bug bounty and for audits.

RAID software needs special license so that the developers will be unable to move away from free license, a license that can't be changed. It's either the owner of the software is RAID as decentralized entity, or it's a license that can't be changed as defined in the license, but there could be holes in the law.

6. Non-profit social networks like Mastodon and imageboards. Imageboards could need next level popularity, next level mainstream adoption, so that people will ask more and more about what is it about being anonymous? Why is it important? So that they will more likely to value privacy, lean towards spyware-free programs and OS.

7. Anything else that governance will be interested in supporting, as long as functionality for grants and financial support for a particular idea is possible to fulfill in trust minimized way and as long as it is not illegal.

Pseudo-anonymous oracle network

While Raid oracles could provide KYC for simplicity of the design, with Chainlink verifiable random numbers it is possible to allow anonymous and pseudo-anonymous oracles to deliver true results. Oracles shouldn't know what role they are performing in a given iteration of publishing results. There have to be two roles: witnesses and supervisors. Chosen supervisors have to be a small uneven amount of all oracles. Supervisors' results are considered to be true, and witnesses results have to match it. If supervisors' results don't match, majority of identical results of supervisors and witnesses are considered true, and minority results are punished, if there is no clear majority, another attempt of choosing supervisors occurs, until supervisors results match, while published results stay, no republishing occurs during that. If in case of lies we will redistribute a liar stake between "honest" oracles, it creates an incentive to attempt and publish fake results by majority of oracles. Therefore in case of lies, at least 75% of the stake should probably be burned or goes to the funding of default campaigns. An honest oracle can easily miss, say, 3 posts out of 10k posts, depending on the resource, therefore there have to be safe limits for inaccuracy which is not considered a lie. To increase the probability of that the several oracles are definitely not one person, we can use these facts about an anonymous wallet:

1.Balance. Allow anonymous oracles only with considerably high balance, we can even start from whales, top 100 addresses, and if nobody joins, decrease the requirements to top 200 addresses, etc. Higher Raid balances have the least incentive to lie and ruin posters' trust.

2.Transaction history. Democracy Earth Foundation is building tech which attempts to measure unique humanness. Measuring DAO choices could be the best and the only way without specifically asking to provide any other information. We could use their framework or build our own which evaluates the differences in views in different DAO choices, and not just membership of different DAOs.

Raid specifically also can use these variables:

3.Language. Language communities can elect oracles, and the probability of them being one person or collaborating decreases even more. An oracle cluster dedicated to specific job could consist of 20 oracles from different language communities with 3 of them being chosen randomly as supervisors every iteration.

4.Poster history activity and uniqueness. Raid can elect only most active unique non-bot posters as oracles, to decrease the probability of oracles being one person even more.

There will probably be more than one poster database contract and oracles for each of them, oracles cannot include any addresses not registered in their given database as eligible for payout, so oracles can at best censor some addresses collectively or approve all existing addresses transactions even if those transactions are fake. If a poster finds out that oracle cluster he is working with censors him, then he moves to a different oracle cluster, so that censoring oracles lose money and will probably lose reputation in the eyes of posters, since the censorship could be verifiable with most resources. In case of fake rewards, the governance will be able to punish oracles, but only within certain limits, depending on the lies occurred. An independent observer software is required for this. This however is still a pending issue to resolve in a trust minimized way but not from the side of posters and governance, but oracles' point of view, because this solution requires oracles to trust governance to be fair with them. If in case of finding a trust minimized solution to this specific issue will be an impossible challenge, like if adopting a supercheap second layer, Arbitrum for example, somehow becomes not possible, the worst what can happen is that the oracles will need to provide Chainlink KYC, so that the punishment can be reduced. Autistic roll-ups could be required.

Oracles constantly verify posts and keep the data on the amount of verified posts for every address in their databases and publish the rewards data every month to Polygon chain, so they won't need to keep the data longer than a month. Oracles then use privacy oracle solution like Deco, to generate random disposable keys to move the rewards data from Polygon to Ethereum mainnet through trust minimized bridge, so that it will be impossible to alter the data.

Adding oracles between posters and the blockchain is also an option in case of fees being to high for posters to cover expenses of posting. And there are numerous ways of implementing that, we could make it the same way, oracles publish posts in bulk, and a poster sends the data to several oracles(relayers), and if these oracles censor this poster, then he moves to a different oracle cluster, essentially censoring oracles lose money again. We optimistically assume that anonymous oracles will have the least incentive ever to censor anybody.

Trust minimized cross-chain bridge

Commit-reveal scheme disallows oracles to alter transactions, the worst they can do is to censor the transaction, which they are less likely to do, if we use the same oracle system with roles assigned by verifiable random numbers. For the user it could be a bit cumbersome but worth it, since it’s trust minimized. First what he need to do is to announceHash(), Hash has to be generated by the off-chain by the user maybe through a web ui and has to correspond with:

keccak256(abi.encodePacked(userAddress,arg1,arg2,arg3,arg4,anyDisposableKey))

The user keeps all arguments and disposable key to himself, until oracles relay the hash to the other chain, he then must verify if the hash is indeed his, and if it is, then he sends the actual transaction with all argument and used disposable key. The contract on the other chain will only accept address, arguments and a key that matches previously posted hash. If the contract indeed receives correct arguments – oracles are rewarded. This bridge allows not just to cross() or simply relay tokens value, but it also allows to callAcross() - to relay data which enables trustless cross-chain contracts communication. This function will be used by the oracles to relay rewards information from Polygon to Ethereum.

The bridge can support any chain or token. For a particular token oracles will create a wrapper contract, if the token lacks liquidity they have no incentive to deploy another ERC-20, but anybody can just request a bridge and pay money for the deployment. For example wrappers on Ethereum Classic, could use a prefix of lower or upper case “c”.

If the oracles are anonymous or pseudo-anonymous, the risk for value transactions is a possible event when all oracles are being paid by a third party and all of them agree to censor a transaction. The possibility is really low, personally I am optimistically assuming that the reputation costs more than censorship. However, for the case specifically like this, a user can allocate value as a tip to oracles. Which decreases the probability of censorship even more. Without KYC however it could still be a leap of faith for transactions exceeding oracle rewards, so the design could be improved, or the bridge just has to operate with KYC oracles.

Fundamentally pure governance

Malicious governance is common. The way is to simply disallow being malicious as much as possible. In case with RAID it’s not just potential riches of treasury, it is also about being compromised by scammers.

1.First problem is updating contracts maliciously. It seems impossible to me to implement any restrictions on upgrades that the governance can approve. The DAO can override nearly any hardcoded limits. Checking a part of bytecode of next logic implementation in assembly is futile, any variables can be reassigned and overriden.

As far as I went, there is no way to implement any limits in proxy contract except of which we currently have in trust minimized proxy, basically we can only set time limits and locks. If the governance is compromised, it could potentially completely ruin the idea behind the project. So very minimum quorum and a long period of voting is definitely required.

2.Second problem is about managing treasury and is a lot harder to solve. This functionality requires absolutely next level DAO' purity of intentions. What I propose to resolve it is to only allow certain options for governance to decide upon fetched by trustless oracle network. For example, to sponsor open source project and to ensure that it is not a scam to get money from RAID governance, oracles fetch only established projects with certain minimum measurable limits like time since inception. Same could go any other grants governance can approve, oracles can propose only existing established companies or individuals as beneficiaries with verifiable profiles or anyhow transparent and convenient. It can be possible by fetching right information from right resources with right filtering.

So the governance can choose options that oracles propose. And in this particular case all oracles will be capable of reaching 100% accuracy matches in results. At least with proxies they probably will be, or we will have to exclude certain websites. Any grant is not being transferred in one big transaction. Claiming of the grant starts from 0, not truly final, and the DAO can shut it down, if something is wrong. With this governance model it’s also possible for the DAO to create verifiable tasks in many fields. Receiving grants address should not be a contract, so it will be much harder for oracles to transparently cooperate for successful lie.

Creating a balanced voting system is a challenge. Passive income for voters is what creates imbalance, a fair amount of voters just do not vote, they only need passive income, and therefore the outcome of voting participation is impossible to predict.

So what I personally believe in is to lock tokens for at the very least 3 years for voting. And, half of last year of token lock voting is forbidden for a voter, unless he prolongs the lock. I believe currently, that even if Founders and liquidity providers have passive income, it should be accessible with their staked liquidity, however only after a lock, if they choose to lock it(or to elect themselves if you will) – they can use it as a voting power, but if they choose to only have passive income, they don’t need to lock it. A lock should be a sort of sacrifice I believe, it has to be long enough, so nobody will lock and disrupt voting balance just because he maybe could be voting, and so that it won’t be way too long and exhausting for a voter to lose interest in voting. The functionality requires only dedicated voters and the numbers are still being collectively worked on by the community.

With this model we can have a high percentage for minimum quorum. We can have 40-60% instead of 4-10% for a proposal to be executed. The governance model still remains the biggest challenge of RAID architecture and probably requires way more brain power than I will ever have. We need to discuss it and decide upon the best possible model.

ERC-20 allowances can be used to trade locked voting power transparently, and while there is a workaround to solve it rather transparently for RAID token, it is not possible for Uniswap LP token as it is a standard ERC-20 created by the factory. So the system really requires truly decentralized distribution, so one party could not be able to maliciously vote and get away with that easily while creating an imbalance in a given proposal vote. Important to mention that the system does not really critically break if there will be ways to trade votes transparently and even trustlessly.

The most critical voting has to be recorded on Ethereum chain. Voting like meme contest and moderators elections could be run on Ethereum Classic.

Where it is required, voting based on fetched by oracles data can be split in stages:

1.Voting by active human posters without taking into account their stake, we could also use KYC but only for small balances without sense of humor.

2.Proposals approved in the first stage go through voting by stake.

For some proposals there could be even more than 2 stages, more sophisticated, but basically it will be a lot harder to compromise such a system. For example, oracles could just fake the data about nonexistent medical facility which has a lot of wallets, enough for all oracles, so active posters will probably reject that.

Beta-test

Beta-test will launch together with Founding Event and will last for at least 2 months. During the beta-test, depending on Mumbai testnet capability and if RAID and Polygon will be able to reach an agreement, transacting will not require any Matic tokens, in other words will be free. Only one campaign will be available during beta-test: RAID campaign. The compensation for one post will be fixed to 0.001 token per post, instead of index of RAID to USD. Supported websites will be imageboards and Twitter. The posters will be able to claim their beta-test rewards after the Founding Event concludes and trading of RAID token goes live. After the platform hits mainnet, the salary will probably start from 1 cent per post using starting token price as reference as there is no price history yet, and will increase if only the price of RAID token has the room for that and current network scale is ready for more posters. While decentralized moderation might not be ready in time, blatant spam-botting and anything illegal will be still banned and no rewards will be received by that poster address. An extensive review will be conducted before beta-test rewards claiming, so attempting to bot it could be pretty much a waste of time. Since there is no requirement at all to join the beta-test, an option to limit beta-test to only Founders exists.

RAID chain

A wizard proposes the chain to be a fork of Oxen. Oxen by default is an XMR POS fork, therefore RAID chain will have privacy of data by default and ETH daemon for smart contracts. Since it's POS it's possible to significantly increase block size for higher transaction throughput without hurting decentralization. Currently 2 options of rewards incentive mechanism for POS nodes are being explored by the community:

1.Default rewards mechanism. With possible slightly modified EIP-1559 without fee burn.

2. Fixed gas price and fixed rewards for smart contract execution regardless of transaction throughput. The nodes will most likely reject contracts which require high transaction throughput, like dex contracts. And, we optimistically assume that the nodes will approve all RAID contracts because those contracts will allow posters to expand awareness of the chain. With RAID token main utility being marketing, nodes could potentially receive higher rewards as the awareness of the chain increases, so default mechanism might not be required. Basically, the nodes will always disapprove contracts that do not provide any value to them, and transaction prices will always stay low, affordable to posters. With this rewards mechanism or similar the chain could also easily restrict transparent trading of locked voting power, which is could be important for the purity of the governance.

In both cases described above, if a situation of insufficient decentralization occurs, posters can be allowed to run nodes with virtual stake which can eventually be filled with their salaries to make the chain decentralized in no time. Virtual stake nodes after accumulating at least some balance could help validate plenty of 0 value transactions.

Secondary projects

Secondary projects will yield no rewards to RAID participants, these projects will aim to increase overall blockchain community awareness of RAID network. If some of these projects require governance it could be RAID governance in some cases, and in most cases autonomous governance specifically dedicated to that project.

Risks

You acknowledge and agree that there are numerous risks associated with purchasing RAID Token, holding RAID Token, and using RAID Token for participation in the RAID Network. In the worst scenario, this could lead to the loss of all or part of the RAID Token which had been purchased. IF YOU DECIDE TO PURCHASE RAID Token, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THE FOLLOWING RISKS:

Uncertain Regulations and Enforcement Actions : The regulatory status of RAID Token and distributed ledger technology is unclear or unsettled in many jurisdictions. The regulation of virtual currencies has become a primary target of regulation in all major countries in the world. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including RAID Token and/or the RAID Network. Regulatory actions could negatively impact RAID Token and/or the RAID Network in various ways. RAID may cease functioning in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction. For the token sale, the sale strategy may be constantly adjusted in order to avoid relevant legal risks as much as possible.

Inadequate disclosure of information : As at the date hereof, the RAID Network is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this white paper contains the most current information relating to the RAID Network, it is not absolutely complete and may still be adjusted and updated by the RAID Network Development team from time to time. The RAID Development team has no ability and obligation to keep holders of RAID Token informed of every detail (including development progress and expected milestones) regarding the project to develop the RAID Network, hence insufficient information disclosure is inevitable and reasonable.

Competitors : Various types of decentralised applications are emerging at a rapid rate, and the industry is increasingly competitive. It is possible that alternative networks could be established that utilise the same or similar code and protocol underlying RAID Token and/or the RAID Network and attempt to re-create similar facilities. The RAID Network may be required to compete with these alternative networks, which could negatively impact RAID Token and/or the RAID Network.

Failure to develop : There is the risk that the development of the RAID Network will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or RAID Token, unforeseen technical difficulties, and shortage of development funds for activities.

Security weaknesses : Hackers or other malicious groups or organisations may attempt to interfere with RAID Token and/or the RAID Network in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of RAID development team may intentionally or unintentionally introduce weaknesses into the core infrastructure of RAID Token and/or the RAID Network, which could negatively affect RAID Token and/or the RAID Network. Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to RAID Token and/or the RAID Network by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

Other risks : In addition, the potential risks briefly mentioned above are not exhaustive and there are many other risks associated with your purchase, holding and use of RAID Token, including those that the risks that RAID development team cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the RAID Development team, as well as understand the overall framework, mission and vision for the RAID Network prior to purchasing RAID Token.

Notice: RAID does not tolerate any illegal activity. Personal attacks is the biggest problem currently legally. And we have find a way to conveniently and legally resolve it.

RAID is aims not to be a security as much as possible in every way.