



Polytimos - Whitepaper

(The Very Precious Store of Value.)

Polytimos is the people's project. It aims to gain support and popularity through 99% word-of-mouth 'advertising'. Providing useful services to the community that will also assist the market value of the project, allowing its users to attain a feeling of becoming part of a Bitcoin type project at the beginning. Not only this, but also implementing totally open source applications and services for use of its community in not only creating a retirement account for themselves or a savings account for their family, but also making use of the tech and services of Polytimos to increase their security online, send money to anyone in the world in seconds, and overall increase their productivity within the realm of technology. The project is called 'very precious' for a reason. It aims to bring projects and services to the people of the community, connect other crypto communities together via assisting them with projects, and create a spirit of camaraderie and technological advancement. With natural growth of the community, market, and price of the project therein, anyone can get involved and make the same as anyone else. A spirit not only of decentralization and co-operation, but of fairness for everyone.

Introduction to Cryptocurrency and Its Existing Concepts.

History

Bitcoin was an idea launched in 2009 by an anonymous developer with the moniker 'Satoshi Nakamoto'. He had the idea to implement a worldwide trustless payments system that could run completely without central control.

The whitepaper was released, and a few people became very interested. Over the years the system was developed further, more and more developers, and users came to the currency. Before long, the thousands that were used on the first pizza purchase, were worth many millions of dollars.

This shows that the people of the world, are not only interested, but are in need of a system such as this. The system is one that allows the people to retain FULL CONTROL over their own finances.

As the blockchain idea advanced, more and more practical applications were developed using the blockchain tech as the foundation. It has been realized that blockchain technology can attain many other goals than simply a currency.

It is the belief of the Polytimos team, that the whole future of the tech space, will be built on one form or another of blockchain technology. Thus, they have created a platform that will be used for many other purposes, while at the same time retaining the 'store of value' nature that Bitcoin is so famous for.

Alternative Blockchain Applications

As mentioned in history section above, as blockchain technology progressed, it became more and more apparent to all involved that the tech was not just something for monetary services. People realized that the underlying foundation of Bitcoin and other blockchain projects, could be built upon with other types of services.

Polytimos aims to not only build these services for its own project platform, but build and assist other projects in completion of their own. Then, to work closely with these others to gain cooperation and advantage over projects with bad intentions (which unfortunately are abundant in the cryptocurrency space.)

Polytimos aims to build physical devices, useful blockchain based platforms, and services that make use of its 'coin' to give use cases. One of the main 'theories' of the creating team of Polytimos, is that of the unnecessary nature of the 'road map' and the fact that announcing a project in this particular space before it is complete, is in essence a lie as it is very likely that things will change in the fast-paced industry, before the service is able to be launched, and thus, the mentioning of the service to the community ahead of time becomes a lie.

Polytimos will never announce anything that isn't for sure able to be completed, and will generally do so only upon actual completion of the said service.

Philosophy of Polytimos

(View the full Polytimos philosophy paper here -

https://docs.google.com/document/d/1v7rBjWkuXAm_pYdF15Y0YJ5F_JkASJDchJWgfBaFso/edit?usp=sharing)

The philosophy of the creating team of Polytimos, is that of fairness, cooperation, and advancement of the crypto space, in the 'bitcoin fundamentalist' manner. What this means, is the project should not only be accessible to anyone, but anyone should have the same amount of opportunity as anyone else to attain coin, use services, and access available features of the project.

The project aims to be a very tight knit community of people with similar goals and underlying ideals. Honesty, integrity, and fairness should be the three priority concepts in the minds of people in the Polytimos community. There is no room for attacks on community members, or anything but kindness and open mindedness within the core.

To work together to obtain a larger goal, should be the goal of most cryptocurrency projects, however, unfortunately we have seen a lot of the opposite in the years since the creation of Bitcoin. Many teams seem to be of the mindset of the old 'corporate structure' where there are constant attacks on competing projects, and overall too much competition in a negative fashion. In order to attain the end goals of true decentralized economy, services, and finances for the world, the Polytimos team believes that we all in the space with good ideas and ideals, must work together to attain the overall much larger goal of replacing the antiquated system that currently runs most of our world.

We believe it is possible, and not only that but likely, given the above criteria are met, for the blockchain space to replace many of the 'traditional' systems within many areas of existing society. From finances, to stock markets, to the internet entirely, internet of things, AI, and much much more can all be built on blockchain based platforms that allow for vastly increased security, easier implementation, redundancy, and availability to the entire world.

Polytimos, when no longer in its infancy and at a stable point, will dedicate itself to the foundation of multiple non-profit organizations for outreach in multiple countries, both bringing blockchain technology to them, and providing them with devices to use that tech, ways to keep finances coming up, and food/water, and other necessary life resources.

We believe there are too many people who do not think about the well being of the world, and that more people should do this.

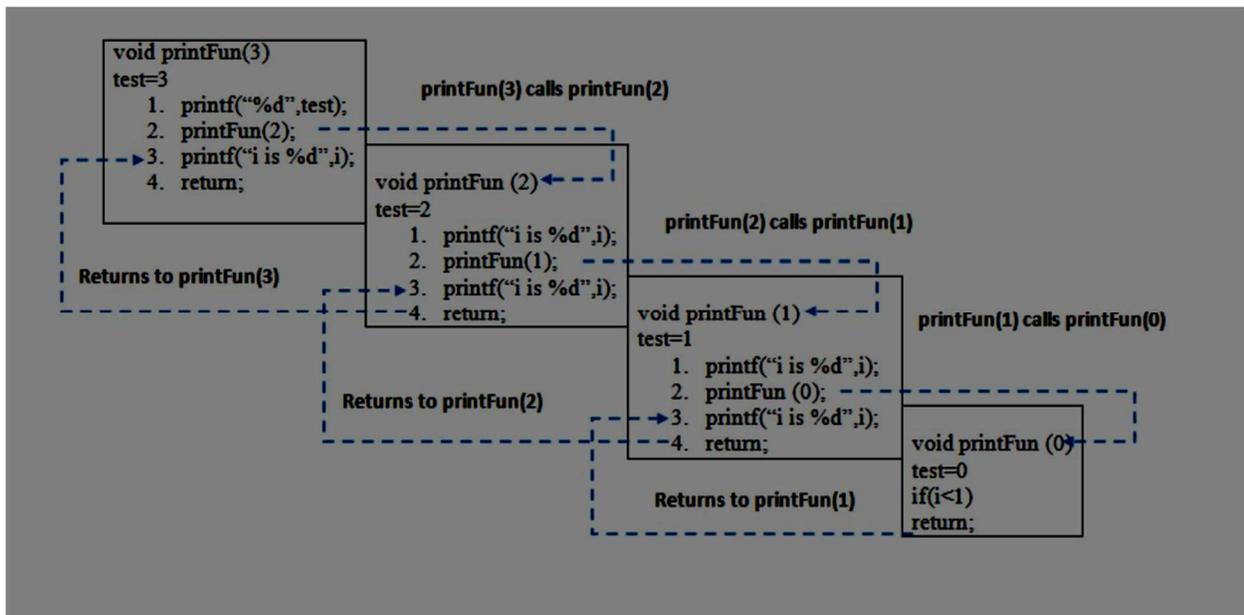
Within the expanded team of Polytimos, are influential persons inside the blockchain space, operating other projects, running useful services in and outside of Polytimos, and building some very revolutionary blockchain based architecture. Polytimos team hopes to work closely with these projects, providing both assistance and cooperation with them and attaining a further technological advancement as the effect.

Partnerships with the team of the QORA project, pools, and service providers will allow Polytimos to be part of what these various teams are building, as well as with QORA, being part of what the team believes could be the future of the internet itself. These are goals that the QORA team hopes to realize in the next 6-12 months with the creation of its Gen 2 platform. Gen 1 already does decentralized web hosting and blogs, and much more. Polytimos hopes to work together with the QORA team in any way possible, and help use its network and services in combination with Polytimos to provide people around the world with a secure, long-lasting store of value on top of a truly decentralized internet. This is only one of the for sure future plans of Polytimos.

Polytimos hopes to become the main location for anyone looking to be part of a great blockchain community, to come, build services, offer their skills for payment, and just become a group that is helpful to each other and can all build accounts to support their families without the need of reliance upon a centralized entity. This is the future, and the future is bright if these ideals are able to be met.

Polytimos State Transition Function & Algorithm

Polytimos has a new hybrid algorithm called “Polytimos” . It is a complex algorithm that uses refined recursion. Recursion in computer science is a method where the solution to a problem depends on solutions to smaller instances of the same problem (as opposed to iteration).The approach can be applied to many types of problems, and recursion is one of the central ideas of applied computer scientific calculations. The Polytimos algorithm supports recursion by allowing a function to call itself within function's code.



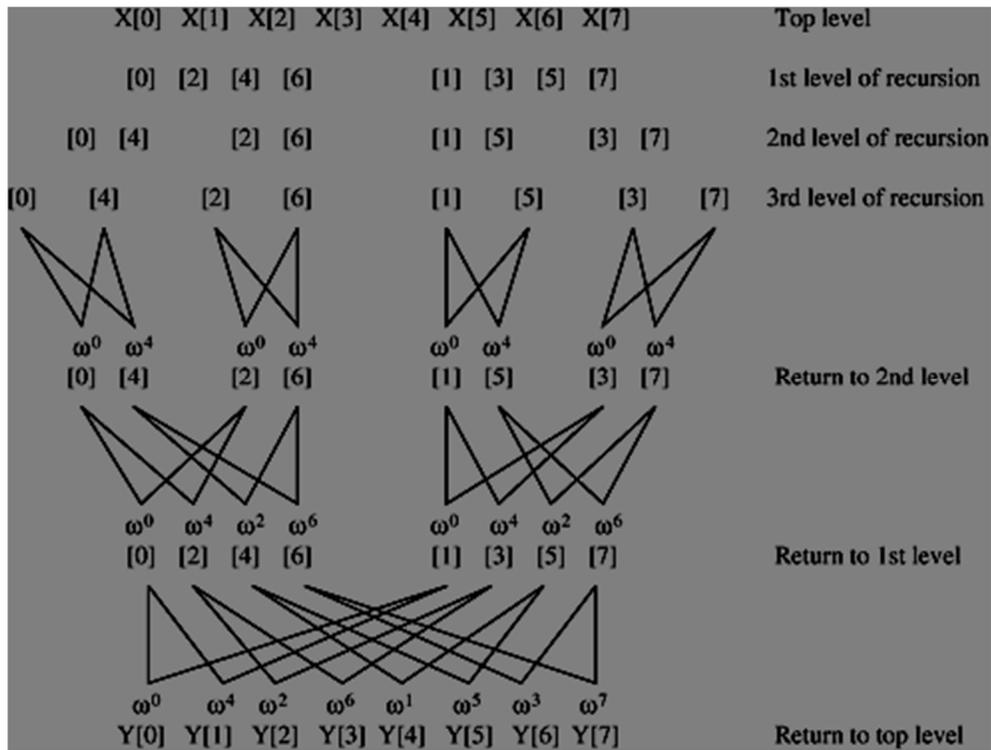
A general procedure for a simple hybrid recursive algorithm is short-circuiting the base case, also known as arm's-length recursion. In this case whether the next step will result in the base case is checked before the function call, avoiding an unnecessary function call. For example, in a tree, rather than recursion to a child node and then checking if it is null, checking null before recursing. This is useful for efficiency when the algorithm usually encounters the base case many times, as in many tree algorithms, but is otherwise considered intensive, particularly in academia, due to the added complexity.

```

function recursive(n)
    if n==base
        return xbase
    else
        return f(n, recursive(n-1))

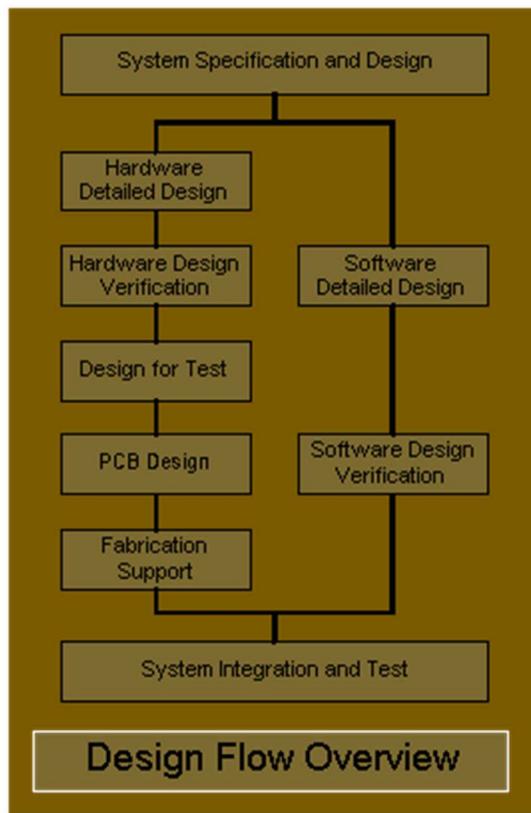
```

Polytimos hybrid algorithm uses a combination of skein, shabal, echo, luffa, fugue and gost. They are proven algorithms as of date and use merge sort, heap sort and integer factorization. The development of a single algorithm from the base level takes tremendous amount of time and constant research. The quickest solution to create a hybrid algorithm is to have a merge and sort coupled with integer factorization in objective C language. Creating a hybrid algorithm such as Polytimos saves the time required for rapid prototyping and beats heavily funded organizations involved in complex computational and scientific research.



The time required to solve a Polytimos block may vary for same input because it depends upon the compute power and memory available during the execution of block solution cycle. It all comes down to how the compute engine processes the Polytimos algorithm with efficient memory management. New generation of GPUs with added instruction sets yield better hash rates as compared to single run design engines. The vendor specific PCB design also plays an important role to assist in high bandwidth results in-return providing faster hash function solving. For example, the nVidia's GP104 based GPU engine uses 3D stacked memory resulting in 4x higher memory bandwidth.

Since Polytimos algorithm relies more on memory and has no ASIC friendly parallel pipelined functions, the long term algorithm is ASIC resistant with the current ASIC machines available in the market. However, a specially designed ASIC hardware with algorithm requirements fulfilled can be custom built to mine Polytimos. The long term evolution of Polytimos Proof of Work stage gives the investors and miners the ability to raise funding for future ASIC machine development and prototyping. Due to the flexibility and openness of readily available SoC and FPGA designs, a proof of concept ASIC miner is a possibility only in future.



A multi GPU OpenCL based system gives better hash solving power at the same time demands more memory to solve a single Polytimos block. In a real world scenario, an AMD based 7990 with Malta chip gives better hash solving on a generic solo algorithm but when faced with a Polytimos hybrid algorithm the resulting hash solving power is poor as compared to the Polaris based chips. The reason being 3GB of memory on Malta GPU compared with upto 8 GB on Polaris. Now if nVidia's Pascal GPU with stacked memory and parallel pipeline engine is used to solve Polytimos, the result is upto 75% better without any tweaking required.

AMD 7990 Dual Malta GPU, 3GB	2.8 Mh / sec
AMD RX 480 Polaris GPU, 8GB	13 Mh / sec
nVidia 1080ti Pascal GPU, 11GB	40 Mh / sec

Code Execution & Mining Phase

Polytimos was launched in what is referred to as 'truly fair'. To keep in line with the above ideals. What this means, is that the blockchain of Polytimos was launched to the community at 'genesis' or block 0.

With this, its hope was to give everyone in the crypto community the same chance at becoming a significant holder of the coin. While at the same time implementing a theory that launching in this manner is the superior way to implement a cryptocurrency into the wild.

The launch went exceptionally well, being started on CPU only mining, with the release of a community-developed GPU miner without charge to the community within a day of the launch. This is exactly what the Polytimos community is supposed to be. A single community dev building something that he then shared with the entire community allowing the project to continue on in its fair manner.

In the future, the Polytimos team looks to develop a set of physical devices for mining of the currency. Known as 'ASIC' devices, these allow mining quicker than GPU with less power consumption. The development of small USB type ASIC devices by the team, hopes to ensure the decentralization of the network, allowing anyone with any computer to plug in this USB device and secure the Polytimos network attaining the block rewards as well as the fees from the use of the coin.

If done correctly, we believe that the ASIC devices could also be used in poverty laden areas and help to provide means for income for low income families, and communities in 3rd world countries.

The mining phase of Polytimos will last 10+ years while creation of new coins is in process, then last forever after that based on the usage of the network and miners attaining the fees from said use.

Polytimos is going to forever use PoW mining, similar to Bitcoin, however, it will also implement what is referred to as Proof-Of-Stake or POS at block 800,000. This will allow anyone with any device and a few coins, to gain a solid 8% on their coins. You can think of this as basically an 'interest rate' similar to that which (used to be?) given by central banks, however done in a way that is provably fair, and given to everyone exactly the same.

PoW/PoS Hybrid Mining

In order to remain as fair as possible, Polytimos implements POW mining to start the release of the coins to the world, however, once the block number 800,000 hits, polytimos then becomes what is referred to as 'hybrid' which means not only can someone attain coins by hashing the polytimos algorithm and supporting the network in that fashion, they may also do so by simply holding coins in their wallet and enabling 'staking'.

Staking also allows blocks to be transacted on the network, however does so without the need for constant power in the form of CPU or GPU (now) or ASIC (eventually) running constantly.

One may simply put the coins in their wallet, and make use of the POS algorithm to secure the chain and at the same time give them an 8% gain on their coins. This also allows for any device to run the network, makes the network more decentralized due to many nodes running all over the world without needing big hashpower, and allows for people to be part of the network by simply running their own wallet and getting

their own 8% increase.

The hope is to become a very strong ‘savings account’ type system, with the services of the community and team backing the project, providing transactions for the network, and enhancing the overall value of the project. Everyone can then grow together in value and see the effect of the ideals of Polytimos being put to work.

Desired applications

Polytimos looks to build many services with which the coin can be used. The first of those, is already running. The first service is called PolyShield, and it currently provides a system of hosted and shared MasterNodes which is in the process of being automated. This system not only provides a way for people to get into a MasterNode without having all the necessary funds, but also provides a solid backing for the Polytimos market by way of 25-100% of each MasterNode the service runs, being used to purchase Polytimos on the market.

This will end up becoming a self-support mechanism for the coin price on the market, volume, and overall stability in price and support.

With working together with other projects, Polytimos hopes to find the best teams providing the most useful services, and work with them to make Polytimos used in their platforms on top of building its own with hopes the teams working together will use them as well. This spirit of working together for the greater goal, we believe will attract many like-minded individuals in the space to work with Polytimos in attaining the larger end result that many people in the blockchain space are looking for.

Further Applications

In the future, Polytimos looks to be a value addition in many fashions to new and existing blockchain platforms. To become the ‘savings account’ of many projects.

Also, the creation of services to assist in the areas of the world that really need the help. Third world countries, poverty areas, etc. Helping these people is a big goal of the Polytimos project. Thus living up to its name in the hearts of those of us not lucky enough to be born in the more wealthy of areas.

Helping people, is something Polytimos really believes in.

The building of small devices that could not only provide the ability for people to make money, but also give them further internet security, and potentially even drastically reduced internet costs via mesh networking and advanced technologies built into the networks of QORA and Polytimos, is something that is definitely in the mind of the Polytimos team.

Consider the invention of something that would allow a community to share multiple internet connections, make money by supporting the network that runs the ability, and host websites to connect their skills to

people looking for them, all at the same time! Things like this are surely being planned for the future of the Polytimos project as well as QORA and their team. The first real partnership of Polytimos and QORA has yet to be officially announced, but is continuing to be discussed between the two teams and will be announced once a combination of the two can be realized within a shared project.

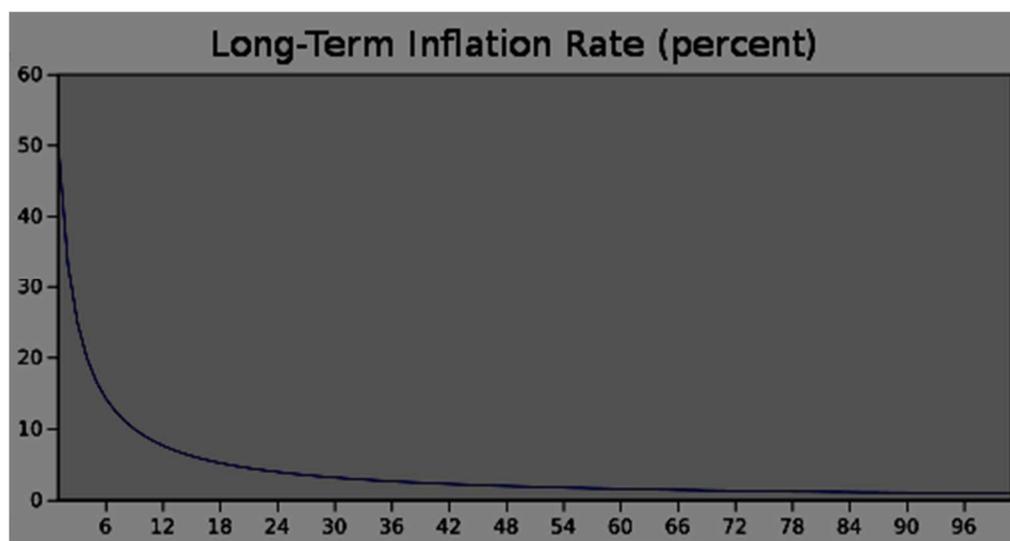
Miscellanea And Concerns

Fees

Unlike the Bitcoin fee structure, the Polytimos fee is static at 0.0001 Polytimos per transaction. A Proof of Work block takes a step ahead with blockchain movement without any fee incremental structure. There is no particular selection method by a miner to include an "X" number of transactions in a current mined block. If a block size reaches maximum transaction size (bytes) structure, the proceeding transaction is automatically added in the next block avoiding any transaction confirmations. The same fee and confirmation mechanism applies to the PoS stage in future.

Computation

Currency And Issuance



Mining Centralization

The fear of mining centralization is always a concern in a blockchain project. The fear of what is referred to as a '51% attack' is always in the back of the mind of teams developing cryptocurrencies. However, with the hybrid mining of the Polytimos network, combined with the newly developed algorithm, the fact that this algorithm cannot be rented on the big services like Nicehash, and the fact that nearly anyone can use any device once POS mining starts... we believe that the concern of centralization is far lower within Polytimos.

This is not to say that it is impossible to have a single group attain large enough power to cause issues during the POW only mining... so, to combat this, the team is working on the development of small USB ASIC miners for the Polytimos algo. These will allow for people all over the world to run them without the need for large powered operations, thus keeping the power far more decentralized.

Also, the support of the pool <https://cryptopool.party> allows for another pool to mine on that is never going to have any malicious intent. This keeps the power from being put on a single or couple large pools, and also since the team running the pool is working closely with Polytimos and has the same ideals, keeps the worry of the pool suddenly becoming malicious and attacking the network, to a 0% chance. Making the network stronger while in the POW phase.

Once hybrid mining starts, the worry of 51% is drastically reduced, due to not only another method of block generation, but also the fact that attaining 51% of both methods becomes much more difficult and expensive.

Decentralization is always the highest priority for the Polytimos team, so much so that they would eventually like to see a community so strong in Polytimos, that they could even step back completely, and have no worry at all that anything negative will happen to the network, and that community developers will pick up where the team left off. This is not to say that the team plans to step back at all, in fact quite the opposite, as there are many future plans which require the team and their expertise and connections to help further the project. They have every intention of completing these required actions, and making Polytimos into the very precious project they know it is.

Scalability

Simplified payment verification - SPV

It's possible to build a Bitcoin implementation that does not verify everything, but instead relies on either connecting to a trusted node, or puts its faith in high difficulty as a proxy for proof of validity. BitcoinJ was an implementation of this mode.

In Simplified Payment Verification (SPV) mode, named after the section of Satoshi's paper that describes it, clients connect to an arbitrary full node and download only the block headers. They verify the chain headers connect together correctly and that the difficulty is high enough. They then request transactions matching particular patterns from the remote node (ie, payments to your addresses), which provides copies of those transactions along with a Merkle branch linking them to the block in which they appeared. This exploits the Merkle tree structure to allow proof of inclusion without needing the full contents of the block.

As a further optimization, block headers that are buried sufficiently deep can be thrown away after some time **(eg. you only really need to store as low as 2016 headers)**.

The level of difficulty required to obtain confidence the remote node is not feeding you fictional transactions depends on your threat model. If you are connecting to a node that is known to be reliable, the difficulty doesn't matter. If you want to pick a random node, the cost for an attacker to mine a block sequence containing a bogus transaction should be higher than the value to be obtained by defrauding you. By changing how deeply buried the block must be, you can trade off confirmation time vs cost of an attack.

Programs implementing this approach can have fixed storage/network overhead in the null case of no usage, and resource usage proportional to received/sent transactions.

Conclusion

We hope to have given everyone a solid idea of the foundation of Polytimos project, and hopefully some ambition to come together with the community and help create something magnificent together. We believe wholeheartedly that community projects are the REAL future of the Open Source World. Come get involved with us and let us begin to make our own futures together!