MERIT

A vision for the new economy

Whitepaper by Adil Wali and Maxim Khailo

September 1, 2017

ABSTRACT

With only one in every two-thousand people in the world having an active cryptocurrency wallet, the entire ecosystem faces a critical problem: real-world usage. While blockchain lays the foundation to powerful decentralized solutions to technical and business problems, the current state-of-usability leaves a lot to be desired. Until this usability gap is closed, the space will continue to be ruled only by financial speculators and forward-looking technologists.

As is the case with any new technology, the long-term efficacy, success, and value of cryptocurrencies will be driven by their future adoption. Despite the deep importance of this problem, innovation in the space largely ignores usability. Instead, most new currencies focus their efforts on either anonymity or programmability. Both of which generally increase the barrier to everyday user adoption.

When examined through this practical lens, the skyrocketing market capitalization of cryptocurrencies in recent months raises an important question:

IF THE USER BASE OF CRYPTOCURRENCY CONTINUES TO BE LESS THAN 1% OF THE WORLD'S POPULATION, IS CRYPTOCURRENCY APPROPRIATELY PRICED?

Merit is a new cryptocurrency that is purpose-built to be used daily by technical and non-technical users alike. Merit believes that a truly human-centered cryptocurrency must be built on three pillars: safety, simplicity, and community. Each of Merit's innovative features is driven by one of these core principles.

Unlike other cryptocurrencies that focus on obfuscation and anonymity, Merit puts community first. Merit is the *world's first invite-only blockchain,* and introduces *proof-of-growth (PoG)* mining, which rewards ambassadors for growing the community. Further, Merit adds easy-to-use aliases to the blockchain that make it effortless for users to send and receive Merit to one another.

Simplicity has a multiplicative effect on community. Merit introduces *GlobalSend,* which is the world's first frictionless escrow on the blockchain. It allows any Merit user to send MRT to any recipient, without having to first know if they are on the Merit network. The recipient can simply create a wallet and claim the MRT in the escrow. The *GlobalSend* protocol goes further to make transactions cancellable and password-protected.

Finally, as it pertains to safety, Merit adds powerful human-centered security features to the blockchain. The most significant of which is the creation of decentralized vaults on the blockchain. Vaults feature two keys: one for spending and one for resetting. They also empower users to create whitelists and rate-limits, which serve to protect users even in the case that their vault is hacked.

TABLE OF CONTENTS

MISSION

To be *the world's most used cryptocurrency* by creating a truly safe, secure, and easy-to-use means by which businesses, families, and individuals can store, transfer, and grow their wealth.

THE METEORIC GROWTH OF CRYPTOCURRENCIES

Since the inception of Bitcoin in 2009, cryptocurrencies have seen astronomical growth as speculative investments. The current combined market capitalization of all cryptocurrencies is nearing $400B, and many believe that this is only the beginning.

There is not a simple *silver bullet* that is driving such adoption of cryptocurrency, but instead a cadre of reasons. The top reasons include:

- ✓ Lack of trust in banks and traditional financial investment institutions.
- ✓ Lack of faith in nations and central banks.
- ✓ Dropping value of many nations' currencies.
- ✓ An increasingly global economy, driven by virtual teams and companies.
- ✓ Fraudulent behavior by corporations and banks.
- ✓ Corrupt behavior by governments.
- ✓ Oppressive tax regimes.

Cryptocurrencies, like fiat currencies, are only as strong as the belief behind them. Instead of a belief in a specific government or central bank, the belief behind cryptocurrencies is in the network of nodes and users and the underpinning cryptographic technologies that ensure the integrity of the system.

THE CHALLENGES IN CRYPTO TODAY

While the inventions of the blockchain and cryptocurrencies as a category are quite significant, *global adoption* is still quite limited. Given that there is around $86.6 trillion in money worldwide[1], cryptocurrencies, even at $400b in aggregate, account for only 46 basis points of the world's money supply.

Further, while the total number of global cryptocurrency holders is difficult to know for certain, a high-quality Cambridge Study estimates it to be between 2.9 and 5.8 million users[2]. This would mean that as few as 1 in every 2607 people is an active cryptocurrency user.

What's potentially worse is that the shape of the top cryptocurrency holdings is almost entirely slanted toward the elite. The top 10% of bitcoin wallets account for 99.41% of total bitcoins in circulation[3]. A full 89.42% of all bitcoins in circulation are held by the top 0.79% of wallets.

[1] https://howmuch.net/articles/worlds-money-in-perspective

[2] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[3] https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

When less than 1% of all bitcoin holders account for nearly 90% of all bitcoins in circulation, it is not difficult to imagine a world where the entire value of the currency collapses because of the decisions of a special few. This centralization is particularly alarming when it is examined alongside the already low adoption of cryptocurrency.

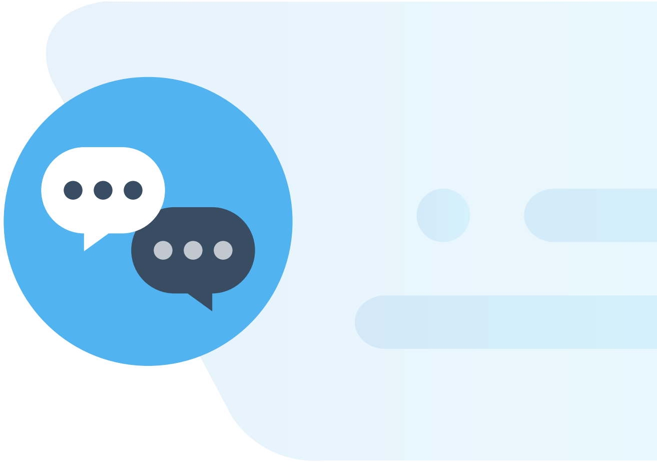
THIS IS, OF COURSE, PARTICULARLY IRONIC BECAUSE IT COMPLETELY OPPOSES BITCOIN'S ORIGINAL VISION OF A DECENTRALIZED CURRENCY FOR ALL

This dichotomy between the number of cryptocurrency holders and the total growth in market capitalization is particularly important because it yields insight to the shape of the problem. Clearly, there is a small group of passionate core users, who represent disproportionate wealth, that have flocked to these cryptocurrencies. The question is: why have the broader masses not yet followed this early adopting group?

While this centralization is concerning, it is perhaps not the most significant problem facing cryptocurrencies today. Any currency, digital or otherwise, is only as useful as it is spendable. Looking past the speculation (eg. buy and hold) use case, the primary focus of any currency is to be used to exchange value. From a consumer perspective, two theoretically well-suited use cases for this kind of spending are *peer-to-peer* and *retail* spending. Both of these use cases are currently held back by the very low adoption of cryptocurrencies today. Merit believes that this lack of broad worldwide adoption is the single biggest challenge facing cryptocurrency today. *This is the problem that Merit is focused on solving.*

We believe that the three primary challenges standing in the way of further adoption are: *incentives, safety, and ease-of-use.*

INCENTIVES: THE CRITICAL SUCCESS FACTOR OF A WINNING ECONOMY



The fundamental underpinning of economic systems are the incentives that drive them. As stated earlier, our core premise is that the primary opportunity for cryptocurrency today is to drive worldwide adoption. So, the operative question is:

WHAT IS THE INCENTIVE FOR USERS TO DRIVE FURTHER ADOPTION IN CRYPTOCURRENCIES?

At the face of it, there may be some answers to this question that are obvious to the technical and financial elite, but not to the rest of us. Let's examine each of them in turn, and understand how they well they stand up in practice instead of theory.

Cryptocurrencies are a great way to send money to friends, family, and colleagues. The primary value of a new currency should, in theory, be to allow people to conveniently send and receive wealth. Yet, we've seen above in the commentary on usability and safety that cryptocurrencies are not actually the best candidates to send money in this way. There are already a number of significantly more convenient and practical mechanisms by which money can be sent to others. These alternatives benefit from a much larger user base, the convenience of identity, and in some cases, the ability to send money to people who may not even be part of the network/community.

Cryptocurrencies are a great way to buy things online. Another primary value of a currency is to be able to transact, of course. Yet, again, we have not seen this borne out in practice. There are a small number of online destinations that actually accept crypto payments. This is further evidenced by the notion that there are entire marketplaces/destinations that have positioned themselves as destinations for spending your cryptocurrency. There, of course, would be no such business opportunity if cryptocurrencies successfully penetrated the broader online economy and the sites that we already shop. It is important to note here that the use of cryptocurrencies does not empower a shopper to access products or services that are unique. The only potential exceptions being illegal purchases such as drugs or firearms, and our belief is that these are not net positives, and we do not validate them as a use case.

Cryptocurrencies are a great way to grow one's wealth. So far, the primary empirical benefit of cryptocurrencies to the community-at-large is that *people want them,* which has dramatically driven up their price, and created astronomical ROI for early investors. In this way, speculative investment is the most validated practical use of cryptocurrencies. Yet, currencies are not designed to be investment instruments. They are used for transacting and transferring wealth, not increasing it. So, we're left with an important question: who, other than the technical and financial elite, would have seen or posited that cryptocurrencies were an instrument for investment and ROI? And, should the growth of wealth be one of the marketed benefits of these currencies?

This final answer, related to growing one's wealth, is the most empirically supported, but also the most non-obvious. Bringing this back to the notion of incentives, we might finally see our first glimmer of incentives to grow the network. Since cryptocurrencies are not backed by physical assets such as gold or the power of a nation's military might, the primary driver of price is simply a function of *belief,* and thereby, demand for purchasing it. So, it stands to reasons that early users of any currency might have an incentive to tell others about that currency, to drive the price up and potentially grow their wealth.

While this incentive to spread the word certainly exists, at best, it is indirect. Users do not see any direct benefit from driving adoption in the network. Given the very high volatility of these currencies, and broader market externalities, it's hard to imagine a single user actually being able to 'move the currency' by telling all their friends.

Our conclusion is that these prospective answers to the incentive question are relatively hollow. There are easier way to transfer money to friends and transact online. And the primary investment motivation, now or in the past, would have been the belief in a stateless currency. Leaving us with no direct incentive for users to actually get their networks to utilize these currencies as part of their daily lives.

SAFETY: THE PRACTICAL GAP BETWEEN SECURITY AND USABILITY

There is a palpable difference between the notion of security and safety, and we use the term *safety* very deliberately here. It is true that the underlying blockchain technology behind most cryptocurrencies is secure inasmuch as the probability of it being hacked is very low and decreases even further as adoption increases. Yet, this secure core technology is limited in scope to only securing the decentralized ledger of which transactions were completed and in which order.

While the ledger of transactions itself is difficult to fraudulently manipulate, there are a number of important practical *safety* gaps that exist in the ecosystem. First, as there is no notion of identity in these systems, there is the practical question of ensuring the money was properly transferred to the intended recipient. Further, there is no notion of trust, ratings, or reviews in any of these systems.

AS SUCH, USERS DO NOT EVEN KNOW IF THE ANONYMOUS NODE THAT THEY ARE TRANSFERRING MONEY TO IS TRUSTED BY OTHER USERS IN THE SYSTEM

This is not to mention that there is no recourse for users who have been defrauded or suffered from a simple case of human error.

It is also worth noting that these cryptocurrencies are actually bearer currencies[4], meaning that she who holds them, owns them. This results in great risk in the event of lost or stolen computers. There is no way to recover stolen accounts or information. And there is no mechanism of account recovery in the case of loss. So, the best-practice in the industry is to copy this private key store it safely in an offline device, known as "cold storage." This is materially worse than the state-of-the-art associated with most modern centralized banks, where such an event can easily be remedied with identity verification and subsequent account recovery.

Most cryptocurrency protocols are built with only one mechanism of authentication. This is less secure than the multi-factor authentication that we have come to expect with basic applications such as email and social media. Further, there is no ability to recover lost credentials. There is not so much as a simple password reset feature. This is a very significant shortcoming that presents great practical risk in a world where human error is a well-understood reality, yet is completely ignored by these decentralized technologies.

Another practical missing link in cryptocurrency today is that there are no limits or failsafes imposed by any crypto protocols today. This means that, in the case of breach, bad actors can instantly transfer all stolen funds out of the system at any time. This lays is in stark contrast with most modern banks that impose daily, weekly, or monthly transaction/withdrawal limits. These limits provide the very practical layer of security in that they can stem the tide of stolen funds in the case of breach.

[4] https://en.wikipedia.org/wiki/Bearer_instrument

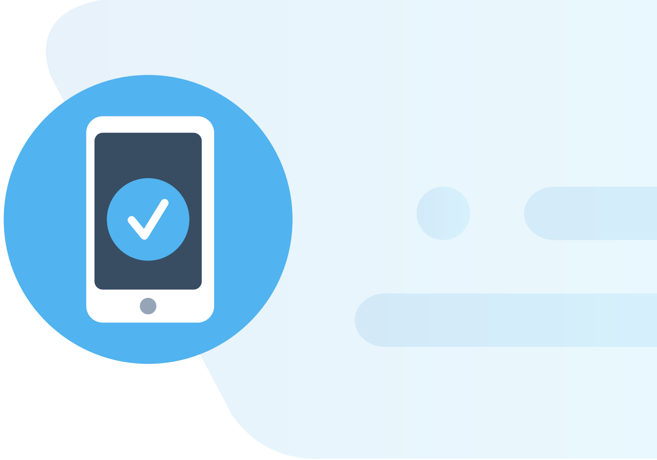
Finally, there is no recourse for bad actors in these systems. Given the anonymous-first approach that cryptocurrencies take, they make it difficult (if not impossible) to identify any bad actors. Some currencies go even further to purposefully obfuscated transaction trails (through zero-knowledge proofs, shielded addresses, or otherwise) to ensure that there is no way to 'follow the money' after it's stolen. That's not to mention that each individual node in these systems treats all other nodes the same way, irrespective that node's history of potentially illicit behavior.

So, while the promise of security in a trustless peer-to-peer system creates inherent security in theory, the *safety in practice* is actually deeply compromised. There have been a significant number of major thefts both in Ethereum and Bitcoin. The numbers are striking, with the largest being the Mt. Gox theft being $436M[5]. We've seen $79M stolen from the DAO, causing a fork in the entire ethereum blockchain[6], and a spin-off currency as a result. This is not to mention the more *casual thefts* like the $30m (to-date) stolen by the 2-line software bug in Parity.

[5] https://en.wikipedia.org/wiki/Mt._Gox

[6] https://www.bloomberg.com/features/2017-the-ether-thief/

EASE-OF-USE: THE DRIVER OF MAJOR WORLDWIDE TECHNOLOGY ADOPTION



Any student of technology, history, and entrepreneurship is likely to take note of how important ease-of-use is to adoption of new technologies. Our modern world is full of examples of easier-to-use approaches that took the world by storm, from NetFlix to the iPhone. Cryptocurrencies today stand in stark contrast to this modern world of easy-to-use applications, devices, and tools.

The day-to-day use of cryptocurrencies involves installing complex software that requires significant hard-drive space and CPU power. That's not to mention that there is a complex array of wallets, miners, and other tools for users to pick from. The setup instructions on these pieces of software varies in complexity and required technical expertise.

Further, the day-to-day realities of running this software is not often made readily apparent to a new non-technical users. There are important details one must understand, such as:

✓ A computer needs to be left on and not in power-save mode for full nodes to operate.

✓ A connected mining computer will generate significantly higher electricity bills.

✓ There is no ability to reset password or recover an account, so tactics like cold-storage should be used.

✓ Users should read about complicated governance measures managed by the community and cast their vote on hard and soft forks.

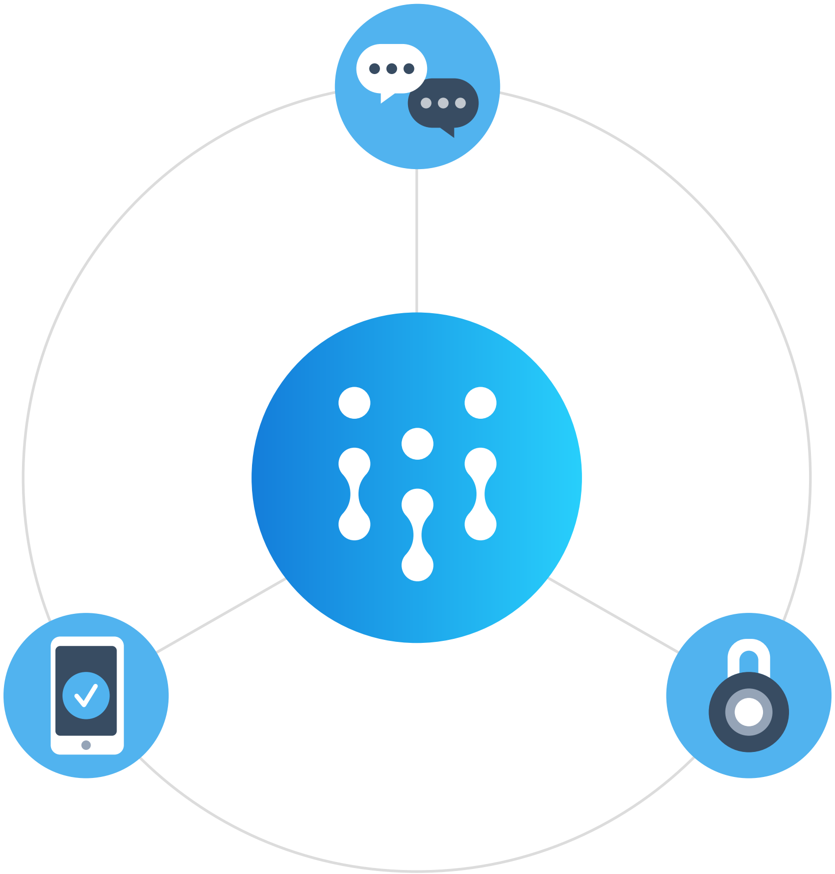
The above *fine print* is important, especially for non-technical users, to understand. But, of course, simply being informed is not enough. Of course, one must possess the knowledge, skills, and experience to actually utilize these complex tools in an effective way. These facts, of course, create an inconvenient or impractical reality for all but the most technical of us.

Let’s assume for a moment that a non-technical user is able to get over the considerable technical hurdles of adoption. The next question we are left with is, how can they use this currency on a practical day-to-day basis? To send money to another user, we must first know their public key, which is a string of 34 characters (ex: 14xEPWuH-C3ybPMfv8iTZZ29UCLTUSoJ8HL). Of course, obtaining this cryptic string requires an extra inconvenient step on the part of both users.

There is no easy way to send money via the forms of contact that we may already have about someone, such as their email address, Twitter alias, or their phone number. It’s worth noting that there is no explicit confirmation step when sending money via cryptocurrencies. Meaning, if we accidentally mis-type one of many characters of the address, we will potentially send money to the wrong person without recourse. Relative to the many convenient centralized ways that we can send money to friends today, the answer to this question leaves quite a bit to be desired.

MERIT: WORKING TO SOLVE THE MOST IMPORTANT PROBLEMS IN CRYPTO

For cryptocurrencies to flourish and become significant on the worldwide scale of money, *we need a better state of the art.* That state of the art needs to address the three biggest obstacles standing in the way of worldwide adoption of cryptocurrencies are *incentives, safety, and ease-of-use.* We've set out to do just that, and in this paper, we introduce Merit, *a currency designed from the ground-up to drive worldwide adoption.*



INCENTIVES: MERIT STAYS TRUE TO A DECENTRALIZED AND COMMUNITY-FOCUSED ETHOS

Incentives are the most important part of any economic system. The creation of a new currency is no exception. Historically, cryptocurrencies have not necessarily advanced the user experience enough to get major adoption as a way to send money or to buy things online. We can think of these potential values of the currency as *unrealized potential.* We cannot discount that the primary empirical value of cryptocurrencies has been the ROI to early investors. This ROI potential has certainly been *realized.*

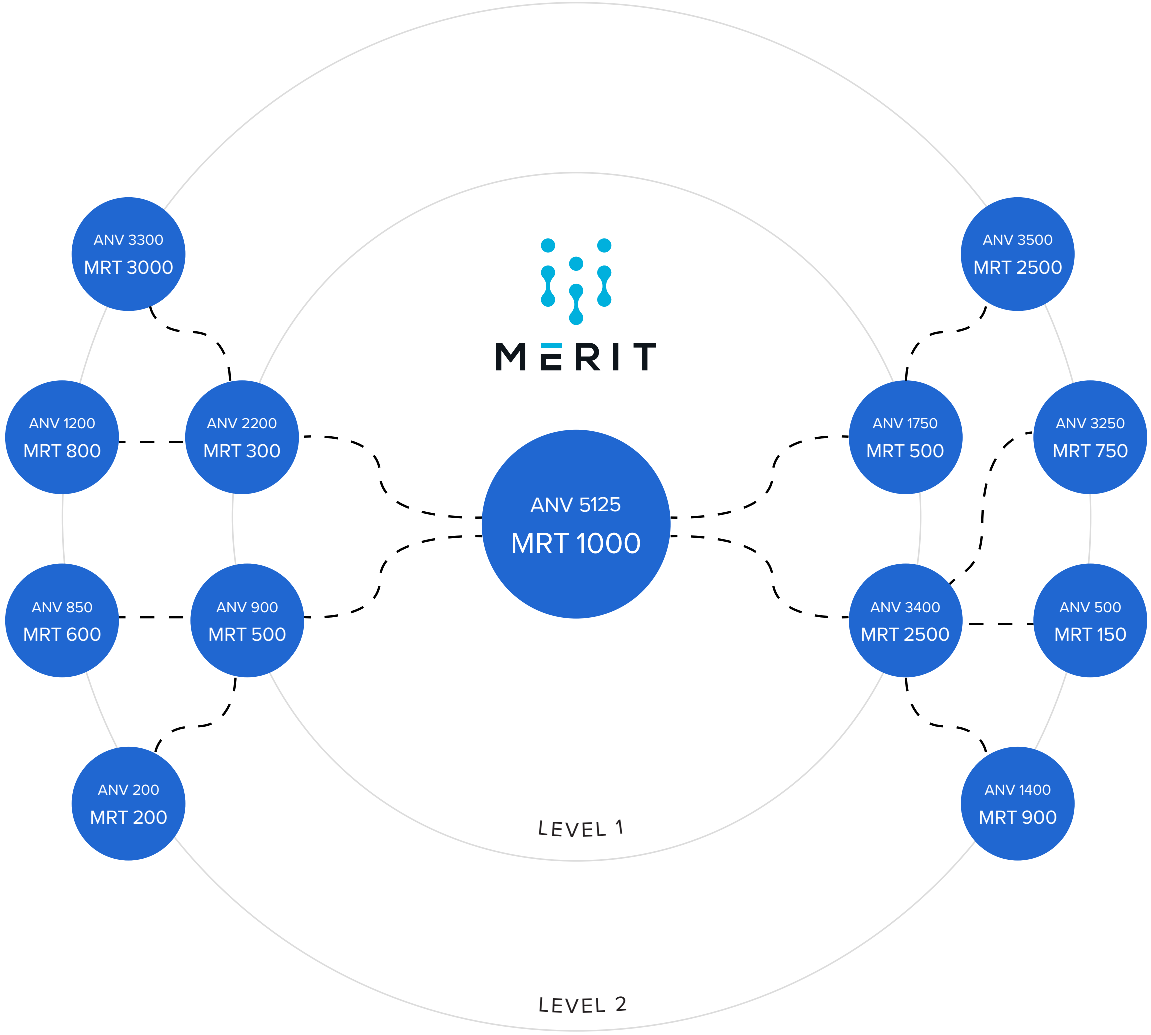
Merit's enhancements in security and ease-of-use can go a long way to making this currency part of our everyday life. And, if we succeed there, we will have *realized the potential* of cryptocurrency from a day-to-day use standpoint. Yet, our vision does not stop there. We believe that robust incentives can even further realize the potential of ROI for early currency holders.

Interestingly enough, both the empirical value of cryptocurrencies and the unrealized potential of any currency are primarily driven by one key factor: *the network effect.* The more people that hold a currency, the easier it is to integrate that currency into our daily lives. The more people that demand a currency that is not rife with inflation, the higher the value of this currency will be on a per-unit basis. As such, the primary incentive in the system should be encourage growth in the total number of currency users and total investment into the currency. Merit's revolutionary *proof-of-growth* mining approach does precisely this.

Other cryptocurrencies incentivize users to make major investments in hardware and data centers to drive *proof-of-work (PoW).* This incentive, while helping to keep the network secure, does nothing to drive further adoption of the currency. The primary alternative to this approach is *proof-of-stake (PoS).* This approach does, in fact, encourage people to invest into the currency and keep their money inside of their crypto wallet. Yet, it does not encourage growth in the network, and it has lingering security concerns that do not exist in PoW.

Merit creates an incentive structure that actually incentivizes users to spread the word and drive worldwide adoption, and also to also be an active currency-holding member of the network. All the while, our approach maintains security in the protocol. We do this through the combination of *proof-of-growth (PoG)* and *proof-of-work (PoW).*

The *proof-of-growth* approach keeps track of the referral forest for for the whole system. We can zoom into the case of an individual user below:



The large bottom number in each circle is the total amount of USD-equivalent Merit in each wallet. The *aggregate network value (ANV)* is listed in the upper line of each circle. As we can see above, user in the centre of the scheme has $1000 worth of Merit in her account, and an ANV of $17,400. The ANV of any user can be computed by computing the ANV of their direct referrals into the network (labeled at Level 1 above.) The levels of referral is always expressed relatively to the user in question. For example, the inner circle users are level 1 referrals for the center user. The ANV for any user is computed 10 levels deep to ensure that the earliest users in the system are not forever advantaged in the system.

To ensure the system is fair, balanced, and built for longevity, we introduce the notion of *Aggregate Age of Network Value (AANV).* AANV tracks the ANV of any particularly user over time, and it is averaged over the course of the previous 30 days. The Merit system uses AANV to determine how many Merit are awarded as part of minting a new block in the system. This is contrast to using it to determine *which users* get to mint new blocks, which would be similar to how PoS systems manage minting blocks. We do this to eliminate the risk of the *nothing-at-stake* problem.

This novel approach is powerful for a variety of reasons. First and foremost, it does not promote the centralized notion of wealth that PoS and PoW systems do. In a PoW system, users with the highest hash power are rewarded. The wealth required to maintain significant hash power scales proportionately with the size of the network. And, of course, we've seen that there are entire data centers built for only this purpose today. PoS is an even more directly-linked incentive to wealth, where she who has the highest "stake" has the highest likelihood of mining the next block. Merit, in contrast, measures the aggregate impact that a user has on the growth of the network. This minting potential is not reserved for the financial elite. Any user can drive significant growth in network, irrespective of their current socioeconomic status.

Further, we view this measurement as a much purer gauge of positive impact on the Merit economy. Whereas in PoW, as the number of total nodes in the network increases, the relative impact of each additional normal (eg. a PC) node drops. This is not the case with PoG. Irrespective of the size of the Merit network, additional growth continues to be meaningful. And, the relative growth impact of each user is measured in a meritocratic way against other users in the system. This approach is not only fundamentally fair, it incentivizes the one behavior that matters above all others in the system: growing the network effect.

SAFETY: HOW MERIT COLLIDES THEORY WITH PRACTICE

Our belief is that practical safety is one of the most significant barriers to adoption in cryptocurrency, especially since they are bearer currencies. Users must have the peace-of-mind that they have come to expect with their current alternatives, such as credit cards or modern banking.

Merit does by attacking some of the largest safety problems facing cryptocurrencies. Let’s examine each one in turn.

- ✓ Fraud – Merit works to ensure that fraudulent transactions are easier to avoid, disincentivized in the system, and that losses are minimized.
- ✓ Bearer Currency – Merit works to ensure that accounts are covered with multiple layers of protection, and that they are recoverable in the case of loss or theft.
- ✓ Theft – Merit works to ensure that accounts are covered with additional layers of protection, making theft harder. Further, Merit works to limit losses even in the case of theft.
- ✓ Ledger Hacking – A blockchain is only as strong as its network strength, and a Sybil attack is always a risk. Merit addresses this with more powerful incentives, and additional layers of intelligence among nodes working against the chain.
- ✓ Burning Currency – By virtue of its invite-only blockchain, Merit cannot be destroyed by mis-typing the address of the recipient.

Merit addresses the above challenges by introducing four powerful and novel notions to our underlying blockchain technology.

- ✓ A limited address space – Merit's invite-only ecosystem requires all users to be vetted by existing members of the community, making it dramatically harder for bad actors to enter the network in the first place.
- ✓ Vaults – Merit ensures that users are protected in both a practical and secure way.
  - Whitelists – Merit vaults employ whitelists to ensure that users are protected even if their vault is breached.
  - Rate Limiting – A powerful progressive rate limiting system built directly into the vault protocol.
- ✓ Trust – We introduce the notion of a trust score that helps users make day-to-day decisions about who to transact with inside the network.
- ✓ Account Recovery – In the case of lost/stolen account credentials, accounts can be recovered in a totally decentralized way.

One of the largest challenges in the cryptocurrency world today is that bad actors have unfettered access to these decentralized networks. A hacker, thief, or scam-artist can generate millions of bitcoin addresses and easily attempt to scam millions of users. In contrast, the Merit blockchain is regulated by the stewardship of the invite-only system. Invite tokens, and thereby addresses, are scarce in the Merit community. They must be mined over time. To activate one million addresses on the Merit network, a bad actor would have to mine a million invites, which would could take years to do.

This stewardship-focused protocol has other distinct advantages as it pertains to security. Because the blockchain keeps an immutable record of invitation activity, the source of bad actors can be traced to their inviter. Further, if a bad actor was to attempt to create a fraudulent community in the Merit ecosystem (by inviting a series of addresses, for example), it is dramatically easier for good actors on the system to identify the this entire *bad actor tree* and ignore or block it.

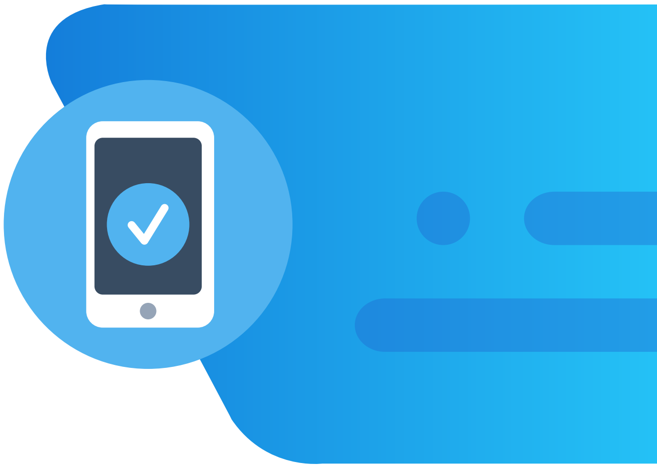
The classic challenge with existing layers of security and safety on the blockchain is that most of them rely on centralization to protect users. This is because existing protocols lack the primitives to manage security effectively on their own. Merit works to innovate in terms of protecting users in a way that stays true to the principles of decentralization.

The instant and anonymous nature of transactions in cryptocurrency merits the need for trust in the system. While we need not necessarily know with whom we are transacting, it is deeply beneficial to understand if the person or organization we are transacting with has positively or negatively interacted with others in the system. As such, Merit builds a Trust Score into the protocol that allows users to understand the reputation of who they are transacting with. The trust score takes into account a myriad of factors, including: number of transactions, age of account, aggregate coin age, verified identities, and positive/negative ratings from others in the network.

While Merit builds additional layers of safety into the protocol, we do not assume that the network is immune to wrongdoing. As an additional practical layer of protection and recourse, we introduce the notion of Progressive Rate Limiting into the protocol. This rate limiting applies to all users in the system, and varies based on the Trust Score of an account. We can illustrate this notion with an example.

Let us say, for example, there is a 10,000 MRT theft on the Merit network. With a classic cryptocurrency protocol, the thief would be able to simply transfer the 10,000 MRT to their wallet and then immediately out of the system through one or many other wallets. Whereas, on the Merit network, the rate limiting feature of vaults would empower a user to prevent this scenario from occuring. If a Vault was set up with a rate-limit of 100 MRT per day, then the owner of the Vault would see the one unauthorized transaction for 100 MRT occured, and can proceed to reset the vault. In this scenario, the thief would have only been able to transfer 100 MRT out of the Vault instead of the total 10,000.

EASE-OF-USE: MERIT MAKES REVOLUTIONARY TECHNOLOGY ACCESSIBLE TO EVERYDAY USERS



Merit not only works to be the safest cryptocurrency available, it also aims to be the most user-friendly and practical choice for day-to-day users. We accomplish this in a variety of ways. First, we empower users to utilize lightwallets that enable all the features of the network. Users need not install complex software and keep it running day-in and day-out to utilize the benefits of the system. Next, we allow Merit users so easily send and receive money based on the current forms of contact and communication they have today. Finally, we empower users to understand the level-of-trust of the users and organizations they are interacting with, so that they can make informed decisions.

As mentioned above, the non-expert user can have significant trouble with installing complex software that requires significant compute resources. Instead of forcing all users to install ‘full-nodes’ in the network, Merit utilizes a two-tier architecture, including a secure lightwallet server that enables light weight wallets that can be run on mobile devices or desktops without significant resource utilization. This secure lightwallet server never holds the private keys of users. It only acts as a layer of convenience. With Merit, lightwallets are able to fully transact on the network in the same way that full nodes are. Not only can lightwallets be fully run on mobile devices, they can also be run with a lightweight footprint inside of the browser. Merit plans to launch a lightweight web lightwallet in the Lazarus release in 2018.

Merit's identity protocol not only promotes security and safety, it makes the system significantly more friendly and practical to use. Perhaps most importantly, these identity features put cryptocurrency on par with the convenience and ease of the many popular centralized alternatives, such as Venmo or Paypal.

Let's illustrate with an example: Merit users A, B, and C have had dinner together and are splitting the bill. Merit *User A* has validated their phone number, and anonymously attached it to their wallet using multiple identity providers. Merit *User B,* who does not have a validated phone number and does not know that *User A* has a Merit wallet, can simply pull out their mobile phone and send money to this phone number with the peace-of-mind that *User A* will receive it. Let's assume that *Potential Merit User C* does not have a Merit wallet yet. *Merit User B* can still send money to the phone number of *Potential Merit User C,* and *Merit User C* can simply access that money as soon as they have validated their phone number with a wallet. And, of course, this example could use any validatable identity such as Twitter, FaceBook, SnapChat, or even email address.

While the identity protocol powerfully creates decentralized peace-of-mind and safety, it is fully optional. Understanding that not every user is going to validate identity via the protocol, we still need a practical way to do business with anonymous users. The Trust Score mechanism providers powerful functionality in this case. Before transacting with another user, a Merit user is able to query that Wallet's trust score, to determine if they'd like to do business with that user. Of course, in the usual course of business, we are often presented with multiple vendors of a certain type. Having this trust score empowers us to choose with whom we want to do business. Further, we are granted the peace-of-mind of knowing that our own trust score will increase as we engage in more successful transactions with other users.

Merit's roadmap takes the Trust Score concept even further. The Kingdom release aims to utilize a sidechain for actual reviews to accompany ratings. This way that users can make an even more educated decision before choosing to interact or do business with another member of the community. And, of course, this usability and practical value is what we've come to expect with the popular centralized commerce sites and networks that we use daily.

Finally, Merit builds the native notion of referring other users into the protocol. This makes it easy for members of the community to spread the word to their friends, colleagues, and family. Further, it extends the 'splitting dinner' example above. User B, in sending money to User C through the use of a convenient form of contact that is already stored in her phone, has effectively referred User C to the system. And the Merit protocol keeps track of this referral, which serves to strengthen the security of the system, enhance the integrity of the Trust Score, and provide better incentives in the system.

THE PAST, PRESENT AND FUTURE OF MERIT

Merit believes fundamentally in decentralization. In the same way that the blockchain provides resilience over a centralized system, a truly global organization is more resilient than a single-state one. As such, Merit Labs exists as an entity in two different jurisdictions: Singapore, and the United states. We believe that this robust approach empowers Merit with the longevity and stability to truly shape the future of commerce.

The Merit Foundation is headquartered in Seattle, Washington. Merit Labs Ptd. Ltd. is headquartered in Singapore. The Merit team includes members in the US, Canada, Ukraine, Russia, and Colombia.

Merit's Genesis release is planned for December 31, 2017. For more information about the Merit release schedule refer to the Merit Roadmap.

To learn more about the Merit protocol, refer to the Merit Bluepaper.