ARMR

PRIVATE FROM THE GROUND UP,
DESIGNED AROUND SECURITY AND ANONYMITY.

WHITEPAPER

REVISION 0.5
PUBLISHED APRIL 2018

CONTENTS

INTRODUCTION

In a world where online privacy is becoming increasingly important, digital commerce doesn‘t get its fair share of the spotlight.

As we find it a very basic human right to have privacy, we don’t want anyone to be able to break that privacy. It therefore stands to reason that entrusting our financial information to banks and credit card companies leaves us exposed. At ARMR we feel that your financial transactions should be even more protected than your browsing habits, and we are putting our money where our proverbial mouth is.

Our network protects one of your most valuable assets; freedom to purchase and buy without leaving a trace. We know it is possible to have fast, reliable, truly anonymous transactions, and we are here to do just that.

ARMR is a privacy-centric cryptocurrency that implements Stealth Proof of Stake (SPoS) and utilizes the TOR protocol. It is natively integrated within the TOR network ensuring anonymity by concealing the wallet node identity and their digital footprint from surveillance and traffic analysis which is achieved by separating identification and routing. It is an implementation of onion routing, that encrypts and then randomly bounces communications through a network of relays around the globe.

Driven by a primary purpose of protecting an individual’s identity and privacy online, we know we must go the extra mile by creating an anonymous, secure, scalable, instantaneous and untraceable payment platform.

ARMR promotes privacy and anonymity by default for cryptocurrency users by significantly reducing the likelihood of identification by third parties through the incorporation of industry-leading cryptographic standards, backed by proprietary algorithms and anonymity-centric networking protocols.

We employ state of the art technologies, such as Stealth Staking and Chainmail Transactions to obfuscate transactions, making it impossible to trace coin movement across the ARMR network. This provides a secure, anonymous platform, operating over a secure, anonymous network in which users can transfer their wealth, free from observation and scrutiny.

COIN TECHNICAL SPECS

Ticker	ARMR
Announcement date	May, 2018
Consensus method	Stealth Proof-of-Stake (POS 3.0 with Stealth)
Block Size	1.5 MB, around 3,000 transactions per block
Hash Algorithm	POSV3
Circulating Supply	26 million, and 14 million locked in dev/marketing/staffing funds
Max supply	40 million, 100% pre-mined
Block time	60 seconds Difficulty retarget each block
Confirmations per transaction	5
Staking Interest	5% P.A.
Confirmations per minted block	50
Minimum holding time before PoS generation	24 hours
Block Reward	~2 ARMR
Maturity	110 Blocks
Min Stake Age	8 hours
Initial Distribution	Airfork
Connection port: 16560	**RPC Port:** 17570
Average ICO Price	None, as there was no ICO
Accepted Currencies	None, as there was no ICO
Technology	Ring Signatures for Anonymous Transactions · Default Stealth Addresses · Stealth Staking · Zero Knowledge Proofs · Full Decentralization

FUTURE ROADMAP

OUR PLANS FOR PRODUCT DEVELOPMENT AND ENHANCEMENTS.

Q2 2018

- ARMR Wallet (Windows, MAC, Linux)
- Stealth Staking
- Default Stealth Mode
- TOR+OBFS4 with Ring Signatures
- Better Sync Performance
- Encrypted Transactional Messaging

Q3-Q4 2018

- Chainmail Transactions
- Blacksmithing
- Master Blacksmith (Masternodes)
- Exchange Integration
- BISQ TOR Decentralized
- Payment API
- 2FA Protection

2019 AND ONWARD

- ARMR Repairs
- ARMR Transactional Protection
- Username Association
- Android App Dev.
- Ecosystem Expansion
- BTC/ETH Wallet Integration
- Gamble Mixer
- Single-use Wallet
- Web Wallet Interface
- Apple iOS App
- Hardware Wallet
- QR Authenticator
- Peer-to-Peer
- Virtual Credit Card Integration

Version 1.0 www.ARMR.network Technical and business factors can make the roadmap change at any point.

PHASE I

Phase 1 consists of security fundamentals which will form the core of ARMR and will be available at launch. These are the very basics for securing and anonymizing transactions on the ARMR network.

STEALTH TRANSACTIONS

It is essential to have complete anonymity from the start, therefore all ARMR transactions will use “stealth” by default. A combination of ring signatures and stealth addresses prevents anyone but the transacting parties from knowing details of a transaction, this is not an optional feature as implemented in other cryptocurrencies.

RING SIGNATURES
(PROTECTS A SENDER‘S WALLET ADDRESS)

Each outgoing transaction is signed by a randomly pooled group of users (including the actual sender), making the transaction look like it could have come from any of the pool members (both the pool size and pool members are randomized for each transaction). The identity of the specific sender is therefore kept anonymous. The transaction authenticity can still be computationally validated but the wallet ID of the sender remains unknown.

A one-time spend key that corresponds with an output being sent from the sender’s wallet is used, making each transaction cryptographically unique.

As an example; if ‘Alice’ sends 500 ARMR to ‘Bob’, there will be no way to be sure that the input came from Alice‘s wallet address as opposed to several other addresses in the pool that might have generated the same signed input. In the event proof is needed, Alice‘s wallet can verify that the ARMR was sent using the one-time spend key.

STEALTH ADDRESSES
(PROTECTS A RECEIVER‘S WALLET ADDRESS)

For each incoming transaction, a one-time public key is generated and recorded as a part of a transaction (corresponding to the one-time private spend key from the sender) to indicate who can spend ARMR in a subsequent transaction instead of associating the receiver’s wallet address in the output that is visible within the blockchain. This prevents outputs from being associated with a wallet address, meaning anyone looking at the block chain could not identify if funds are moving from one wallet to another and could therefore not link wallet addresses.

Example: When ‘Bob’ receives 500 ARMR from ‘Alice’, the output will not be associated with Bob‘s wallet address and in the event proof is needed, Bob‘s wallet can verify that the ARMR was received from Alice.

STEALTH STAKING

To complement ring signatures and stealth addresses, we have implemented “anonymous mining” through Stealth Proof of Stake (SPoS). Staking is done using stealth addresses in such a way that by simply having your wallet address and going through the ledger, no one can tell how much you have staked or how much you have earned as a result. This way the privacy and anonymity of all involved parties (sender, receiver, and miner) are protected.

TOR+OBFS4+MEEK

All transactions use the TOR network, with miners forming secure nodes and as always with TOR, your IP address remains hidden, regardless of whether you are mining, sending, or receiving.

OBSF4 and MEEK bridges makes it possible to use ARMR in countries where TOR is blocked.

TRANSACTIONAL MESSAGING

Transactional Messaging is peer-to-peer (or end to end) encrypted messaging between transacting parties, with the messages only existing in plaintext within the sender & receiver wallets and encrypted elsewhere.

Transactional Messaging allows users to verify, amend, negotiate transactions, and interact safely & securely with one another.

BETTER SYNC PERFORMANCE

With asynchronous syncing, wallet syncing is improved and resource management becomes more efficient. Wallets intelligently optimize available resources to achieve optimum sync performance.

PAYMENT REQUEST

If you know someone's wallet address, you can send them a payment request without leaving your wallet.

PHASE II

Phase 2 will improve upon the core features of ARMR. The following features compartmentalizes and obfuscates the ledger in ways that make it impossible to obtain any useful data from the block chain itself.

CHAINMAIL TRANSACTIONS (MIXER)

Our way of making our transactions even harder to trace, by having transactions interlinked across multiple wallets and broken down into micro-transactions.

Suppose an attacker (or just someone who is interfering or trying to find information) tried to trace a transaction by identifying the amount of ARMR that 'Alice' sent to 'Bob'. Enter "Chainmail System", where the transaction value is broken down into random separate amounts (Say 25 micro-transactions which in this case will all add up to a final sum of 500 ARMR) and each micro-transaction (of varying, randomized amounts) appears to have happened at a different time.

Each of the micro-transactions will be passed through a different wallet address and leave a would-be attacker unable to track a specific transaction. The entire 500 ARMR however, would instantly be available to the receiver.

BLACKSMITHING

To make mixing possible, wallet holders may choose to keep their wallets running and enable the “Blacksmithing Protocol”. This will allow the Chainmail system to covertly route transactions through their wallets, thus fortifying ARMR’s anonymity and security. The more ARMR in a wallet, the more the user can help anonymize transactions on the network.

Blacksmithing-enabled wallets will receive a percentage of the transaction costs routed through them. The percentages will be increased the longer a Blacksmithing-enabled wallet remains active. The final step on this ladder is the Master Blacksmith (or Master Node).

Should the number of transactions on the network be reduced, ARMR guaranties no less than 3% of wallet holdings per year. By Blacksmithing for a significant period of time users may receive an additional 5% per year as a bonus for helping secure the network.

MASTER BLACKSMITHING

We wanted to offer our users the ability to be Master Blacksmiths, without having to invest X amount of their hard earned money. To become a Master Blacksmith (or a Master Node) you simply need to meet certain criteria. That criteria is based on trust. We wanted to allow more people to become Master Blacksmiths because the more “Smiths” we have the stronger and more secure the network, therefore there is no minimum amount of coins required, but instead is based on how long your wallet has been staking and how many transactions your wallet has helped to process. Users will be given a trust-rating based on their time as a Blacksmith and the number of transactions processed through the wallet. If a wallet is taken offline or fewer transactions are processed the rating will decay and “Master Blacksmith” status may also decay.

Master Blacksmiths will earn a massive 35% of the transaction costs, possibly increasing to 45% over time, this is capped at a maximum of 8% of total ARMR held in the wallet per year. To reward our Master Blacksmiths further we will also have an exclusive reward that will be revealed in our next whitepaper version.

MASTER BLACKSMITH GUILD

Master Blacksmiths, as above, are wallets who have been online, staking and helping to secure the network. After being a Master Blacksmith continuously for 6 months, you will join the Master Blacksmith Guild. Guild members have “earned a stake” in ARMR and will therefore have voting rights for the forward movement and future of ARMR, based on the roadmap and development teams ideas etc.

BLACKLISTING

An option for users to block suspicious or malicious wallet addresses to prevent abuse and/or fraud. Blacklisting is done on a “per user” basis and is carried out from the “client side”. This is for users own security and is a block on a user’s wallet client not a block of a wallet on the block chain itself.

PHASE III – 2019 AND ONWARD

ARMR REPAIRS

We also want to reward users who spend their ARMR, not just those who stake and hold their coins. Each transaction initiated on the network will have a small part of the fee go to an "ARMR Repair Pool" transaction fees paid out will go towards "ARMR Repair Tickets", tickets will increase in price from ticket #1 to #2 etc., tickets are only valid on the day they are rewarded. At the end of each day one lucky random Ticket Holder will receive the collected fees from the ARMR repair pool.

TRANSACTIONAL PROTECTION (ESCROW)

'Alice' wants to conduct a transaction with 'Bob'. Alice sends ARMR to Bob and Bob delivers proof of services rendered or goods dispatched to Alice via the encrypted messaging system. After Alice receives the goods or service, they tick the transaction as received in their wallet and Bob receives the sent ARMR. In effect, the transaction between Alice and Bob is placed in escrow until both parties agree that all terms of their agreement have been satisfied.

To ensure this system is not abused there will be a Mutually Assured Destruction (MAD) approach implemented. If both users confirm payment sent/goods received etc then the coins are released and the trust ratings of both users would increase. If either user does not confirm receipt of goods / payment sent then the Escrowed coins would not be released and would be destroyed, neither party would receive the coins or a refund. Both users trust rating would be negatively affected.

Higher trust ratings will result in lower fees for the Escrow Service and more users willing to deal with higher-trusted users, whereas a lower trust rating would increase fees/costs and likely reduce the number of users willing to deal with lower trusted users.

The higher the percentage of escrow defaulted payments in a given wallet, the higher the transaction costs would be, i.e. if you have 10000 escrow transactions, but only 10 marked as defaults, your transaction fees will be much lower than someone with 5 escrow default payments, but with only 10 escrow payments total.

Another deterrent for abusing this system is that a user's trust rating will affect a wallet owners ability to Blacksmith and Master Blacksmith on the network. If a user/wallet reaches a critical rate of 50% escrow payment defaults (lower trust rating), the wallet owner will no longer receive rewards from Blacksmithing. In order for this to not only impact the transactional cost of the sender, receivers will also have a minimal transaction fee. The more escrow payment defaults, the higher this will be.

BISQ TOR DECENTRALIZED

We will be adding the decentralized possibility to trade our coin through BISQ.

PAYMENT API

An API with R.E.S.T. based architecture which can be integrated for receiving payments to a business for goods and services. Compatible with many services currently offered and easily integrated into an existing payment system (Point of Sale Systems or E-Commerce).

RECURRING PAYMENTS

The opportunity to send or receive payments on a regular, pre-defined interval i.e. daily, weekly or monthly basis. Recurring payments are transactions from one user to another, which repeat over a fixed interval as stipulated by both parties. Setup and use of such subscription-like transactional services will be via an easy to use interface.

HARDWARE WALLET

Hardware wallet for cold-storage integration.

QR AUTHENTICATOR

Two-step verification for enhanced security connected to your wallet to ensure YOU are in charge of YOUR funds.

BTC/ETH WALLET INTEGRATION

Bitcoin and Ethereum wallet integration so you can store Bitcoin, Ether and ARMR all in one place.

SINGLE-USE WALLET

For additional security you can generate a single-use wallet to receive funds. Once funds are received the wallet disappears never to be traced again.

PEER TO PEER

Users can “trust” other wallets to enable instant transactions between them. Payments are still directed through the Chainmail system and remain fully anonymous.

USERNAME ASSOCIATION

Users can create usernames at their own discretion, not only allowing others to more easily send payment, but also for easier access to the ARMR web-interface.

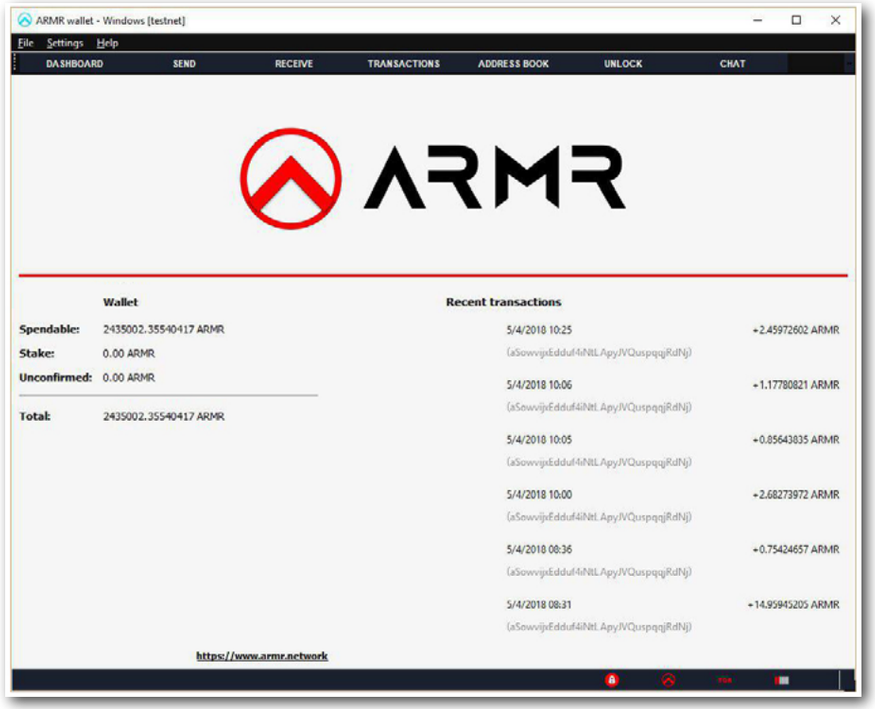
WEB WALLET INTERFACE

Allows users to access their wallets using a mobile of desktop browser, only available if users have enabled 2FA.

VIRTUAL CREDIT CARD INTEGRATION

The ability for users to generate virtual credit cards which allow transactions from their ARMR wallet in FIAT currencies, while remaining anonymous. The virtual credit card will be linked to the balance of the associated wallet.

WALLETS



Windows Wallet Alpha Preview

LINUX

LINUX WALLET ADDRESS

MAC OSX

MAC OSX WALLET ADDRESS

WINDOWS

WINDOWS WALLET ADDRESS

Our latest wallets can always be found on our website:

https://armr.network/#wallets

THE TEAM

ANONYMITY GOES BOTH WAYS

We have decided, for now, to keep the members of the development team anonymous. We do plan on releasing info about the members of the core team at a later stage, but as some of us are working in businesses where anonymous crypto coins might not be well looked upon, we have chosen this approach.

For now you can find us on Telegram as:

CORE TEAM

CEO/Founder	@armr_core
CPO (Chief Product Officer)	@armr_product
CBO (Chief Branding Officer)	@armr_team
Lead Developer	@lead_developer_armr
Head of Marketing	@pr_armr
Head of Webdeveloping	@core_webdev_armr

COMMUNITY TEAM

Advisor	@azazel002
Advisor	@blockmastery
Moderator	@newral

CONNECT WITH US

Stay up to date with the latest news and releases from ARMR.

- **@Medium**
  https://medium.com/@ARMR.Network
- **@Telegram**
  https://t.me/joinchat/Fui6dktBiSptg-aFXH3V-A
- **@Twitter**
  https://twitter.com/ARMR_Network
- **@Bitcointalk**
  https://bitcointalk.org/index.php?topic=2711866.msg27742782#msg27742782
- **Steemit**
  https://steemit.com/@armr
- **InvestFeed**
  https://www.investfeed.com/armr_network/
- **Reddit**
  https://www.reddit.com/user/ARMR-Network

DISCLAIMER

ABOUT ARMR

Founded by a group of block chain enthusiasts ARMR aims at providing users with digital asset transactions and services which are designed around security and anonymity, integrating premium assets worldwide, and constructing a state of art block chain platform. ARMR is not a company, there was no ICO held upon the launch.

PRIVACY POLICY

Our Privacy Policy can be found in full on our website:
https://armr.network/ARMR_Privacy_Policy.pdf

TERMS AND CONDITIONS

Our Terms and Conditions can be found in full on our website:
https://armr.network/ARMR_Terms_and_Conditions.pdf