A1 Exchange

Grin Analysis

January 15, 2019

1 Overview

Grin (GRIN)

Grin is an new and exciting privacy cryptocurrency. Started in October 2016 as the first implementation of MimbleWimble, Grin aims to be a secure and bare-bones MimbleWimble implementation. MimbleWimble protocol is addressing the scalability and privacy issues in blockchains solely by relying on battle-tested strong cryptographic primitives and avoiding any unproven technologies.

Website
grin.mw

Whitepaper
github.com/mimblewimble/grin/doc/intro.md

Explorer
grinmint.com/explorer

Blockchain
Grin

Consensus Mechanism
Proof of Work

Algorithm
Cuckoo Cycle Variant

Genesis Date
January 15, 2019

Maximum Supply
Uncapped

2 Summary

MimbleWimble was introduced by a pseudonymous person called "Tom Elvis Jedusor" in 2016. [2] Within days after the publishment of the paper, a small community have started working on an implementation that becomed Grin.

Grin is an open-source effort of implementing MimbleWimble without an organisation or a company behind. Grin has no initial coin offering (ICO), premine or developer reward from blocks mined.

Grin is able to build transactions that are completely opaque and pruned, but still can be properly validated with ease. By generalising those properties to blocks, a large amount of blockchain data can be eliminated which opens the opportunity for great scaling and fast synchronisation of new peers.

If we look at a Grin explorer, there are a number of differences from conventional blockchains:

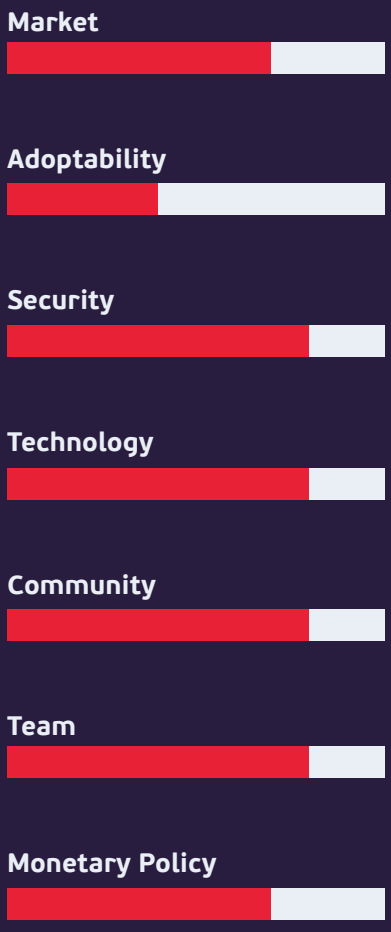
- Addresses don't exist
- Amounts don't exist
- Transactions that spend one another are merged in a block to form only one, removing all intermediary information. This enables extremely efficient scaling in Grin.

Without addresses and amounts, all transactions are indistinguishable from one another. Unless you have participated in the transaction, all the inputs and outputs look like random pieces of data.

Additionally, there are no singled out transactions in a block. A Grin block looks like one giant transaction and it is practically impossible to associate inputs and outputs. This is a huge feature for anonymity and privacy.

Grin is an exciting open-source example of how privacy and scalability can be achieved together.

A1 Rating: BBB



3 Analysis

3.1 Market

> What does this project aim to solve? Why will people use it? If they have competitors who are they and how do they compare to this project?

Privacy cryptocurrencies, commonly referred as privacy coins, are cryptocurrencies designed to preserve the privacy of their users. This is one of the major categories of cryptocurrencies with strong examples such as Monero, Zcash, and Bytecoin. Privacy cryptocurrencies currently has around $1.5 Billion market cap of $123 Billion total cryptocurrency market cap. This group of cryptocurrencies had a weak performance compared to other categories in the recent years. [11] However, this lagging could mean a bigger upper potential compared to overall cryptocurrency market. On the other hand, privacy cryprocurrencies market is one of the small number of categories with a viable use case in the short term.

Present popular privacy cryptocurrencies are able to handle their demands. [12]

However, none of them offer a scalable solution. Along with very recent proposal of ZK-STARKs, MimbleWimble protocol is certainly one of the most interesting privacy blockchain solutions. [13]

MimbleWimble, therefore Grin, introduces a new approach on how to offer great privacy and scalability.

MimbleWimble transactions demonstrate strong privacy and confidentiality properties. It is not possible to see amounts transacted in Grin transactions, hence the strong confidentiality.

BEAM is another MimbleWimble project that has many similiar properties as Grin.

Grin aims to maintain a simple implementation of the MimbleWimble protocol. BEAM on the other hand, has made large modifications to the MimbleWimble approach with the aim of providing extensive features.

Compared to BEAM, two of Grin's unique features are the use of DAGs and partial history syncing.

Grin uses Directed Acyclic Graph (DAG) to keep the mempool state. This improves the performance and the scalability of Grin, while preventing duplicate unspent-transaction-outputs (UTXOs).

Grin's innovation on partial history synchronisation enables faster node start-up times. Depending on the size of the blockchain, bandwith and machine performance, synchronisations on new node creations could take days. Therefore, this feature could be valuable as the blockchain of Grin grows.

While BEAM has many unique features that separates it from Grin, the most notable ones are possibly having addresses, a great wallet experience and non-interactive transactions which allows a better user experience and adoptability.

Even though BEAM seems better suited for mass adoption, there are many controversial choices BEAM has made regarding its economy. Most notably, BEAM has a treasury mechanism which is populated with a 20% "Founders Reward" from every block mined for 5 years.

3.1.1 Market score: 7

There's no doubt that Grin will become a strong player in the $1.5 Billion privacy coin market. In terms of protocol, its competitor BEAM currently has a way better user experience and is better suited for wide adoption but fails to provide an egalitarian economic model due to its controversial monetary policy and governance. That said, Grin seems to be a better choice for an egalitarian economy.

3.2 Adoptability

> How can this project reach mass adoption? Why is it appealing to the end user in terms of user experience? Is it easy to pick up or understand? Are there mechanisms in place for increasing adoption?

Partly due to its new and complex technology, Grin is extremely hard to use for beginners. Since Grin eliminates the conventional concepts that almost all cryptocurrencies employ, it is difficult to understand even for people who are familiar with well known cryptocurrencies. Most importantly, the lack of addresses in Grin leads to confusion on how to transact with other parties.

Grin currently has a built-in wallet, which is impossible to use by non-tech savvy users. This wallet requires a running Grin node and a Linux system. The user should compile the wallet to use it. Users transact with each other by running their wallets at the same time and entering each other's IP addresses.

Another wallet implementation named Wallet713 enables a better experience by using a relay service called Grinbox which uses public keys like addresses to route transactions. [4] [5] It's also possible to use Wallet713 with personal keys published on Keybase.io. [6]

Although Wallet713 shares most of the shortcomings of the original Grin wallet, it allows the comfort of handling Grin with addresses, while compromising on decentralization by relying on a third-party relayer service.

At the time of this writing, there are no pre-built binaries for these wallets. They need to be built from their source codes on Linux.

3.2.1 Adoptability score: 4

Grin definitely needs to work on its user experience and ease of use. It is already difficult enough to get people to use cryptocurrencies as it is, and Grin does not make it any better, it makes it worse if anything.

3.3 Security

> What is the track-record on security? How is consensus achieved in this network? How secure is this network? What is the hashrate dispersion between miners?

3.3.1 Exploit Risks

Grin Council has collected their target $100.000 for paying a security audit on December 20, 2018. [16] The team were planning to launch the mainnet after the completion of a security audit, but nothing was heard from the developers on this as of January 15, 2019. [17]

As the Grin team expresses it clearly: "While the Grin development team has done everything it can to identify and fix possible major security failures, Grin is still a very young and unproven codebase." [16]

3.3.2 Proof of Work

Grin uses a GPU oriented Cuckoo Cycle variant named Cuckaroo 29 for its proof-of-work algorithm. [15]. Cuckoo Cycle is a memory bound graph-theoretic proof-of-work algorithm based on finding cyclic routes in given graphs. [10] A simple explanation of the algorithm along with more details on the algorithm choice is provided by the Grin team in their documentations. [14]

Choosing to have or not have ASIC resistance in networks is a debated topic, which some researchers claim having ASICs is better for total network security but a cost of centralization in mining power due to its hyper-capitalistic nature.

3.3.3 Security score: 8

All things aside, Grin has an excellent team of well-known veteran cryptographers, security experts and programmers therefore easily has the means to deliver a secure product.

3.4 Technology

> Is the technology there? Is it technologically possible/practial? What is the current progress and how does the codebase look so far? Is the technology properly outlined and explained?

Grin is a MimbleWimble protocol implementation which was built from scratch in Rust programming language.

Grin transactions demonstrate strong privacy and confidentiality properties. It is not even possible to see the amounts transacted in Grin transactions. Nodes verify that transactions are valid by comparing the sum of inputs and the sum of outputs.

However, bad actors might try to trick this mechanism by transacting negative values, which would still make the transaction valid if the sums are equal. To solve this problem, Grin uses a cryptographic concept called range proofs, a proof that a number falls within a given range. [3] Grin nodes verify that transactions are transacting a positive amount by making use of Range proofs. Thus, nodes are able to verify transactions are valid without requiring to know the amounts transacted.

Another important concept of Grin is a pruning technique they called "cut-through". [18] Cut-through allows the Grin blockchain to gain;

- Extremely good scalability: This is because by using cut-throughs a great majority of transaction data can be eliminated over time without compromising security.
- Further anonimity: Mixes and removes transaction data (Only the proofs are stored).
- Faster node synchronisation: By eliminating a large portion of the data nodes are able to sync with the network very efficiently.

Due to MimbleWimble protocols design, all Grin transactions are aggregated into one big transaction by miners. This one big transaction is considered a block. This structure allows the following benefits

- All outputs look the same: just very large numbers that are impossible to differentiate from one another. If one wanted to exclude some outputs, they'd have to exclude all.
- All transaction structure has been removed, making it impossible to tell which output was matched with each input.

Jedusor realised that all transaction structure can be eliminated and the order of inputs and outputs do not matter anymore. However, the sum of all outputs in this block, minus the inputs, is still guaranteed to be zero.

Grin transactions require interaction between the sender and the receiver (meaning wallets need to exchange data). This does not mean that both parties need to be online at the same time. Grin has a couple of easy methods to transact between users.

3.4.1 Scripting and Contracts

By default the protocol MimbleWimble used in Grin does not support scripts thus not supporting smart contracts. But this is circumvented by Grin using some cryptographic tricks. So far the following features have been demonstrated for Grin:

- Multi-signature transactions
- Atomic swaps
- Time-locked transactions and outputs
- Lightning Network

3.4.2 Dandelion

Grin also implements Dandelion protocol. [9] Dandelion is a privacy preserving transaction aggregation and propagation protocol. In regular transaction broadcasting mechanisms, nodes carry the risk of eavesdroppers associating transactions with their source IP addresses. In general, Dandelion provides a significant improvement to the confidentiality of the P2P layer of any cryptocurrency that chooses to implement it. In Grin's implementation, the confidentiality benefits of Dandelion is further improved by using some protocol-specific tricks, thus making it even more robust against potential attackers.

3.4.3 Interactive Transactions

Grin transactions require interaction between the sender and the receiver (meaning wallets need to exchange data). This does not mean that both parties need to be online at the same time. Grin has a couple of easy methods to transact between users.

3.4.4 Technology score: 8

Grin demonstrates a new approach to how we understand and interact with blockchains. Even though its core protocol does not allow or easily integrate with certain features, Grin circumvents most of these with some clever programming.

3.5 Scalability

How scalable is this project?

Due to the MimbleWimble transaction and block format in Grin, transactions are merged where an output is directly spent by the input of another. If when Alice gives money to Bob, and then Bob gives it all to Carol, Bob was never involved and his transaction is actually never even seen on the blockchain. This means that Grin is able to scale extremely well.

Grin also removes all spent output data from the blockchain. This allows for new nodes to download and verify the entire blockchain in just a few gigabytes or less (assuming a number of transactions similar to Bitcoin).

This implies that the Grin blockchain scales with users (unspent outputs) and not by the number of transactions. This approach requires for a small piece of data called "kernel" to be stored for each transaction which every kernel is around 100 bytes. Grin aims to optimise this piece of data further.

3.5.1 Scalability score: 8

Grin perfectly demonstrates how privacy and scalability can be achieved together without any compromises. Syncing up with the network is a matter of a few gigabytes.

3.6 Community

> Is there a community? Who contributes to this and why? Is controlled by a corporation or is it open source?

Grin is an open-source project and is not controlled by any company or organisation. Grin Council, which is geologically distributed, oversees the development efforts.

Grin has achieved a massive following and popularity prior to its launch. The project has been frequently mentioned by known cryptocurrency figures and companies in the the media. This has rallied many talented developers to join its development effort. Even when the project was in its Testnet and development stage, many developers and companies started building and further improving on Grin.

3.6.1 Community score: 8

Grin has gained an excellent following of talented people and big organizations. Many developers and companies started to build on and integrate with Grin prior to its mainnet launch.

3.7 Team

> Who is building this? What is their track record? Is it possible for this team to deliver on their promises? Is the team engaged with the community and do they provide timely updates?

Grin has a core team of hardened veterans in cryptography and software development. The development effort is lead by Ignotus Peverell and has more than 100 contributors from all around the Internet. The governance nature of the project is reminiscent of a true open-source effort where the team raises funds via community donations for the development costs and security audits.

The team has many important connections with strong academic and industrial personalities. These connections could bear fruits for Grin project. For instance, the crypto investment and infrastructure engineering platform Layer1, which is backed by Peter Thiel, announced that they are "deeply involved" with Grin. [7]

3.7.1 Team score: 8

The Grin team consists of some of the best talent in the cryptospace such as Andrew Poelstra and Ignotus Peverell.

3.8 Monetary Policy

> How much of the supply is controlled by the founders? How dispersed is the economy? How inflationary or deflationary is the currency's model?

The block reward in Grin is currently set at 60 Grin and a block-time of 60 seconds.

Grin team argues that the main reasons behind this comparatively high mining reward is the fact that dilution trends toward zero. As the circulating supply increases, the mining reward will get smaller comparatively.

Although it doesn't make a monetary difference, a higher number of block reward might attract miners, especially in the earlier phases of the project.

Grin's rationale behind the designed inflation dynamic could be best explained by the following quotation:

"As an experimental hypothesis, Grin's inflation rate may discourage hoarding, improving its distribution. This disincentivizes "whales," who otherwise have an inordinate amount of control over the price of an asset, and downplays speculative bubbles and price swings. This argument is discussed at length in Bitcoins are not digital greenbacks, in which Wei Dai himself considers "Bitcoin to have failed with regard to its monetary policy". This could provide enhanced supply/demand certainty for all types of users, and allow transparent and natural pricing. Note: Bitcoin becoming widely usable as a method of exchange versus a strict store of value depends on the concept of "Keynesian beauty contests." The experiment is ongoing." [3]

3.8.1 Monetary Policy score: 7

While Grin has strong arguments and data against having a capped supply and low emmision rate, it seems to be a risky experimental approach.

4 Methodology

A1 Exchange research committee analyses cryptocurrency projects for listing the deserving ones on A1 Exchange. To be able to select the projects with highest potential benefit to A1 Exchange, we follow standardized procedures, as described in this section, to ensure consistent analyses and ratings. Our methodology is developed to be systematic, and rigorous to maintain the high quality of A1 Exchange analyses and their comparability across different projects.

To fulfill our commitment on transparency to our users, and to get feedback on our decision making, we publish these reports with the public.

4.1 Resources

The analysis process starts by obtaining information about the project. The projects considered for A1 Exchange are usually in their early stages, which makes it difficult to find objective secondary resources on them, if any. Therefore the research committee usually consume primary resources.

Primary resources mostly consist of papers and content written by the project team.

These resources may include public conversations on Telegram, Discord, Slack, Gitter, and email groups. In case the resource of a public conversation used in the analysis could not be referred through a URL, the citations include the relevant quotations with the available information such as channel name and date.

In many cases, we are forwarding our questions to the team of the project, or other parties. These conversations could affect the analyses, but not cited unless explicitly allowed.

The research committee conducts a reasonable investigation of data accuracy and fact-checking. However, to a certain extent, A1 Exchange relies on information it receives from sources to be credible.

4.2 Analysis Topics

Projects are rated under the following topics: Market, Adoptability, Security, Technology, Community, Team, and Monetary Policy. These topics are determined to cover all aspects for a project to be worthy of being listed on A1 Exchange.

Projects are given a rating for each analysis topic. These ratings are used to calculate A1 Rating, and A1 Exchange's decision on listing the project.

Each topic rating starts at a baseline rating of 5, and goes up or down from there. A rating of 5 is average. Any rating above 5 should be considered above average, whereas only ratings below 5 are below average.

Ratings are decided unanimously by the research committee.

4.3 A1 Rating

A1 Exchange rates projects with the following letter ratings: AAA, AA, A, BBB, BB, B, CCC, CC, C, D, and E. These ratings correspond to number ratings from 10 to 0. Since obtaining a rating of 10/10 or even 9/10 is very unlikely for a project in our rating methodology, A1 Ratings are given as letter ratings.

A1 Rating is calculated by taking the mean average of the ratings from analysis topics, and rounding the average to the nearest integer. Then, A1 Rating is derived from the integer numeric rating.

Only if a project's A1 Rating is AAA, AA, A, or BBB, the project is eligible to be listed on A1 Exchange.

As with everything else in A1 Exchange analyses, A1 Ratings do not constitute investment advice. For more information, read the **Important Disclaimers** section below.

4.4 Publication

Once an analysis is ready to publish, the project's team is provided an opportunity to review the analysis to allow the team to check for factual accuracy and possible presence of confidential information. This notification is given in writing at least one working day before the intended publication.

Prior to this disclosure, the project team will be asked to keep this communication, and the analysis paper confidential, and not to use this information to their advantage. This commitment from the project team is crucial not to allow insider trading, or any other abuse of information asymmetry.

A1 Exchange evaluates any feedback or comments from the project team. However, we retain the full editorial control over such feedback.

A1 Exchange aims to publish its analyses to the public shortly after these notifications. A1 Exchange analysis publications are communicated through our social media channels and email lists as soon as they become publicly available.

4.5 Updates

A1 Exchange ratings are typically monitored on an ongoing basis. We accept feedback and recommendations for our analyses. Feedback for our analyses through our GitHub repository issues are available publicly [1].

Analyses are subject to scheduled reviews typically a year after the last update.

Changes in our methodology are applied to both the new and the existing analyses. A review of an existing analyses will be completed withing six months after a methodology change.

Upon an analysis review, the project's ratings could be updated. In case the A1 Rating falls below the listing threshold, the project could be delisted from A1 Exchange, following the delisting procedure.

5 About A1 Exchange

Our vision with A1 Exchange is being the platform only for the best cryptocurrency projects and traders. In order to make this possible, we have several processes that we execute before listing a new project. We focus on the fundamentals when choosing a new project to list on the platform.

6 References

[1] "A1 Exchange Analyses", GitHub.
https://github.com/A1Exchange/a1-exchange-analyses

[2] https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf

[3] https://infoscience.epfl.ch/record/128718/files/CCS08.pdf

[4] https://github.com/vault713/wallet713

[5] https://grinbox.io

[6] http://keybase.io

[7] https://www.coindesk.com/peter-thiel-backs-2-1-million-round-for-crypto-investment-startup-layer1

[8] https://github.com/mimblewimble/docs/wiki/Monetary-Policy

[9] G. Fanti, et al. "Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees", 2018. https://arxiv.org/abs/1805.11060

[10] John Tromp, "Cuckoo Cycle: a memory bound graph-theoretic proof-of-work", 2018. https://github.com/tromp/cuckoo/blob/master/doc/cuckoo.pdf

[11] "Cryptoasset Classification and Analysis of Crypto Sectors' Historical Growth", Pavel Pankratov. https://hackernoon.com/cryptoasset-classification-and-in-depth-analysis-of-crypto-sectors-historical-growth-675b0af8660b

[12] "Blockchain Activity Matrix", Block'tivity. https://blocktivity.info

[13] E. Ben-Sasson, et al. "Scalable, transparent, and post-quantum secure computational integrity" 2018, https://eprint.iacr.org/2018/046.pdf

[14] "Grin's Proof-of-Work", GitHub.
https://github.com/mimblewimble/grin/blob/master/doc/pow/pow.md

[15] "Choice of ASIC Resistant PoW for GPU miners", John Tromp.
https://www.grin-forum.org/t/choice-of-asic-resistant-pow-for-gpu-miners/1017/61

[16] "Security Audit Funding", Grin. https://grin-tech.org/sec_audit.html

[17] "Security audit funding campaign", Grin Forum. https://www.grin-forum.org/t/security-audit-funding-campaign/962

[18] "Pruning Blockchain Data", Grin. https://github.com/mimblewimble/grin/blob/master/doc/pruning.md

7 Important Disclaimers

For the purposes of MiFID II, the A1 Exchange Analyses are marketing communications and are not in scope for any MiFID II / MiFIR requirements specifically related to investment research. Furthermore, the A1 Exchange Analyses, as nonindependent research, have not been prepared in accordance with legal requirements designed to promote the independence of investment research, nor are they subject to any prohibition on dealing ahead of the dissemination of investment research.

This document is a general communication being provided for informational purposes only. It is educational in nature and not designed to be as advice or a recommendation for any specific investment product, strategy, plan feature or other purpose in any jurisdiction, nor is it a commitment from A1 Exchange or any of its subsidiaries to participate in any of the transactions mentioned herein. Any examples used are generic, hypothetical and for illustration purposes only. This material does not contain sufficient information to support an investment decision and it should not be relied upon by you in evaluating the merits of investing in any securities or products. In addition, users should make an independent assessment of the legal, regulatory, tax, credit, and accounting implications and determine, together with their own professional advisers, if any investment mentioned herein is believed to be suitable to their personal goals. Investors should ensure that they obtain all available relevant information before making any investment. Any forecasts, figures, opinions or investment techniques and strategies set out are for information purposes only, based on certain assumptions and current market conditions and are subject to change without prior notice. All information presented herein is considered to be accurate at the time of production, but no warranty of accuracy is given and no liability in respect of any error or omission is accepted. It should be noted that investment involves risks, the value of investments and the income from them may fluctuate in accordance with market conditions and taxation agreements and investors may not get back the full amount invested. Both past performance and yields are not reliable indicators of current and future results.

To the extent permitted by applicable law, we may record telephone calls and monitor electronic communications to comply with our legal and regulatory obligations and internal policies.

Personal data will be collected, stored and processed by A1 Exchange in accordance with our Company's Privacy Policy. For further information regarding our regional privacy policies please refer to the EMEA Privacy Policy; for locational Asia Pacific privacy policies, please click on the respective links: Hong Kong Privacy Policy, Australia Privacy Policy, Taiwan Privacy Policy, Japan Privacy Policy and Singapore Privacy Policy.