CrushCrypto

Deep Dive Review into Grin

Private and lightweight Mimblewimble blockchain

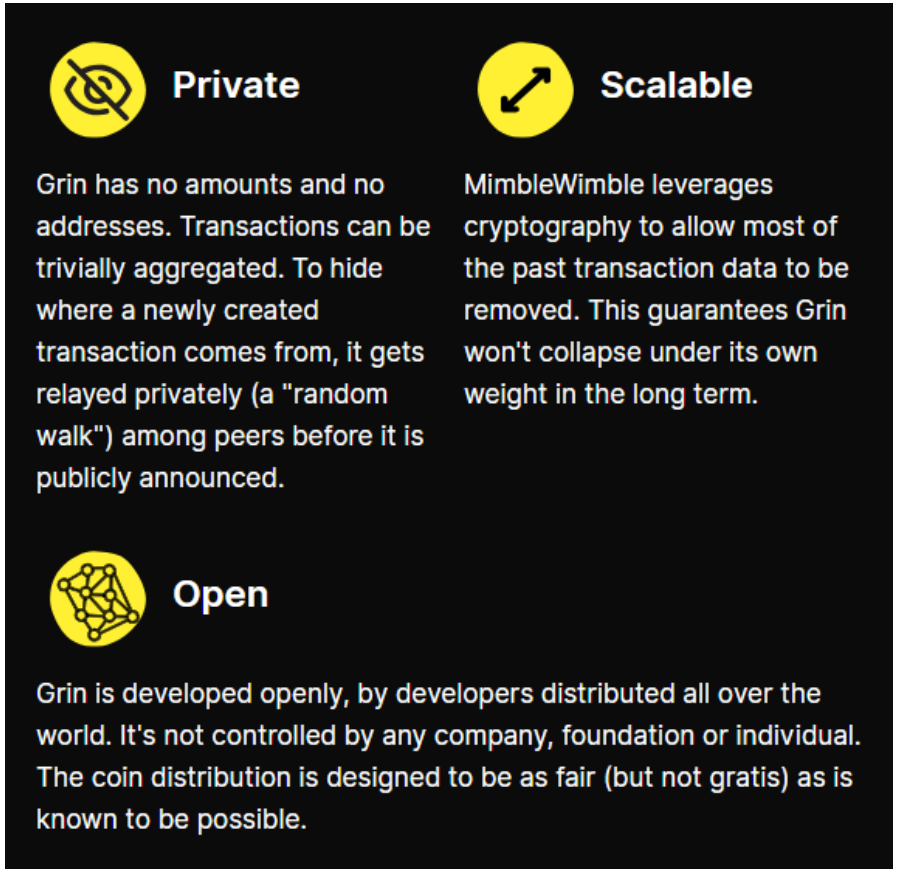
March 11, 2019

What is Grin?

- An open source blockchain that uses the Mimblewimble protocol to provide extra privacy.
- Mimblewimble is a protocol where transactions can be cryptographically verified despite hiding the amount that is being sent.
    - Every Bitcoin transaction reveals both the sender's and receiver's addresses and the exact amount of BTC sent. This mechanism ensures security as anyone can confirm the correct amount of BTC being transacted or in a specific address at any given time.
    - Mimblewimble attempts to hide the amount of cryptocurrency in a transaction while still allowing others to prove the transaction is valid.

Main characteristics of Grin

- Privacy by default, enabling complete fungibility with the ability to selectively disclose information as needed.
- Scales with the number of users instead of number of transactions to save space.
- Strong cryptography – Mimblewimble and Grin use Elliptic Curve Cryptography.
- Design simplicity allowing for easy auditing and maintaining.
- Community driven with a focus on mining decentralization.



Grin transactions

- Grin transactions are unique because there are no addresses or amounts, and two transactions (one spending the other) can be merged in a block to form one, removing intermediary information.
    - Example: If Alice sends money to Bob, who later sends it all to Carol, Bob is never technically involved, and his transaction is never seen on the Grin blockchain.
- A Grin transaction consists of three components:
    - A set of inputs that reference and spend a set of previous outputs
    - A set of new outputs (these are called Pederson Commitments)
    - A transaction "kernel"

Achieving scalability

- Grin is achieving scalability by using these Mimblewimble transactions and unique block format. As most outputs are eventually spent by another input, all spent outputs can be removed from the blockchain. This keeps the size of the data on the blockchain relatively low when compared to existing chains like Bitcoin.
- This is how the Grin blockchain mostly scales with the number of users instead of the number of transactions. The number of users is represented by unspent outputs (i.e. any wallet with a balance greater than 0), and individual transaction data is not necessary to include in the block.

Grin Consensus Mechanism

- Grin uses a basic proof of work (PoW) algorithm called Cuckoo Cycle, specifically designed to be resistant to hardware arms-races. It is primarily a memory-bound algorithm, which means that solution time is bound by memory bandwidth rather than raw processor or GPU speed.
- In theory, mining Cuckoo Cycle solutions is viable on regular hardware and require less energy than other GPU, CPU, or ASIC bound PoW algorithms. Avoiding strict hardware requirements should increase the decentralization of mining over time, opposite to the increasing centralization seen with other PoW blockchains.
- Grin implements a difficulty target that is intended to evolve according to the available network hashpower. The goal of this difficulty is to keep the average block solution time within a target range, which is currently 60 seconds. For reference, the Bitcoin average block time is 10 minutes and Ethereum is roughly 15 seconds.

Key features

- **Mimblewimble** – The privacy protocol that allows Grin transactions to be verified while hiding the details. It uses transaction blinding factors called Pedersen Commitments to hide these inputs and outputs.
- **Scalability** – The Grin blockchain only stores unspent outputs and a small data kernel for every transaction in a block, which means the blockchain size grows slower over time and scales with the number of users instead of number of transactions.
- **Organic launch** – There was no ICO and no pre-mine to launch Grin, and there is no mandatory portion of the mining rewards given to the developers.
- **Cuckoo Cycle** – The algorithm behind Grin's proof of work consensus mechanism. It is a memory-intensive algorithm that does not require specific hardware and may be able to preserve a high level of mining decentralization.

Key milestones

- **July 19, 2016**: The first paper on Mimblewimble was released by an anonymous person who went by Tom Elvis Jedusor.
- **October 6, 2016**: Andrew Poelstra, a mathematician at Blockstream, released a more detailed paper expanding on Mimblewimble and added further scaling improvements.
- **October 2016**: An anonymous person who called themselves Ignotus Peverell started a GitHub project called Grin.
- **March 2017**: Ignotus Peverell posted a technical introduction to Mimblewimble and Grin on GitHub.
- **January 15, 2019**: The first main-net Grin block was mined, and Grin network was officially released.

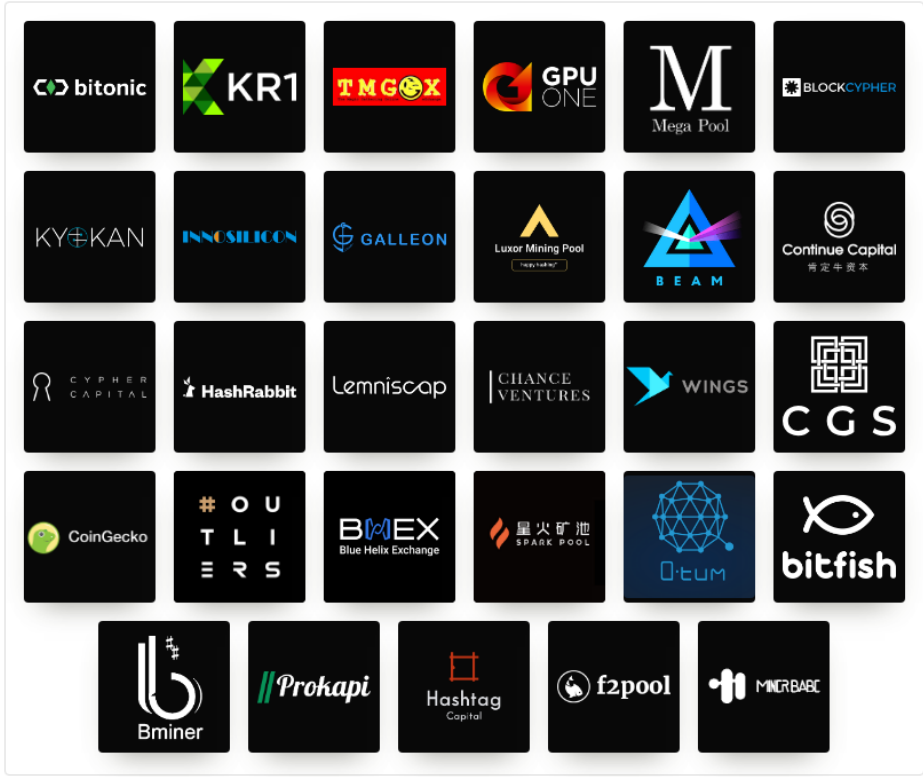
Token economics

- As of March 6, 2019, the circulating supply of Grin is 4,336,260 with a market cap of $14 million.
- The rate of new Grin coins being released is 60 per block, or 1 every second. This rate is likely to remain constant forever, meaning the inflation percent will decrease every year as the circulating supply grows.
- After 10 years, the inflation rate will fall below 10% - after 20 years, below 5%. In 25 years, Grin will have a 4% inflation rate, comparable to Bitcoin's rate 10 years after its creation. Additionally, the Grin team has cited multiple studies to estimate that 2% or more of Grin tokens will be lost from circulation each year.

The team

- Grin was not created by a company and has no CEO or official leadership team, although there are companies who have donated or supported the project.
- The individuals working on Grin are volunteering their time to the project and are solely funded through community donations. There are no public profiles of the team. However, we can see that the open-source project has 121 contributors so far.
- Donors to the Grin project include individuals and companies such as BlockCypher, Bitonic, CoinGecko, Cypher Capital, and many more.

Companies



Strengths

- Mimblewimble is a promising privacy protocol that completely shields transaction information from any third parties. It also allows for transactions to be verified while storing minimal data on the blockchain, which means Grin is a highly scalable blockchain.
- Grin launched with no ICO, no pre-mine, and no allocation for the founders, which may be viewed positively in the crypto community and discourage speculators who only want to get rich quick.
- The open-source project is being developed by a highly competent group of developers. From the Grin GitHub, there are 121 contributors to the project and development is very active.

Strengths (continued)

- The token economics of Grin are straightforward and ensure the inflation rate will decrease every year. This would help Grin to establish a clear-cut monetary policy that would not be easily changed in the future.
- Even though Grin is a young project, it has already developed a decent community and exposure among the cryptocurrency space, with multiple solid exchanges (Poloniex and Bittrex) listed the coin.

Weaknesses

- The decentralized nature of Grin is very different from many tokens that have a founding company and a public team. However, it has been seen with Bitcoin that having no true leadership can lead to long disputes over how to update the blockchain, and this could be an issue for Grin going forward.
- Since there is no fundraising, Grin developers rely on donations to fund the project. If such donations eventually stop coming in, the Grin developers will have to volunteer their time to work on the project. This may cause developers to leave Grin for other projects with more funding or a foundation that pays its developers.
    - Yeastplume, a core developer for Grin, had been raising donations multiple times to fund his development of the project. There is no assurance that the donations would keep up in the future.

Weaknesses (continued)

- Grin has a lot of competition in the market as privacy coins like Zcash and Monero have a first-mover advantage, larger communities, and more widely known privacy protocols.
- The future of privacy coins in general is still uncertain. Even if they work perfectly, there still must be a sizeable market of people who want financial privacy in order for the coin to succeed. There is also significant uncertainty with respect to government regulation that could make it hard for Grin to thrive.
- The diluted market cap for Grin is very large right now. According to Messari, Grin is the 7th most valuable cryptocurrency using coin supply at year 2050, higher than both Monero and ZCash.

Conclusion

Overall Rating: B.

- Grin is one of the first implementations of the promising new privacy protocol Mimblewimble. It has a clear mission to be a highly scalable and privacy-focused coin, which could help it in the long run as other blockchains continue to face privacy (for coins without a private-by-default system) and/or scaling issues.
- However, Grin has a lot of competition in the privacy coin market segment, in particular projects that are or have plans to implement Mimblewimble protocol (Litecoin, Monero, and Beam).
- The monetary policy for Grin, while simple, would lead to very high inflation in the first few years of the network. Miners would keep selling their mined coins on the market which leads to constant selling pressure.

Conclusion (continued)

- Grin was launched in a similar fashion to Bitcoin in a truly decentralized fashion with no token sale, airdrops, pre-mine, or reserved block rewards. Contributions come from a community of developers who are funded solely by donations.
- However, this is a different time than when Bitcoin was launched. There is now a lot more competition for talented blockchain developers. It just takes more effort nowadays for blockchain projects to stand out from the crowd and build a sizable community.
- It might be difficult for Grin to compete on talent with other well-funded competitors. Considering the rise of the ICO model and companies launching their own tokens, it will be interesting to see if Grin's organic release will be beneficial or harmful in the long run.
- As Grin is still a very young project, we don't believe it should be the 7th most valuable cryptocurrency under diluted market cap but it is indeed a promising protocol.

CrushCrypto