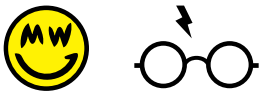
SMITH+CROWN

ORIGINAL RESEARCH

Grin & MimbleWimble

Grin is among the earliest projects building on MimbleWimble, a privacy-focused protocol leveraging elliptic curve cryptography and an Unspent Transaction Output (UTXO) model to enhance the privacy of transactions. Grin builds on MimbleWimble by introducing a memory intensive PoW consensus mechanism designed with ASIC-resistant permutations. Led by a predominantly anonymous team whom contribute to the open-source codebase, Grin relies on donations to fund development. Multiple narratives contribute to Grin's status as one of the year's most widely discussed and eagerly anticipated projects, and commentary on these from a Smith + Crown analyst helps clarify Grin's prospects and challenges.



MimbleWimble Overview

MIMBLEWIMBLE NOTABLE DEVELOPMENTS

2013
A whitepaper proposes anonymizing BTC transactions via One Way Aggregate Signatures (OWAS)

July 19, 2016
Tom Elvis Jedusor (an anagram of 'Je suis Voldemort') publishes the MimbleWimble text file on a Bitcoin IRC channel

October 6th, 2016
Andrew Poelstra, a mathematician and cryptographer releases his own whitepaper that builds upon and refines the MimbleWimble protocol

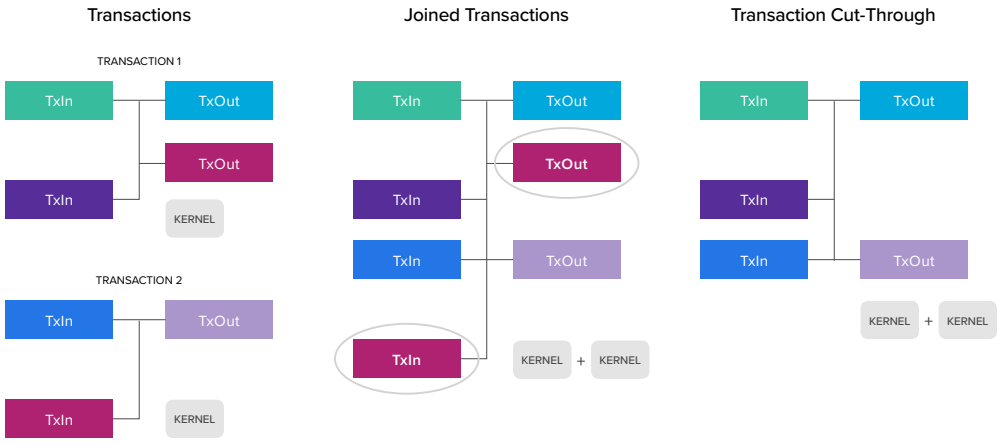
Grin builds on the MimbleWimble protocol, and the project's unique contributions are best appreciated in contrast with MimbleWimble's base features. MimbleWimble is a blockchain protocol published July 2016 as a text file posted on the #bitcoin-wizards IRC channel by the pseudonymous 'Tom Elvis Jedusor.' The paper combined existing research in novel ways, using many of the Bitcoin blockchain's features to add privacy features without the corresponding drastic increase in hardware requirements to validate the history of the network. MimbleWimble achieves its privacy benefits by approaching UTXO transactions differently from other privacy-focused cryptoassets, such as Monero and Zcash. Specifically, in lieu of a published address, cryptographic commitments representing the amount transacted among parties are all that is published to the chain.

MimbleWimble's approach to UTXOs is a core differentiating feature. Essentially, a new node joining a MimbleWimble based blockchain can verify the current state of the chain by processing the current unspent transaction outputs, rather than running through the history of every single transaction, as is the case in Bitcoin. The UTXO approach can briefly be described as a protocol where multiple cryptoasset inputs of differing amounts are combined to achieve an amount equal or greater than that which a user desires to send to someone else. For example, a user may have .5, .8, and .3 BTC inputs in her account. If she desires to send 1 BTC to someone else, the protocol might combine .8 and .3 into a transaction, then return the remainder of .1 BTC back to the original sender, less transaction fees. This .1 BTC 'refund' is recorded as its own transaction on-chain. During this process, the Bitcoin blockchain publicly records information, such as the sending account, the amount transacted, and the receiving account. This publicly available information is often useful for transparency and accounting purposes, but is considered to offer insufficient privacy for many blockchain use cases.

Diagram 1

Cut-Through Transactions

Cut-through transactions significantly shorten the information required to validate the history of transactions by focusing on the UTXOs



> Essentially, a new node joining a MimbleWimble based blockchain can verify the current state of the chain by processing the current unspent transaction outputs, rather than running through the history of every single transaction, as is the case in Bitcoin.

MimbleWimble's privacy-focused design, which hides amounts transacted and where addresses do not exist, can appear unintuitive to those more accustomed to either Bitcoin's UTXO model or Ethereum's accounts-based approach. Cryptoassets built on the MimbleWimble protocol, such as both Grin and BEAM, enjoy several privacy features, most notably the obfuscation of amounts being transacted and the identities of those transacting. MimbleWimble's privacy features, unpacked below, are enabled by several technologies used in tandem with the Bitcoin UTXO model, such as elliptic curve cryptography.

MimbleWimble: A Different Approach to UTXO

> *"Mimblewimble is a design for a cryptocurrency whose history can be compacted and quickly verified with trivial computing hardware even after many years of operation. As a secondary goal, it should support strong user privacy by means of confidential transactions and an obfuscated transaction graph"*
>
> — Andrew Poelstra, Mimblewimble October 2016

MimbleWimble aims to make this UTXO-based transaction design more private and scalable. It does so by:

- **Removing transacting addresses** altogether, to preserve privacy
- **Representing transaction input and output amounts as cryptographic hashes**, thereby preserving privacy
- **Leveraging a non-interactive version of Greg Maxwell's Coinjoin in order to combine all transactions within a block into a single transaction**, obscuring transaction details
- **Enabling more efficient verification of the current chain state** with 'Cut-Throughs', requiring reference to significantly fewer data-points

The first two features above enable the privacy and anonymity of transacting parties and amounts, while the last two features aim to organize UTXO data in a way that reduces data storage requirements, obscures individual transaction data, and ultimately reduces the hardware requirements needed to verify the state of the network. MimbleWimble combines the following technologies to achieve these features and their benefits:

CONFIDENTIAL TRANSACTIONS

Confidential Transactions (CTs) were originally conceived by Blockstream co-founder Greg Maxwell to hide both the amounts transacted and addresses of the transacting parties. CTs are enabled by Pedersen Commitments, cryptographic commitments that have homomorphic properties allowing verification that the inputs to a transaction equal the outputs, without actually revealing the amounts. CTs require significant data storage capacity from validating nodes, which is their main drawback. MimbleWimble mitigates this drawback using a technique known as 'Cut-Throughs'. Cut-Throughs significantly reduce the information required to validate the history of transactions. Essentially, by focusing on the UTXOs, validators can skim over much of the detail composing the individual transactions. This additionally further obscures which inputs contribute to which outputs.

CUT-THROUGHS, KERNELS, AND BLINDING FACTORS

A 'Cut-Through' (of the transaction structure) is used for each block, where some inputs to transactions within a block are previous UTXOs, to perform blockwide transactions rather than many transactions in one block. Cut-Throughs obviate the need to store intermediate UTXO transactions within a block, reducing data storage requirements for nodes. For each intermediary transaction, the kernel is effectively a multisig key for participants that allows the protocol to determine coins' ownership. These small (in data size) kernels are stored by full nodes as a record of valid transactions. MimbleWimble repurposes Blinding Factors from the original Confidential Transactions design into private keys authorizing the output's expenditure; this effectively eliminates the concept of an address while preventing double-spends.

COINJOIN-INSPIRED TRANSACTION OBSCURING

Greg Maxwell also invented CoinJoin, which obfuscates individual transactions by combining multiple transactions together. This improves privacy, as determining which inputs (unspent outputs from previous transactions) come from which users becomes more challenging. Other implementations of CoinJoin are optional for users, which reduces the privacy guarantees and require an interactive step from each for each transaction. In MimbleWimble, CoinJoin functionality is enabled by default.

MimbleWimble Design Limitations

While the question of whether design choices constitute genuine limitations ultimately rests on the goals and use-cases of relevant parties, compared to like protocols, MimbleWimble's privacy improvements come with certain trade-offs.

> Transactions are sent to a mempool before they are included in a block by nodes, which gives observer nodes the opportunity to gather data and potentially uncover the sender's IP address.

- The protocol's privacy design requires transacting parties to communicate and arrange transaction terms off-chain. Additionally, all parties must be online for transactions to complete successfully. This represents a significant user experience hurdle—one that initiatives such as Grinbox are actively working to remove.
- Confidential Transactions require resource intensive range-proofs on cryptographic commitments to verify that the inputs for a transaction are greater than or equal to the outputs without revealing the details. Bulletproofs, also a form of zero-knowledge proof used in Grin to ensure that no invalid creation of tokens is possible, without revealing the transaction amounts to a third party, reduce the amount of data needed to store a Confidential Transaction by an order of magnitude. Bulletproofs are also used by the Monero network.
- Transactions are sent to a mempool before they are included in a block by nodes, which gives observer nodes the opportunity to gather data and potentially uncover the sender's IP address through the data's analysis. Grin and Beam's implementations of MimbleWimble attempt to overcome this protocol weakness by using a transaction routing method called Dandelion, which aims to obfuscate the IP address originating the transaction. Dandelion is relatively untested and the extent to which it obscures traffic is dependent on the number of peers participating.
- MimbleWimble lacks expressive scripting by design, so cannot execute code on-chain; accessory solutions proposed by developers may address this limitation. MimbleWimble's current lack of expressive scripting means smart contract functionality is not currently possible using this protocol, that Lightning network style payment cannot be implemented, that cross-chain atomic swaps are not supported, and that MimbleWimble is unsuitable for a wide range of blockchain use cases requiring the execution of code in some

form. However, initial research within the Grin community suggests that some version of primitive contracting functionality may be developed in the future, particularly for atomic swaps.

> MimbleWimble lacks expressive scripting by design, so cannot execute code on-chain; accessory solutions proposed by developers may address this limitation.

MimbleWimble's suitability for a variety of use cases largely depends on these characteristics.

Grin Overview

GRIN NOTABLE DEVELOPMENTS

October 2016
Pseudonymous developer **Ignotus Peverell** creates a GitHub repository for a minimal MimbleWimble implementation known as Grin

June 2018
Developer 'Yeastplume' publishes a draft web-wallet for Grin

December 20th 2018
Grin testnet (Floonet) released

January 3rd 2019
Beam, another MimbleWimble implementation, launch their mainnet

January 15th 2019
Grin mainnet is launched

Grin, written in Rust, makes all transactions using the project's native currency, called GRIN, private in default. The Grin protocol builds on MimbleWimble's base feature set in a manner designed to overcome some of the previously summarized limitations introduced by MimbleWimble's protocol design, though, like MimbleWimble, relies on off-chain peer-to-peer interactions in initiating transactions.

Launching a new, high-profile Proof of Work blockchain also has unique considerations in 2019 that did not exist when Satoshi Nakamoto mined the first Bitcoin block in 2009. These circumstances are reflected in Grin's approach to consensus and mining. Despite this, the nature of Grin's launch and the ideology shared among its core developers have lent itself to viewing Grin, perhaps uncritically, as a sort of 'philosophical successor' to Bitcoin. A working understanding of Grin's approach to consensus, mining, monetary policy, and governance contribute to assigning the narratives' surrounding Grin their proper credence.

Transactions and Privacy Features

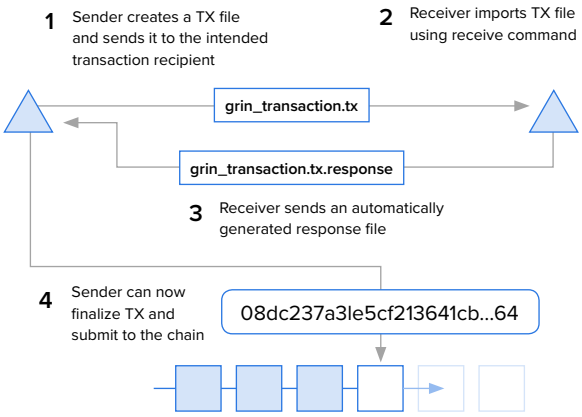
Sending a transaction in Grin requires transacting parties to communicate off-chain, since the MimbleWimble protocol it is based on does not use addresses to send or receive GRIN, a departure from many other cryptocurrencies. Rather than use addresses, Grin users spend unspent transaction outputs (UTXOs), using just private keys associated with those UTXOs and knowledge of amounts sent. The process for sending a transaction, depicted in Diagram 2, is broadly as follows:

1. The sender creates a file describing the amount to be sent, signed by their private key.
2. The receiver then responds with their commitment to the data in the file and with their signature.
3. The original sender finalizes the transaction and awaits its verification by mining nodes.
4. After the transaction is verified, the receiver can prove ownership of a portion of the output by specifying their private key and amount of Grin transacted. Outputs in Grin are represented as cryptographic commitments.

Brandon Arvanaghi's Grin Transactions Explained, Step-by-Step provides a more detailed yet still approachable walkthrough of Grin transactions.

Diagram 2

Transacting via Grin



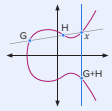
Grin's Use of Pedersen Commitments

In Grin, inputs and outputs are represented publicly as cryptographic commitments where G & H are publicly known values describing an Elliptic Curve.

$$\left(\text{USER'S PRIVATE KEY} * G\right) + \left(\text{AMOUNT OF GRIN} * H\right)$$

In order to spend a given output, one must know the private key and the amount of GRIN sent.

Elliptic Curve



This requirement of interactivity between sender and receiver presents a significant opportunity for developers to produce smooth user experiences around the off-chain agreement to transact. Once the transacting parties have communicated, the sender can submit the transaction to the mempool, which is then randomly aggregated amongst others before miners form blocks. Since the outputs are cryptographic commitments, composed of both publicly available information (Elliptic Curve Generators) and information known only to those transacting (private keys, amount transacted), transactors are able to effectively prove their ownership of UTXOs.

> Grin utilizes two variations of the Cuckoo Cycle algorithm; 90% of the initial block rewards accrue to the variation that is most ASIC-resistant, with this proportion dropping linearly until all block rewards accrue to the non-ASIC resistant algorithm in 2021.

Consensus and Mining

The Grin protocol employs Proof of Work, a somewhat novel choice given that most recent base blockchain launches have used Proof of Stake or variants thereof, generally due to Proof of Stake's potential scalability and environmental benefits. This choice of Proof of Work invites comparisons between Grin and Bticoin's launches.

Bitcoin could be mined on consumer hardware for the first few years among the small initial user base. With the development of ASICs, mining turned industrial. Firms such as Bitmain grew and individuals had difficulty mining profitably without large capital outlays. The advent of increasingly sophisticated and expensive hardware raises barriers to entry for mining in many crypto-assets and concentrates consensus contributions in the hands of relatively few. For example, the Bitcoin industry standard Antminer (S15) produced by Bitmain costs $1020; two mining pools owned by Bitmain

(AntPool and BTC.com) produce over 30% of BTC blocks.

In an effort to resist the increasing dominance of mining by large, heavily capitalized firms, Grin chose to implement a Cuckoo Cycle Proof of Work system. Cuckoo Cycle is the first graph theoretic Proof of Work algorithm and is designed to be memory intensive. Proofs of cycles on graphs are easy to verify: verifiers trace the path once to determine if it is indeed a cycle, making path verification much simpler than path discovery. While Cuckoo Cycle is designed to be mined by GPUs, which do not currently have available ASICs, many believe ASICs development is inevitable, given the economic incentives. History would seem to add weight to this belief; Ethereum's Ethash consensus algorithm was also designed to be memory intensive and ASIC resistant, though ASICs were developed several years after network launch.

Grin approach to block rewards appears to acknowledge the long-term probability of such ASIC's development whilst also attempting to support individual mining. Grin utilizes two variations of the Cuckoo Cycle algorithm; 90% of the initial block rewards accrue to the variation that is most ASIC-resistant, with this proportion dropping linearly until all block rewards accrue to the non-ASIC resistant algorithm in 2021. Grin has also stated its intention to fork the protocol to facilitate updates to the mining algorithm every 6 months. Successful miners are rewarded at a rate of sixty GRIN per one minute block.

The Cryptoeconomics of Grin

Grin Token Function

GRIN, the cryptocurrency, is the native token of Grin, the blockchain. GRIN is designed to function as a means of private payment. Miners are compensated with GRIN for their role in securing the network. Owning GRIN does not confer any formal or informal governance rights over the network.

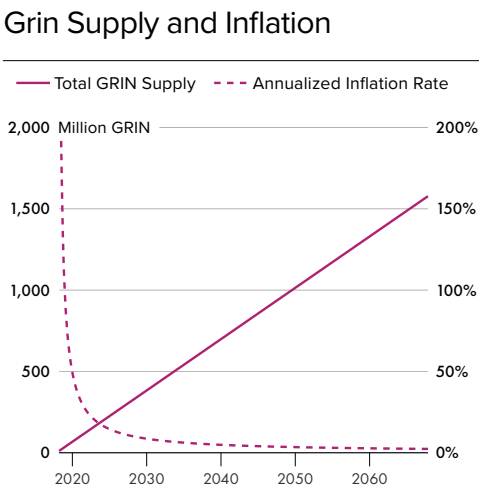
Grin Supply and Distribution

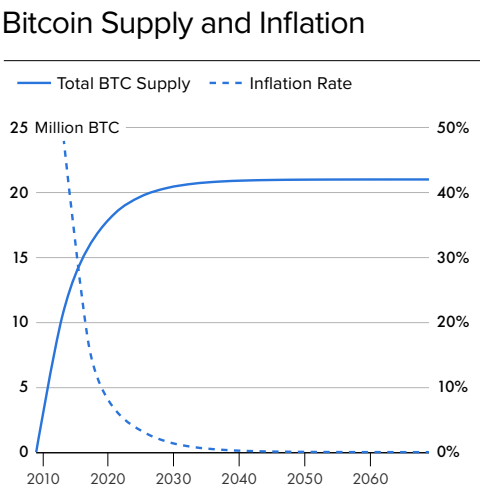
Grin's monetary policy sharply contrasts with that of Bitcoin's. GRIN monetary supply will exhibit linear absolute inflation with an unlimited total supply; the same amount of GRIN will be emitted at a constant rate forever—one new token per second. This makes the supply unlimited, whilst the inflation rate as a percentage of the total Grin in existence will tend to zero. This approach renders Grin 'closer to digital cash then digital gold', with an estimated 4% inflation rate in 25 years. Grin details the motivation for their monetary policy in their Github documentation, arguing that "sound money has more to do with transparent emission than a capped supply." Since a deflationary token issuance schedule, i.e. a decreasing amount of new tokens introduced over time, may incentivize holding tokens as speculative instruments in anticipation of their increasing in value (as supply is gradually outstripped by demand), such tokens (ie, Bitcoin's) might have difficulty finding use as an everyday medium of exchange.

Diagrams 3 and 4

Supply and Inflation in Grin and Bitcoin

Grin's monetary policy is diametrically opposed to Bitcoin's, and is intended to make the currency function more as digital cash than digital gold





Governance & Funding

Grin's governance system is broadly similar to Bitcoin's: no formal on-chain mechanisms, funding for developers, or rigid power structures. Many in the small team of Grin developers are anonymous, including the leader Ignotus Perevell. The core developers and community considered forming a foundation to coordinate development and funding efforts, but ultimately decided against it, citing the various issues that foundations for other projects have encountered.

Central amongst these problems is that foundation structures are perceived as concentrating power in a small minority, and, as such, are anathema to Grin's focus on decentralization. Instead, Grin has a technical council consisting of eight core developers, Ignotus Peverell, Antioch Peverell, Hashmap, Jaspervdm, Lehnberg, Quentin le Sceller (BlockCypher), Yeastplume (Michael Cordner), John Tromp and Gary Yu, that lead decision-making processes. There are no formal processes for appointing or removing these members, though discussions concerning a move to a more structured governance system are ongoing. Notably, this structure is similar to early Bitcoin development and the original cypherpunk movements, although Bitcoin's governance model went through a long era of being criticized as overly technocratic and too slow, among other things.

A potential drawback of this structure is the comparatively slow development pace of Grin; while the original MimbleWimble whitepaper was released in 2016, the Grin mainnet did not launch until early 2019. This structure is also contrasted notably by Beam, which has a VC-backed startup organizing development efforts—Beam's startup is funded by 20% of the ongoing block rewards.

In tandem with an informal governance structure, Grin uses a funding structure for development broadly similar to Monero's Forum Funding System. In the absence of an ICO, a pre-mine, or any portion of mining rewards being allocated to development, Grin solicits donations from community members for various causes, relying on participants' ideological alignment to realize a distributed MimbleWimble blockchain. Individual contributors can request funds for specific projects.

Grin also solicits funds from the community for a 'General Fund', which is a multi-sig wallet controlled by the Grin Technical Council. Speaking to the community-driven emphasis of the Grin project, donations for these causes often originate with various service providers and auxiliary businesses that benefit from Grin development. Soon after the launch in January 2019, entities such as the Grinmint mining pool, the Obelisk ASIC manufacturer, and the Poloniex exchange have all committed to donating a percentage of revenue or trading fees to the General

> In the absence of an ICO, a pre-mine, or any portion of mining rewards being allocated to development, Grin solicits donations from community members for various causes, relying on participants' ideological alignment to realize a distributed MimbleWimble blockchain.

Fund. While these businesses do not receive concrete remuneration for donating to this fund and are under no obligation to actually contribute the pledged amounts, they may view it as an efficient way to support the Grin ecosystem and drive revenue to their own core businesses lines of trading or mining hardware.

Grin vs. Key Crypto Projects

Relative to Beam

Unlike Beam, a company, Grin is an open-source, community funded project, which presents significant deviations in the two projects' funding and business models. Beam's emission schedule involves a block reward halving every four years and a long-run cap of approximately 263 million Beam; this is similar to Bitcoin's approach and distinct from Grin's. Beam uses a form of Equihash, Ethereum's PoW algorithm, and has also committed to hard forking the network early on in order to remain ASIC resistant. Additionally, Beam is exploring an auditability feature that would allow users to selectively disclose transaction histories, allowing Beam to remain compliant with existing or future regulations surrounding privacy coins.

Whilst Grin and Beam both have the significant upside of not requiring a trusted setup to provide private transactions, as ZCash does, transactions are not all of the same exact degree of privacy. Unlike Monero or Zcash, the extent that MimbleWimble-based transactions are obfuscated from sufficiently competent attackers is dependent on users being able to find simultaneous transactions to help obscure theirs. This is because Cut-Through transactions help preserve privacy insofar as there are other parties transacting, and Dandelion routing better obscures IP traffic when there is more traffic to work with.

Relative to Bitcoin

In Bitcoin, a new full node must replay every transaction since the genesis block to find the current chain state. Per the UTXO model, many transactions are effectively just refunds to the originator of the TX. All such data must be stored on chain. In Grin, these intermediate transactions are not stored on chain past the initial confirmation block, thus reducing total chain size. MimbleWimble does not achieve a meaningful increase in tx/s relative to BTC or similar traditional cryptocurrencies; in fact, confidential transactions are relatively resource expensive compared to simple transactions revealing information in a manner similar to BTC.

Grin utilizes a BTC-style UTXO transaction mode, except that amounts are hidden and not associated with addresses but rather are replaced by homomorphic commitments. Thus, Grin's approach requires considerably less storage than a Bitcoin blockchain that were to implement Confidential Transactions, though it is unclear if Grin will be a smaller blockchain than the currently implemented Bitcoin. Grin has estimated a total size of less than 2GB for a Grin chain with ten million transactions.

Diagram 5

Comparison of Publicly Auditable Information

Grin's more minimal declare set creates both ease of verification and privacy advantages compared to Bitcoin, yet poses unique challenges to usability.

Bitcoin Block Declares	Grin Block Declares
• Block Height • Previous Block Hash • Nonce • Fees • Reward + Number of Transactions + Transacting addresses (Send/Receive) + Transaction Amounts	• Block Height • Previous Block Hash • Nonce • Fees • Reward

Relative to Monero

Grin resembles Monero in several respects, including its default privacy functionality and intention to minimize the influence of ASIC miners on the network. Neither protocol relies on a trusted setup (such as zCash) in order to ensure transaction privacy. The issuance schedules are subtly different: Grin has a constant inflation of 1 Grin/sec in perpetuity, Monero uses a deflationary schedule, similar to Bitcoin, up until the issuance of 18. 132 million tokens, after which 0.3 XMR are created every minute for as long as the network operates.

Grin: A Commentary from S+C Research

In this section, Brant Downes of Smith + Crown offers his perspective and commentary on Grin, the narratives surrounding it, and how the community so far has been approaching it.

Grin as a protocol vs. Grin as a narrative

While the previous section considered Grin alongside several peer cryptocurriences, it is also useful to consider Grin within the context of the broader industry. While in the eyes of many, Grin is among the most widely discussed and eagerly anticipated projects to have launched in several years, a number of prominent narratives have also developed in relation to Grin, and arguably MimbleWimble more broadly. Considering these narratives provides both a more complete understanding of Grin's place in the larger blockchain ecosystem and useful insights into the evolutions of the broader industry as well.

Central amongst these narratives are the matter of Grin's supposed fair launch, the supposed $100 million reported to have been invested into GRIN mining operations by venture capital, and perhaps most substantially, the question of Grin's supposed philosophical similarities with Bitcoin itself. While each of these could easily be the subject of very extended treatment given the number of critical issues each touches upon, merely a cursory examination is sufficient to spark thoughtful reflections that help situate Grin alongside peer cryptocurrencies and provide meaningful observations on its place within a broader, evolving cryptocurrency ecosystem.

Grin as a Philosophical Successor to Bitcoin?

One of the most interesting arguments related to Grin concern its supposed role as philosophical successor to Bitcoin. From a certain perspective, a number of similarities can indeed be observed, yet upon closer inspection many of these claims actually appear to be quite superficial. The reality is not merely that a description of Grin as a successor to Bitcoin is likely misleading. That Grin can even be described as such can be seen as a revealing commentary upon the ways in which the cryptocurrency ecosystem has evolved in the years since Bitcoin's launch.

In terms of the apparent ways in which Grin can be considered a philosophical successor to Bitcoin, there are indeed several. For instance, just as Bitcoin was launched by an anonymous individual who bootstrapped the project through launch, Grin itself was launched by an anonymous team of developers without any fundraising

events or presales. The lack of a premine, founders allocation, or any other advantage to Grin's developers is also identical to Bitcoin's unveiling and initial mining. Even Grin's privacy focus can be viewed as embodying the spirit of Bitcoin, which was itself understood to represent a private, anonymous currency at the time of its launch.

> One of the most interesting arguments related to Grin concern its supposed role as philosophical successor to Bitcoin. From a certain perspective, a number of similarities can indeed be observed, yet upon closer inspection many of these claims actually appear to be quite superficial.

While these similarities are evident and real, and clearly do suggest a significant inspiration from Bitcoin's own history, a closer examination also reveals enough differences between the two that it remains difficult to realistically consider Grin as Bitcoin's true successor in the most important functional sense. The primary reason for such an argument concerns the different economics of the two projects and the implicit comment these differences make relative to the outlook of their creators.

Bitcoin, created with a fixed supply of 21 million bitcoin, is considered to have been inspired by The Austrian School of Economics, and appears to have been at least partly inspired by anger at the bank bailouts associated with the financial crisis of 2008. The text embedded in Bitcoin's genesis block, referencing a January 2009 article on a proposed second bank bailout, is widely considered to have been a statement of protest against the flexibility of fiat currencies, where governments and bankers could expand monetary supplies at their discretion. It would appear that Bitcoin's own approach was shaped by the widespread sentiment during and after the financial crisis, that bank bailouts were recklessly expanding money supplies, and that Bitcoin's fixed token supplies would act, much like the gold standard had previously, to ensure the responsible governance of the currency. This view of the value and legitimacy of cryptocurrencies as fundamentally deriving from their fixed supply and unalterable monetary policies has subsequently come to be seen by many as a core aspect of Bitcoin's appeal.

Contrasted with Bitcoin's ultimately deflationary approach—deflationary because bitcoin supplies, once they have reached their ultimate supply, cannot be subsequently emitted, even if economies and the supply of bitcoin holders expands—Grin has a fundamentally different economic proposition. That is, Grin's own money supply calls for the emission of one coin per second, or 60 per minute, in perpetuity. While it might be claimed that at least Grin's supply is predictable, fulfilling at least one portion of Bitcoin's

foundational objective, the endless inflation of Grin's money supply represents a vision of currency management and emissions that is in effect diametrically opposed to Bitcoin's approach, as well as the views of much of the early cryptocurrency community.

While a few criticisms of Grin for precisely this fundamental divergence in monetary policy have been noted, the numerous suggestions that Grin represents an updated and improved version of Bitcoin that equally addresses a number of Bitcoin's perceived shortcomings, can be considered to signal two realities. One is a surprising disregard for the importance of monetary policy in comparing distributed digital currency protocols. Another is an effective shift in values across the community as much of the original vision that inspired Bitcoin's adherents to consider themselves a particular counterculture community is being supplanted by a more pragmatic group of experienced financial professionals. This new group, rather than seeing crypto as a unique community or subculture, often view cryptocurrencies as just another asset class within a larger market and financial ecosystem.

Without making a value judgement relative to this transformation—a transformation that is plain to see whether in the context of exchange traded Bitcoin futures, trading and custody solutions under development by Fidelity, or JPMorgan's own efforts to develop an in-house cryptocurrency—this episode highlights a transition in the spirit and vision of the community. This transformation, and the thinking that has allowed it to go largely unnoticed, is also apparent when considering another of the major themes relevant to Grin, that of discussion around the so-called fairness of Grin's launch and token distribution.

What is a "Fair Launch"

The question of GRIN's launch has been the subject of a number of commentaries, and the discussion undoubtedly has both a practical and a nostalgic element. This is a practical issue because the nature of a cryptocurrency's launch can have tremendous impacts on future evolutions, thus the structures and mechanics of launches do matter. It is also a nostalgic issue because, while many recent token launches have seen a variety of curious, questionable, and sometimes unsavory practices including huge raises for untested projects, excessive allocations to insiders, or discounted sales to early or otherwise 'strategic' supporters, these are often contrasted with Bitcoin's ostensibly 'pure' launch, where anyone could have mined BTC alongside of and on an equal footing with Satoshi from the earliest blocks. In reality, such comparisons are more than a little simplistic. They might even be considered anachronistic, selectively retelling the story of Bitcoin's origins while offering little value in accurately understanding where the industry stands today.

> The point is that 'fairness' in the historical context in which Bitcoin was launched—no exchanges, no market price on Bitcoin, no billion dollars in aggregate value no pre-existing global mining infrastructure, no VCs scouring the industry for investments—cannot be recreated even if it were universally considered ideal.

While most such discussions of fair launches are favorable to Grin, considering it to be a very fair launch that calls to mind Bitcoin's own launch, it might equally be said that such discussions overlook important points. One is the very real issue of how ensuring funding for a cryptocurrency's continuing development arguably represents an important step in attracting followers, purchasers, users, and investors willing to confidently hold a cryptocurrency. Ensuring the continued development of a cryptocurrency is equally a question of responsibility towards users who may be exposed to substantial losses should a blockchain or cryptocurrency actually fail. It is worth noting the irony in this: the lack of dedicated developer funding was a long standing criticism of Bitcoin, inspiring protocols like DASH and Decred to allocate a portion of mining rewards to fund ongoing development, ZCash to implement a founder's wallet, and various protocols to implement premines specifically to developers.

The question of the supposed fairness of Grin's launch is a delicate issue because it can be argued that 'fairness' is being judged both abstractly and within a context of Bitcoin looming as an idealized model of how a currency ought to be launched. While neither perspective is necessarily incorrect or inappropriate, such comments also implicitly illustrate a number of tensions and inconsistencies that shape the way many think about cryptocurrencies more broadly.

Descriptions of these comparisons are highly subjective because Bitcoin, as the foundational cryptocurrency, was launched into a context where it had no value, a very modest community, and only gradually attracted curious miners. Likewise, mining was open to all followers because, in effect, there was no large-scale competition to mine what was merely a proof-of-concept project without value. In such a setting, the selflessness of the approach was less a choice than an obligation. Thus while it is admirable that Grin in a certain sense employed a similar approach of effectively equal and 'fair' access, legitimate questions related to the responsibilities inherent in deploying a new blockchain also exist. For instance, is launching a new blockchain in a manner that does not create structures for funding and supporting ongoing development, in effect institutionalizing a dependance upon donations and general goodwill, an effort that can be considered truly fair in the way Bitcoin's argument is? The point is that 'fairness' in the historical context in which Bitcoin was launched—no

exchanges, no market price on Bitcoin, no billion dollars in aggregate value no pre-existing global mining infrastructure, no VCs scouring the industry for investments—cannot be recreated even if it were universally considered ideal.

Moreover, from the perspective of potential purchasers, including those who may be unaware of an absence of funding structures, and who may find themselves suffering losses if ever Grin is unable to continue as a viable project as a result of lack of donations to fund necessary development, is this unquestionably a 'fair' model?

Rather than lauding Grin as a 'fair' launch according to an imprecisely defined set of terms that may not, as suggested, fully capture the various ways in which 'fairness' may be measured, the real evaluation metric for launches might be viewed somewhat differently. If, for example, one establishes the long-term survivability of a blockchain as a necessary consideration even relative to the launch format and structure, and considers this as a fundamental element of 'fairness' relative to that blockchain's users and stakeholders, then perhaps the important comparison becomes one between a corporate model of a launch and a more informal, open-source, loosely organized launch. If this perspective is chosen then Grin's fellow MimbleWimble-based cryptocurrency BEAM represents an excellent contrast.

Grin + BEAM?

BEAM, launched in early 2019 and led by CEO Alexander Zaidelson, is structured as a corporation that held a pre-sale to raise initial funds for the project. Bearing a certain similarity to ZCash, also a corporation, BEAM established a foundation to guide its operations, while also retaining for itself a 20% block reward founder's tax intended to fund initial development. Beam's centralized organization includes defined management and engineering teams. The decision by BEAM leader's to retain a deflationary monetary policy with a fixed total supply similar to Bitcoin, and a decision to develop an auditable wallet intended to appeal to corporate or business groups maintain verifiable records suggests a clear focus on establishing BEAM's user base, and likely its price appreciation as well.

But while these differences have been noted, discussions of these two MimbleWimble implementations tend towards the comment that 'time will tell which triumphs', a view that clearly presupposes a conflict or competition. While Grin and BEAM are indeed based upon interpretations of MimbleWimble, they have considerably different objectives, and only a simplistic understanding of the industry that ignores the role of monetary policy could overlook this in a way that would allow them to be considered competitors. Grin, given its high inflation rate, is clearly targeting a role as a transactional currency, supported by its inbuilt privacy functions. Beam, with an inflation rate identical to Bitcoin's, is assuming its deflationary economics will encourage holding as a store

> While Grin and BEAM are indeed based upon interpretations of MimbleWimble, they have considerably different objectives, and only a simplistic understanding of the industry that ignores the role of monetary policy could overlook this in a way that would allow them to be considered competitors.

of value. A careful observer might easily wonder whether these two privacy-focused cryptocurrencies, one structured to represent a useful medium of exchange and the other a long-term store of value, might not be entirely complementary?

In such a view, the question of the structure around the launch can also be seen differently. For instance, while the idea of a crowdfunded cryptocurrency with no advantage to insiders has an intuitive appeal, questions about how development will be supported remain critical. The recent incident where Ignotus Peverell criticized the Grin community for not providing sufficient support to allow Grin developer YeastPlume to work full-time on Grin illustrates the potential pitfalls of this approach, where even the most basic development tasks do not have assured funding. While arguably not inappropriate for a cryptocurrency intended to serve primarily as a medium of exchange, for users could simply switch to another medium of exchange token should Grin ever fail, such a model would be rather disconcerting for a cryptocurrency such as BEAM which is deliberately intending to serve as a long-term store of value. Might it not be preferable to ensure the long-term viability of a token intended to fulfill a long-term currency role via a well-funded development strategy? In such a case, is not BEAM's model of a centralized company ensuring the development of a currency in which it also receives payouts and financial support a more appropriate model? There is not necessarily a definitive answer to such concerns, but the questions are significant enough to merit serious consideration.

The above suggests the question of fairness or appropriateness of launch approaches may be less of a philosophical one related to the supposed fairness of a launch, but a question of the appropriateness of a launch structure relative to a token's long-term intended role and functions. While it may be too strong to accuse the community of an excessively narrow manner of considering this question, it certainly is the case that more expansive consideration of the question might have yielded different conclusions.

Interestingly, this question of appropriately considering a token's long-term prospects and viability can also be seen as highly relevant to another of the major narrative structures surrounding Grin, that of the supposed millions invested in the mining of the currency. The question is relevant because while it highlights the importance of correctly understanding a currency's long-term role before developing additional

hypotheses about a currency, turning this approach to narratives surrounding Grin's mining situation is also a useful exercise.

Smoke, Mirrors, and Misconceptions Surround Grin Mining Rumors

While Grin has garnered significant attention as an eagerly awaited launch, one widely seen as being an especially fair one, it has equally garnered significant attention as a result of rumors that more than $100 million was invested in establishing mining operations targeting this new blockchain. The insinuation appears to be that only an especially promising blockchain, one likely destined for considerable price appreciation, would motivate such actions. Given that venture capital is widely regarded as smart money that is tuned into the best opportunities, this further reinforces the sense of anticipation and expectation regarding Grin. The widespread sentiment, noted above, that Grin can also be considered the philosophical successor to Bitcoin, only compounds the sense of opportunity and expectation surrounding Grin.

> In terms of actual evidence of this supposed $100 million plus invested in Grin mining operations, it must be acknowledged that all are sourced from one blog comment that has since simply been repeated numerous times.

But two important questions arise when considering this supposed VC investment in Grin mining capacity. The first and most obvious is to ask whether this actually occurred, and what meaning should be ascribed to this did it occur. The second is whether if, as suggested above, considering Grin as the successor to Bitcoin is a slightly dubious proposition, does this undermine the premise that likely informed this investment. If so, this further complicates the vquestion of what Grin's actual prospects may be.

In terms of actual evidence of this supposed $100 million plus invested in Grin mining operations, it must be acknowledged that all are sourced from one blog comment that has since simply been repeated numerous times. Assuming this source to have been correct and not merely an attempt to shape a narrative, an already generous assumption given the virtual impossibility of proof, there nevertheless remain numerous questions. Was this, for instance, newly committed capital, or simply repurposed machines? Conceivably, this 'spend' merely refers to an allocation of previously paid for and idled machines towards Grin mining, one that suggests a considerably less enthusiastic view of Grin's prospects than breathless accounts of over $100 million in newly purchased machines being allocated towards Grin-specific infrastructure.

Ultimately, if a group truly considered Grin to represent an outstanding opportunity, one meriting millions in investment in mining operations in a 'fairly launched' coin offering tremendous prospects but also no easy route for VC investors to accumulate positions ahead of the public, would such a group not be incentivized to remain discrete regarding their supposed investment? From this perspective one cannot help but wonder if rumors of Grin mining investment were not merely attempts to create secondary market demand on the part of whoever already had mining positions, and a need to sell accumulated coins in order to cover their expenses related to establishing and operating a mining operation.

But even if one concedes that $100 million in new spending was allocated towards Grin mining, other significant questions also remain. If, as suggested above, Grin's monetary policy effectively disqualifies it from consideration as Bitcoin's philosophical successor, might this also be relevant to expectations surrounding Grin's price prospects? Given Grin's unique monetary policy, with continual inflation, and its focus on acquiring a role as a transactional, means-of-payment cryptocurrency, it is unclear why a similar price trajectory to Bitcoin's might be anticipated.

Even were Grin to capture widespread use as a transactional cryptocurrency, the question of no checks on Grin's velocity suggest no compelling argument as to why price escalation would be anticipated or could be forecast as a function of network activity. In this case, and already having established that Grin is unlikely to acquire a store of value role in the sense that Bitcoin may have, the lack of compelling arguments for why Grin would escalate in price beyond mere speculation may ultimately prove problematic for any miners who allocated capital spending towards establishing Grin mining operations. Given the absence of knowledge regarding whether this supposed $100 million in spending towards Grin mining operations actually occurred it is impossible to forecast what the impacts might be upon the Grin mining ecosystem, but this question certainly merits close observation. In the worst case of no appreciation and miners facing debt burdens being forced to shut down operations, the network's hash power could itself be reduced, potentially to the point of putting at risk the network's viability. At a minimum, exposure to 51% attacks could be significantly increased, with potentially highly negative impacts on Grin's prospects.

What is clear is how this consideration of the narratives surrounding Grin, and especially how many of them suffer from some considerable shortcomings resulting from lack of careful analysis, reinforces the importance of carefully considering the circumstances surrounding the different blockchains and cryptocurrencies into which one may invest or otherwise employ for some service or function.