Pirate Chain: Anonymous Digital Cash

Privacy Focused Decentralized Network

Enforced Encrypted Peer-to-Peer Transactions

Version 3
March, 1st 2022

Abstract

Pirate Chain is a privacy focused digital cash network that enforces shielded only Peer-to-Peer (P2P) transactions. Interactions between peers are encrypted using zero-knowledge, Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) which eliminate the information shared in a typical pseudonyms transparent transaction such as the sender's address, the receiving address, amount, and transaction history. This requirement solves the issue of unintentional metadata being leaked when using transparent addresses which could allow an observer to link transactions and identities.

By enforcing shielded P2P transactions, no previous transaction history is revealed. On the Pirate Chain network, this solves the problem of "tainted" coins which is defined as a transaction balance having a transaction history linked to black listed or otherwise undesirable addresses that may cause exchanges or other entities to refuse or devalue otherwise legitimate transactions. For this reason, Pirate Chain's native currency (ARRR) is 100% Fungible and functions as a digital cash.

1. INTRODUCTION

As cryptography based digital currencies continue to gain wide spread adoption, they are proving their resilience to attacks and lead us to new discoveries in what may be possible with blockchain technology. Public trust in these decentralized networks is increasing as more individuals and institutions participate in the space. New projects are being introduced at an accelerated rate that build on the foundations created by the early design with the intention to solve real problems in new and innovative ways.

The original reference design of bitcoin is built upon a transparent public ledger, as are many of the subsequent major networks. With each transaction, the sender reveals to the recipient their entire transaction history and balances. In the past, pseudo anonymity was sufficient for miners that were not required to reveal their identity to acquire the network's coin and were able to mine to unique addresses. Since cryptocurrencies have become widely adopted, it is now most common to acquire a particular coin through the public market. In recent years we have witnessed the growth of blockchain analytic companies that monitor networks to reveal a transaction's full history, and ultimately link all those transactions to the identities that have interacted in that history chain.

Pirate Chain was created to protect the privacy of its users by requiring peer-to-peer transactions be shielded by default. To an outside observer, not only are the important details of the transaction encrypted (viewable only by the sender and receiver), but all transactions appear identical. The observer knows a message was sent on the network, but they cannot know who it was meant for, who sent it, or the amount. The anonymity set therefore grows with every unspent transaction on the ledger.

Because of increased regulation and clarity of transaction history through advanced chain analysis, if a transaction has a history that includes an address that is blacklisted or has been linked to nefarious acts or identities, that balance may be rejected or have a decreased value. A user may unknowingly receive a payment that includes such history and be stuck with valueless, non-fungible coins. Pirate Chain solves this problem by removing all transaction history from every Peer-to-Peer transaction, any transaction made on the network is identical to the outside viewer. Being 100% fungible means each ARRR in an address is identical to every other ARRR on the network, strengthening the overall privacy even further as it grows and gains adoption.

2. PIRATE CHAIN ORIGIN

Pirate Chain is an asset chain of the Komodo platform ecosystem. “The Komodo platform focuses on empowering blockchain entrepreneurs and the average cryptocurrency user with freedom and ease of use through blockchain technology” (jl777c, founder and head developer of Komodo Platform, 2018). An asset chain is a Komodo run-time fork that inherits the source code’s features and is a complete independent blockchain. Komodo itself is a highly modified fork of Zcash. the Zcash project is a fork of Bitcoin. Thus, all the features designed by Satoshi Nakamoto in the Bitcoin protocol, as well as the zk-SNARK implementation of Zcash, and the improvements by the Komodo platform are all the source code Pirate Chain builds upon.

Pirate Chain was created on the 29th of August, 2018 in a Discord conversation as a theoretical chain concept that leverages required encrypted, shielded transactions utilizing zk-SNARK proofs with no optional transparent end points meant to solve fundamental privacy issues observed in other projects. The development work of jl777c on Komodo Asset chains enabled the ability to enforce shielded transactions in a new asset chain (Grewal 2018) which would become known as Pirate Chain.

While Pirate Chain initially began as a proof-of-concept, the community quickly realized its potential after jl777c successfully implemented delayed proof-of-work making Pirate Chain feature complete, the first blockchain in the industry to to have enforced shielded P2P transactions based on the zk-SNARK methodology, and notarized into a Bitcoin equivalent security chain protecting against 51% attacks.

3. NETWORK PARAMETERS

Pirate Chain enforces the following network rules and technical features:

Mining algorithm:	Equihash Proof-of-Work
51% attack security:	Delayed Proof-of-Work
Average block interval:	60 seconds
Standard transaction fee:	0.0001 ARRR
Transaction signing:	< 1000ms
Transactions per second:	31 TPS
Payments per transaction:	Up to 100
Maximum block size:	4MB
Typical transaction size:	*Coinbase reward*: 184 Bytes *dPOW notarization*: 1669 Bytes *P2P Transaction:* 2373 Bytes
Block Halving:	Every 388,885 blocks (~270 days)
Maximum Supply:	200 Million (199,109,119.994205)
Removed from Circulation:	1,294,335 (locked in Sprout Pool)
Founder’s Fee / Block Tax:	0%
Premine:	None
Central Authority:	None
Capital Investors / loans:	None
Governance:	Autonomous Community Project

4. COIN DISTRIBUTION AND ACCELERATED EMISSION

Pirate Chain is a fair launched community created project. There is no premine, no founders fee, and no block tax. There is no central promoter or issuing authority. The total coin supply will come into existence through public mining rewards outlined in the Emission Schedule.

The Emission schedule begins with a coinbase reward of 256 ARRR for each mined block. The reward amount will be reduced by 50% every 388,885 blocks (approximately ~270 days) until a reward amount of 1 arrrtoshi in approximately the year 2043+.

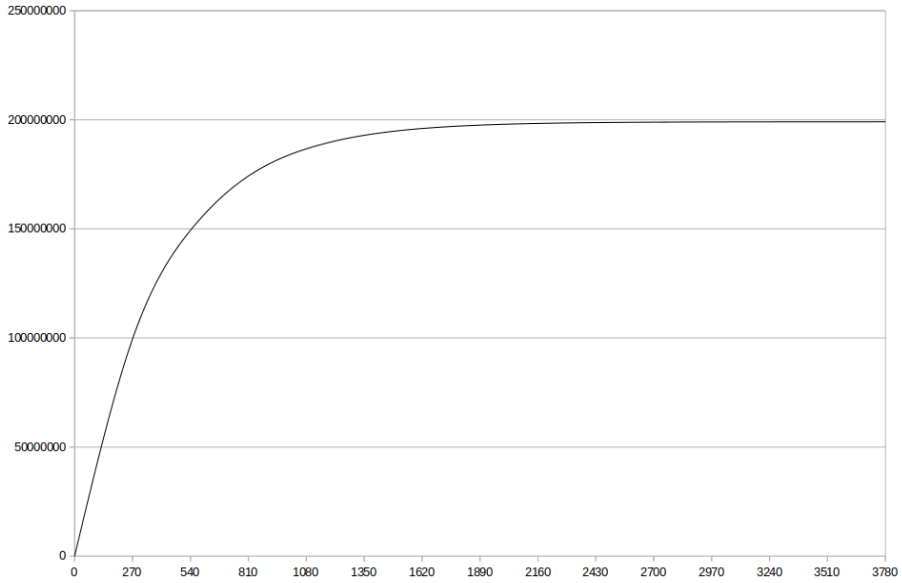

Figure 1: Pirate Chain Initial Coin Emission Chart

NOTE: In December of 2018 Pirate chain was upgraded and a new shielded address pool was added. Previously all transactions were shielded in the Sprout address pool. There was a forced migration to the Sapling pool that completed February 15th 2019. Although the community donated personal funds to those that missed the deadline, all remaining funds in the Sprout address pool are now locked and permanently removed from circulation. The total amount locked is 1,294,335 ARRR.

Era	Coinbase Reward	Start Block	Block Quantity	End Block	Era Total Rewarded	Cumulative Supply
1	256.00000000	0	388885	388884	99554560.0000	99554560.000000
2	128.00000000	388885	388885	777769	49777280.0000	149331840.000000
3	64.00000000	777770	388885	1166654	24888640.0000	174220480.000000
4	32.00000000	1166655	388885	1555539	12444320.0000	186664800.000000
5	16.00000000	1555540	388885	1944424	6222160.00000	192886960.000000
6	8.00000000	1944425	388885	2333309	3111080.00000	195998040.000000
7	4.00000000	2333310	388885	2722194	1555540.00000	197553580.000000
8	2.00000000	2722195	388885	3111079	777770.000000	198331350.000000
9	1.00000000	3111080	388885	3499964	388885.000000	198720235.000000
10	0.50000000	3499965	388885	3888849	194442.500000	198914677.500000
11	0.25000000	3888850	388885	4277734	97221.2500000	199011898.750000
12	0.12500000	4277735	388885	4666619	48610.6250000	199060509.375000
13	0.06250000	4666620	388885	5055504	24305.3125000	199084814.687500
14	0.03125000	5055505	388885	5444389	12152.6562500	199096967.343750
15	0.01562500	5444390	388885	5833274	6076.32812500	199103043.671875
16	0.00781250	5833275	388885	6222159	3038.16406250	199106081.835938
17	0.00390625	6222160	388885	6611044	1519.08203125	199107600.917969
18	0.00195313	6611045	388885	6999929	759.54101563	199108360.458984
19	0.00097656	6999930	388885	7388814	379.77050781	199108740.229492
20	0.00048828	7388815	388885	7777699	189.88525391	199108930.114746
21	0.00024414	7777700	388885	8166584	94.94262695	199109025.057373
22	0.00012207	8166585	388885	8555469	47.47131348	199109072.528687
23	0.00006104	8555470	388885	8944354	23.73565674	199109096.264343
24	0.00003052	8944355	388885	9333239	11.86782837	199109108.132172
25	0.00001526	9333240	388885	9722124	5.93391418	199109114.066086
26	0.00000763	9722125	388885	10111009	2.96695709	199109117.033043
27	0.00000381	10111010	388885	10499894	1.48347855	199109118.516521
28	0.00000191	10499895	388885	10888779	0.74173927	199109119.258261
29	0.00000095	10888780	388885	11277664	0.37086964	199109119.629130
30	0.00000048	11277665	388885	11666549	0.18543482	199109119.814565
31	0.00000024	11666550	388885	12055434	0.09271741	199109119.907283
32	0.00000012	12055435	388885	12444319	0.04635870	199109119.953641
33	0.00000006	12444320	388885	12833204	0.02317935	199109119.976821
34	0.00000003	12833205	388885	13222089	0.01158968	199109119.988410
35	0.00000001	13222090	388885	**13610974**	0.00579484	**199109119.994205**

Table 1: Pirate Chain Coin Supply Distribution Schedule

The nature of an emission schedule with a diminishing block reward creates a condition for scarcity, a necessary requirement for sound money. To measure this, we refer to scarcity in terms of stock-to-flow ratio. Stock is the amount of the asset available in the world, and Flow is the annual production rate. Stock to flow ratio is a measure of abundance, mathematically the amount of a commodity held in inventories divided by the annual production. Bitcoin (56:1 S/F), like gold (65.9:1 S/F), are favorable commodities

with high monetary value due to their high stock-to-flow ratio, unlike consumable commodities such as copper which has relatively lower stock to flow ratios.

Halving	Rewards	ARRR Emission (Flow)	ARRR Supply (Stock)	Stock To Flow	Annual Supply Inflation
Genesis	256	99554560	99554560	1.0	100.000%
post-halving 1	128	49777280	149331840	3.0	50.000%
post-halving 2	64	24888640	174220480	7.0	16.667%
post-halving 3	32	12444320	186664800	15.0	7.143%
post-halving 4	16	6222160	192886960	31.0	3.333%
post-halving 5	8	3111080	195998040	63.0	1.613%
post-halving 6	4	1555540	197553580	127.0	0.794%
post-halving 7	2	777770	198331350	255.0	0.394%
post-halving 8	1	388885	198720235	511.0	0.196%
post-halving 9	0.5	194442.5	198914677.5	1023.0	0.098%
post-halving 10	0.25	97221.25	199011898.8	2047.0	0.049%
post-halving 11	0.125	48610.625	199060509.4	4095.0	0.024%
post-halving 12	0.0625	24305.3125	199084814.7	8191.0	0.012%
post-halving 13	0.03125	12152.6875	199096967.4	16383.0	0.006%
post-halving 14	0.01563	6076.359375	199103043.7	32766.8	0.003%
post-halving 15	0.00781	3038.1875	199106081.9	65534.5	0.002%
post-halving 16	0.00391	1519.097656	199107601	131069.7	0.001%

Table 2: Pirate Chain Stock-to-Flow and Annual Supply Inflation Table

With its accelerated Bitcoin-like emission schedule, Pirate Chain reaches a high Stock-to-Flow ratio becoming more scare than Bitcoin and gold after its 6th halving. Simultaneously, Pirate Chain will have an annual supply inflation rate lower than Bitcoin and below 1% for the remainder of its distribution, encouraging its use as a digital cash.

Typical stages of coin maturity in depreciating flow vs increasing stock (halving) assets:

BULK DISTRIBUTION STAGE | High Supply Inflation | Low Stock-to-Flow
Majority of asset distributed. Circulating supply exceeds demand

MIDDLE STAGE | Reducing Supply Inflation | Increasing Stock-to-Flow
Demand increases and supply inflation reduces while asset matures as a Store-of-Value

MATURITY | Distribution Complete | Infinite Effective Stock-to-Flow
The supply distribution has completed as the asset transitions from a Store-of-Value to a useful Medium-of-Exchange

To achieve the design objective of a fungible *digital cash*, it is desirable for Pirate Chain to maintain a fair period of distribution through the supporters of the network (mining nodes), while transitioning from a Store-of-Value to a Medium-of-Exchange achieving maturity in the most sensible period of time.

5. TRANSACTIONS

The initial coinbase reward to the miner of a block is transparent for supply audibility. From that point on, all Peer-to-Peer transactions of the Pirate Chain network are required to be shielded. The details of the transaction are encrypted meaning no outside observer can know the sender, receiver, quantity of ARRR, or the optional message stored in the memo field. Every subsequent transaction is verified by the network utilizing the zk-SNARK methodology developed by Zcash to prove the ARRR quantity of the inputs always equal the ARRR quantity of the outputs, proving no new coins have come into existence despite being a shepherded transaction.

Transparent P2P transactions are not allowed as a fundamental parameter of the Pirate Chain network. In networks where transparent addresses are allowed, a condition is created where the end points are observable. For example, when an amount publicly visible on a ledger is sent from a transparent address to a shielded address, the amount is no longer visible. However, if that same amount is later unshielded to a transparent address, it now becomes possible (with advanced chain analysis) to have a high probability linking these transactions, despite being shielded at some point. Pirate Chain solves this as all P2P transactions have shielded end-points, leaving no meaningful way to link transactions on the distributed ledger.

The sender of a shielded transaction is further protected as the receiver can only know the amount and their own receiving address (senders address is not revealed). If an audit of an account is required, viewing keys may be generated which allows viewing of the transactions and balances for an address.

EXCEPTIONS. *There are specific exceptions to the shielded transaction rule. All coinbase rewards are transparent. The first transaction of a coinbase reward is required to be sent to a shielded address.*

DPOW transactions are required to be transparent to support notarization functionality into other chains. Komodo notary nodes are elected by the community. Their public keys are whitelisted in the source code for the election period allowing them to complete notarization tasks. This process does not reduce the privacy of any other transactions on the network or affect decentralized consensus in any way.

Further, there are certain integrations in the network that allow functionality, such as arrrtomic swaps via the AtomicDex exchange, which creates a temporary disposable P2SH multisig address to perform atomic swap.

6. DELAYED PROOF OF WORK (dPOW)

Delayed Proof-of-Work is a native feature of the Komodo platform that notarizes a “snapshot” into other PoW blockchains. It provides a unique and innovative form of security which is as strong as the network it attaches to, yet does not require the cost to run that network. Delayed Proof-of-Work is a solution that utilizes multiple existing methods into a single hybrid consensus system that is as energy efficient as Proof-of-Stake (PoS), while being secured by Litecoin’s Proof-of-Work. Users who build independent blockchains (asset chains) in the Komodo ecosystem can choose to have a block-hash serving as a “snapshot” of their own blockchain inserted into the Komodo main chain. In this manner, the records of the asset chain are indirectly included in the block-hash of Komodo that is pushed onto the blockchain of Litecoin. To 51% attack the Pirate Chain, an attacker would need to simultaneously control the hashpower of Pirate Chain, Komodo, and Litecoin.

The dPoW notarization service allows blockchains to benefit from Litecoin's hash-rate and this in turn makes Litecoin's power usage more eco-friendly as it is securing the entire ecosystem of dPoW in addition to itself (Jl777c 2016). Other than Pirate Chain, dPoW has been successfully implemented in a large number of asset chains such as Game Credits, Einsteinium (EMC2) and Pungo among others (Komodostats 2018).

The Komodo security service is performed by notary nodes which are needed to record block-hashes onto the Litecoin blockchain, referred to as notarization (Figure 2). Notarization entails the creation of a group signed Litecoin transactions containing the most recent block-hash of Komodo, signed by an unknown combination of 13 of 64 notary nodes (Jl777c 2016). Block-hashes of Pirate Chain (among other asset chains) are inserted in the Komodo blockchain in a timely fashion as well, using the same method. In this manner, even a single surviving copy of the Komodo main chain will allow the entire ecosystem of asset chains to overwrite and overrule any of an attacker’s attempted changes.

The notary nodes pay the Litecoin transaction fee for notarizing the Komodo block chain using funds provided by the Komodo Platform. Notary nodes are compensated for their work by mining KMD blocks at a CPU difficulty, receiving the block rewards and transaction fees. It is therefore expected that the financial interests of the stakeholders, is to be voting for notary nodes that the stakeholders value. 64 largely distributed notary nodes are up for election and are expected to be an optimal representation of a decentralized ecosystem making any type of 51% attack highly improbable.

In order to reorganize and attack the Pirate Chain the attacker would need to destroy:

- *all existing copies of the Pirate Chain;*
- *all copies of the Komodo main chain;*
- *the PoW security network (Litecoin) into which the Komodo blockchain notarized data is inserted.*

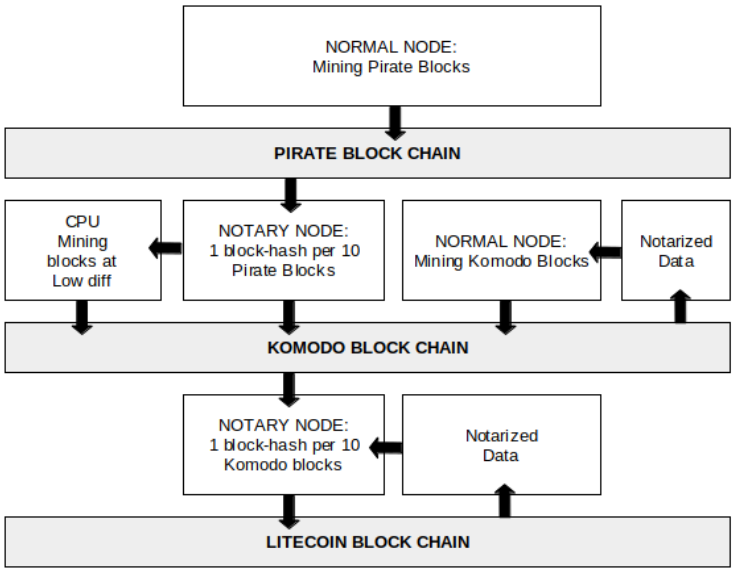

Figure 2: A block schematic representation of delayed Proof-of-Work.

Furthermore, notary nodes have the freedom to switch the notarization process to another PoW network if a shift in hash rates between the large blockchains occurs in the future, adding additional security through adaptability. Delayed Proof-of-Work provides Pirate Chain with a high level of Proof-of-Work security, while avoiding the eco-unfriendly use of scarce resources, and the excessive financial costs of running the security network itself.

7. ANONYMITY SET

A anonymity set is the size of of a pool of data that is indistinguishable. In a CoinJoin transaction with three equal inputs, and three equal outputs, the effective anonymity set is three. Because all P2P transactions of the Pirate Chain network are encrypted, all unspent transactions are identical. Therefore, every unspent transaction of the Pirate Chain network effectively increases its anonymity set, making all other transactions more private. Pirate Chain has one of the highest anon-sets for a privacy based cryptocurrency.

8. PRIVACY

As outlined in the original Bitcoin white paper, the traditional banking system achieves a level of privacy by limiting access to information to the parties involved, and the trusted third party. Identities are directly tied to transactions. The Trusted Third Party relays these transactions to the Counter party. You must trust the Trusted Third Party to not reveal more information than needed to the counter party. Because no public ledger is used, the public doesn't know the details of these transactions, but you must now trust that the trusted third party and counter party do not reveal to the public any of the details they now possess.

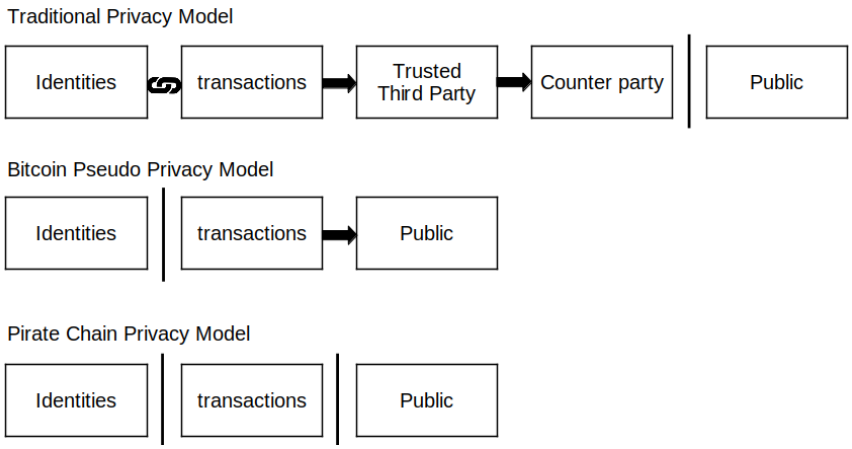

Figure 3: Privacy Model Flow Chart

In Bitcoin's Pseudo Anonymous Privacy Model, which reflects the majority of the transparent networks, the ledger is viewable by the public. Therefore, all transactions and their details are public knowledge. These transparent chains achieve pseudo anonymity as long as a real identity is not linked to an address or transaction. Once a real identity is connected, all previous transactions on the ledger, and all future transactions can then be linked through chain analysis as the ledger persists for the history of the network.

Pirate Chain's Privacy Model provides full anonymity as Peer-to-Peer transactions are required to be shielded. In the case that an identity is connected to any particular transaction, no other information is revealed as all other transactions on the public ledger are shielded. For example, if Bob provides a receiving address to Alice so she may pay him, she cannot know any other transactions to the address and no balances are revealed.

To ensure full privacy, a receiving address should not be provided to more than one trusted sender. For example, Alice provides a receiving address to Bob and anonymously to Charlie. Bob knows the address belongs to Alice, but Charlie does not know who it belongs to. If Bob and Charlie collude, Charlie will now know the address belongs to Alice. While no other information is revealed, to prevent 3rd part collusion a unique receiving address should be provided to separate parties.

9. REFERENCES

Bowe, S. 2017. “Cultivating Sapling: Faster zk-SNARKs--Zcash Blog”. Zcash Blog.

EXAKING. 2018. “PoW 51% Attack Cost”. 2018. https://www.exaking.com/51.

Grewal, Satinder. 2018. “Satinder’s notes on the PIRATE chain”. 2018. https://blog.komodoplatform.com/pirates-of-komodo-platform-cdc991b424df.

Hopwood, Daira, Sean Bowe, Taylor Hornby, en Nathan Wilcox. 2016. “Zcash protocol specification”.

Japparova, Irina, en Ramona Rupeika-Apoga. 2017. “Banking Business Models of the Digital Future: The Case of Latvia”. European Research Studies 20 (3A). Professor El Thalassinos: 846.

Jl777c. 2016. “Delayed Proof of Work (dPoW) Whitepaper”. Github. 2016. https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)-Whitepaper.

Kappos, George, Haaroon Yousaf, Mary Maller, en Sarah Meiklejohn. 2018. “An Empirical Analysis of Anonymity in Zcash”. arXiv preprint arXiv:1805.03180.

Komodostats. 2018. “Asset Chains Notarizations Summary”. 2018. https://komodostats.com/acs.php.

Lee, James. 2018. “Komodo: An Advanced Blockchain Technology, Focused on Freedom.” Komodo.

Moser, Malte. 2013. “Anonymity of bitcoin transactions”.

Nakamoto, Satoshi. 2008. “Bitcoin: A peer-to-peer electronic cash system”. Working Paper.

Ocminer. 2018a. “Network Attack on XVG / VERGE”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.0.

———. 2018b. “Network Attack on XVG / VERGE (Page 57)”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.msg38135174#msg38135174.

PTY X. 2018. “What is a Parallel Chain (Asset Chain)?” Komodo Platform. 2018. https://komodoplatform.atlassian.net/wiki/spaces/KPSD/pages/71729160/What+is+a+Parallel+Chain+Asset+Chain.

Quesnelle, Jeffrey. 2017. “On the linkability of Zcash transactions”. arXiv preprint arXiv:1712.01210.

Roberts, Jeff John. 2018. “Bitcoin Spinoff Hacked in Rare ‘51% Attack’”. FORTUNE. 2018. http://fortune.com/2018/05/29/bitcoin-gold-hack/.

Saberhagen, Nicolas Van. 2013. “CryptoNote v 2.0”.

Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, enMadars Virza. 2014. “Zerocash: Decentralized anonymous payments from bitcoin”. In 2014 IEEE Symposium on Security and Privacy (SP), 459–74.