



Bitcoin Private

The Revolution of Privacy

Fulfilling Satoshi's Vision for 2018 and Beyond

February 2018

1st Edition

Authors:

Bitcoin Private Community

Jacob Brutman, Ph.D.

Jon Layton

Christopher Sulmone

Giuseppe Stuto

Geoff Hopkins

Rhett Creighton

www.btcprivate.org

Abstract

Since the dawn of the digital age, the internet has empowered humankind in uncountably many ways. However, this easily accessible store of information has, in many ways, marginalized our privacy. Too often and through no fault of the end user, a third party with inadequate security is breached, and sensitive information is compromised or stolen. A better system is needed which is free of “trusted” middlemen such that any two individuals can freely and securely transact. Herein, a new cryptocurrency, Bitcoin Private, is presented. Bitcoin Private follows the principles of Bitcoin creator Satoshi Nakamoto’s roadmap as a low-fee, fast, and private transactional network. This is made possible through a “fork-merge” of Bitcoin with Zclassic. The resulting Bitcoin Private chain has transaction speeds four to six times faster than Bitcoin as well as significantly lower fees. Most importantly, a peer reviewed privacy technology, originally implemented by the Zcash Foundation, “zk-SNARKs”, is incorporated. This privacy technology allows for provably anonymous and private transactions - an accomplishment no other privacy technology can claim. The UTXO sets of both Zclassic and Bitcoin will comprise the initial coins in this new ledger. This makes for approximately 20 million out of 21 million coins mined at fork time, ensuring that Bitcoin Private will have the lowest inflation to ever exist in the cryptocurrency universe. The commercial applicability of Bitcoin Private is also discussed, as well as the coin’s potential for future development and community-driven focus.

Table of Contents

1. Introduction
2. Fork Methodology
3. Proof-of-Work & Equihash
4. Transparent vs Shielded Transactions
5. Voluntary Miner Contribution Program
6. Treasury Fund Governance
7. The Future of Bitcoin Private
8. Commercial Applications
9. Community-driven Project
10. Conclusion
11. Acknowledgements
12. References

1. Introduction

For most of written history, transactions have been private and fairly anonymous. The information of a transaction was only disclosed to the sender, the recipient, and those they wished to inform. Recently, the large majority of financial transactions are facilitated by technology, making it increasingly difficult to maintain financial privacy. These most common methods (e.g. credit/debit card, apply pay, etc.) result in all the information of a transaction being stored digitally. While there are immense benefits that come with these transaction methodologies, it should not preclude the utility of financial privacy for the average consumer. Considering how often breaches occur within large financial institutions resulting in significant leaks of personal and financial information, it is clear there is a need for financial privacy options.^{1,2} Furthermore, various financial institutions have been caught selling customer data,³ as well as blocking legal transactions with no valid legal basis.⁴

In October 2008, Satoshi Nakamoto released the academic article titled “Bitcoin: A Peer-to-Peer Electronic Cash System” in which the foundation for the first cryptocurrency was detailed.⁵ Satoshi’s vision was to create a currency which enabled removal of third party institutional control of transactions, limited inflation, and monetary freedom through anonymous transactions. Since the launch of Bitcoin in 2009, over 1000 different cryptocurrencies have been created and immense progress has been attained.⁶ Indeed, many new cryptocurrencies far outpace Bitcoin in terms of transaction speed and fees. Regardless, Bitcoin still remains the most popular cryptocurrency due to its first mover advantage and significant number of base-pairs available for trading.

As the Bitcoin blockchain grew through the years, notable issues began to rise including a fixed, small block size (which led to higher than practical fees), slow block time (10 min average), long difficulty adjustment period (every 2 weeks), and the development/mass-production of advanced ASIC mining devices (for rapidly calculating SHA256; this algorithm is a key consensus parameter) leading to further centralization. In order for Bitcoin to address these items, migration of over 50% of its miners would have to consent to changing the code they are running; to-date, no such event has happened. This has driven the creation of hard forks of Bitcoin (such as Bitcoin Cash and Bitcoin Gold), to enable some of these technological improvements. For example, Bitcoin Cash remodeled to allow for larger block sizes (≥ 8 MB vs 1 MB), which reduces fees and increases transaction throughput. However, this did not come without tradeoffs - its price potential was damaged because of its lack of a fixed block-size and “fee market.” The fee market in the Bitcoin mempool challenges transactions big-and-small to compete against the opportunity cost of each other; this makes the value of its ownership even more urgent, causing higher demand. Bitcoin Gold took another route, instead reducing the block time (2.5 min), switching the PoW algorithm to Equihash (ASIC resistant), and introducing an enhanced difficulty adjustment algorithm, which occurs every block. It largely satisfied its goal as a GPU-compatible Bitcoin fork, but it lacks the widespread adoption of Bitcoin, and the developers performed a pre-mine cash

grab which many argue is less than ethical given that it happened behind closed doors.⁷ Despite the best of intentions, Bitcoin forks have indisputably remained second to bitcoin in the cryptocurrency markets as of Q4 2017.

At the core of Satoshi's vision, many find themselves drawn to technology's capacity to manifest a deflationary unit of financial value that also allows us to enjoy and leverage anonymity. The "Right to Privacy" is a crowning liberty in the free world,⁸ and is essential to the principles set forth by Satoshi and the cryptocurrency community. With financial privacy being a critical principal in Satoshi's vision of a new digital currency world, many are still at a crossroad with pseudo-anonymous transactions on blockchains. Furthermore, there are government and private sector organizations that leverage massive data-sets and machine learning to identify the individuals associated with such a transaction. Indeed, BitFury is capable of de-anonymizing up to 15% of Bitcoin transactions as of January 2018, a figure that increases daily and could markedly alter the cryptocurrency hemisphere in the years to come.⁹ This lack of privacy in relation to Bitcoin is incredibly alarming given the original intent of its creator.

Various cryptocurrencies have attempted to solve this privacy issue. Unfortunately, many of these are still capable of being compromised through various techniques, due to their on-chain transaction systems that promise anonymity through obfuscation or TOR nodes. In 2014, a groundbreaking research paper by MIT researchers discussed "zero-knowledge non-interactive arguments of knowledge", or zk-SNARKs.¹⁰ Remarkably, cryptocurrencies that implement zk-SNARKs allow for shielded transactions - funds sent which are completely anonymous with no transaction appearing on the ledger. In 2016, the authors of this research developed and launched Zcash, the first cryptocurrency to incorporate zk-SNARKs. A "founder's tax" was incorporated into the code of Zcash, allowing the development team and early investors to collect 20% of coins mined by the community. After listening closely to the mining community, Rhett Creighton decided to fork Zcash just 8 days later, eliminating the founder's tax and creating Zclassic - a Zcash platform built on transparency through community development. Unfortunately, Zclassic suffered from the same ideas which it derived its greatness: the absence of a founder's tax led to a lack of active development. However, there are various governance methods to prevent this stale development.

Bitcoin Private, a supposed "fork-merge" of Bitcoin and Zclassic, is intended to add privacy and spendability to the Bitcoin blockchain while remaining cognizant of the challenges, choices, and failures of prior forks. To accomplish this, Bitcoin Private will use a larger block size (2 MB), a shorter block time (2.5 min), and an ASIC-resistant (GPU-friendly) proof of work (PoW) algorithm for mining - Equihash. Furthermore, due to the dual nature of this fork-merge, more of the crypto-community will find themselves involved. After the snapshot, ZCL (t & z) and BTC (segwit & normal) addresses will receive BTCP (1:1 for both) at the same address. This is a first-

of-its-kind fork and the open-source blockchain community is finally beginning to fully explore the malleability of UTXO sets.

Table 1: Comparison of Bitcoin Private with Bitcoin, Bitcoin Cash, and Bitcoin Gold.

	Bitcoin Private	Bitcoin	Bitcoin Cash	Bitcoin Gold
Total Supply	21 million	21 million	21 million	21 million
Privacy	zk-SNARKs	None	None	None
Block Time	2.5 min	10 min	10 min	2.5 min
Block Size	2 MB	1 MB	8 MB	1 MB
PoW Algorithm	Equihash	SHA256	SHA256	Equihash
Difficulty Adjustment	Every Block	2 Weeks	2 Weeks	Every Block
Closed Premine	No	No	No	Yes
Community-Driven	Yes	No	No	No
Governance	Yes	No	No	No

2. Fork Methodology

For Bitcoin Private, a “fork-merge” is proposed, whereby the UTXOs of two cryptocurrencies are combined into one blockchain. This will formally happen off of the Zclassic blockchain, since zk-SNARKs and JoinSplit transactions are fundamentally part of this new blockchain. The snapshot will only need to retrieve the address state from Bitcoin and Zclassic at a single point in time, which will be carried to the new chain. This approach is effective and results in a significant reduction in storage required by the blockchain, in this case reducing it from 157 GB to only 10 GB (at launch). Additionally, the Bitcoin Private clients will support blockchain pruning and SPV techniques like Electrum in order to reduce the burden of the blockchain on user devices.

A significant issue that any fork must handle is a so-called “replay attack”, in which a post-fork transaction on the original blockchain is made valid on the new blockchain. All coin forks must have replay protection in order to ensure legitimacy and independence from the original blockchain. To safeguard against replay attacks from Bitcoin and Zclassic, Bitcoin Private will feature 2-way replay protection. This is a studied problem, and we are using the industry standard approach which will be incorporated in a 2-way manner as stated above.

3. Proof of Work: Equihash

As discussed in the introduction, mining of Bitcoin is predominantly performed by ASICs, specialized instruments capable of significantly outcompeting GPUs. Unlike GPUs, ASICs are far more difficult to acquire and have led to significant centralization of Bitcoin mining. Indeed, Igor Homakov has suggested that over 60% of Bitcoin network hash rate is located in China.¹¹ Meanwhile, ASIC resistant algorithms are far more likely to be decentralized as GPUs are more readily available throughout the world. Decentralization of the network hash allows for significantly more democratization of the blockchain, decreased susceptibility to a 51% attack, and ensures that the cryptocurrency generated via mining, as well as associated fees collected, are spread throughout the community as evenly as possible. This further prevents the ability of a few miners to influence the blockchain development as well as manipulate the market via mining significantly large amounts of the cryptocurrency.

Bitcoin Private will utilize the well-renowned Equihash PoW algorithm, which was developed by Alex Biryukov and Dmitry Khovratovich at the University of Luxembourg as an asymmetric proof of work (PoW) mechanism.¹² Unlike other ASIC-resistant PoW algorithms, Equihash is based on the “Birthday Problem” and the enhanced Wagner algorithm utilized to solve it. Furthermore, Equihash features “memory hardness” whereby a steep computational penalty is associated with a reduction in memory usage and speed. This feature increases the ASIC resistivity of Equihash due to the cost of implementing more memory into ASICs in order to make them competitive with GPUs or even CPUs. The authors of the original paper discuss that while memory hardness does not protect against bot-net based CPU mining, the large amount of memory consumption would be extreme such that the user-base of infected PCs would notice a significant difference in performance and take necessary actions to remove the infection.

4. Transparent versus Shielded Transactions

Bitcoin Private is an amalgamation of two transaction systems - transparent and shielded transactions. Transparent transactions operate on the same principles as Bitcoin - input, output, amount, and signature. Sources of all funds, destinations, and amounts are stored transparently on the blockchain. Shielded transactions, conversely, encrypt these details into a special section of a block called the “joinsplit”. These transactions are verifiable but indecipherable to third-party observers. When spending shielded notes, the integrity of the blockchain is kept via a specialized zero-knowledge proof algorithm called zk-SNARKs.⁶ This algorithm runs a series of computations to show the input values sum to the output values for each shielded transfer. Then, the sender proves that they have the private spending keys of the input notes, giving them the authority to spend. Finally, the private spending keys of the input notes are cryptographically linked to a signature over the whole transaction, in such a way that the transaction cannot be modified by a party who did not know these private keys.¹³ This entire methodology relies on the Zcash trusted

setup: at Zcash launch, keys necessary for zero knowledge proofs and private transactions were generated and subsequently destroyed; this was called “The Ceremony.”⁶ By doing this, the system can ensure “one-time strong unforgeability against chosen message attacks.”¹⁰

5. Voluntary Miner Contribution Program

To raise funds for the maintenance and development of Bitcoin Private, a *Voluntary Miner Contribution Program* was launched. In this program, 62,500 Bitcoin Private are auctioned to miners up to a total of 50,000 Zclassic donated to the Bitcoin Private treasury fund via hash power. The payout for any given miner in the program can be determined by the following equation:

$$P = Z_m * 62,5000/Z_p$$

Where P is the payout for the miner, Z_m is the Zclassic mined by the miner, and Z_p is the total Zclassic mined by the entire pool. The 62,500 Bitcoin Private are generated at the fork and deposited to the corresponding wallet addresses provided by each miner. The pre-fork ZCL multi-sig wallet that was established for this program will contain upwards of 50,000 Zclassic and subsequently be forked into BTCP to establish a treasury for development, bounties, continued marketing and the overall development of Bitcoin Private by the community. This is one of several methods to address the original Zclassic stale development issue.

In some regards, this program could be seen as a “pre-mine” which is a concept the Bitcoin Private contribution team is vehemently opposed to. However, pre-mines have generally been performed by and directly for the core group and that is not the case here. Therefore, we propose calling this an “open pre-mine” whereby everyone from the mining community is able to voluntarily choose to donate funds in exchange for pre-access to mining Bitcoin Private. Furthermore, due to the auction-like style of the program the mining community is able to choose how much each ZCL donated will be worth as a collective: this type of free-market methodology is at the core of Satoshi’s original vision for Bitcoin.

These funds will be used for exchange listings (50%), development (25%), marketing (15%), and general/administrative (10%). All ZCL and BTCP will be spent responsibly so as to prevent altering their market value. When, necessary the treasury fund can convert funds to BTC via a partnership with a large over-the-counter exchange, which will allow for conversion without altering the market value of either cryptocurrency.

The mining pool for Zclassic will remain functioning at a 10% donation rate after the fork in order to continue collection for any expenses that occur; the funds collected from this ZCL pool will directly go to continued infrastructure support for Zclassic. Furthermore, a *Bitcoin Private Developer Donation* mining pool at a 10% donation rate will also be opened after the fork for the

same reason. In this way, members of the mining community can voluntarily choose to continue supporting the project rather than being coerced into paying a tax. A one-click miner with a similar

6. Treasury Fund Governance

A treasury fund governance council has been assembled from three members of the community and two members from the mining community. At the time of publication, Jacob Brutman, Ph.D. (Operations Lead), Giuseppe Stuto (Marketing Lead), and Peter Hatzipetros (General Counsel) represent the community, while Adib Alami and Evan Darby represent the mining community. The funds from the Voluntary Miner Contribution Program are deposited into a 3-of-5 multi-signature wallet controlled by the aforementioned council. In order to utilize funds, a unanimous vote must be secured by the council, however, members must recuse themselves for matters in relation to themselves. The 3-of-5 format of the wallet is to ensure that the funds can be moved to a new governance wallet address should wallets be compromised.

7. The Future of Bitcoin Private

Improving privacy across the board is an important piece of the Bitcoin Private project. Currently, zk-SNARKs are quite RAM and CPU intensive during signing of the transaction, which can take up to a few minutes. One of the first improvements to be implemented post fork is the new sapling, termed “Jubjub,” currently in development by the Zcash core development team.¹⁴ This new sapling will allow for a significant improvement in the speed and user-friendliness of zk-SNARKs privacy coins. Another methodology for improving the privacy of Bitcoin Private is to utilize the “Dandelion” privacy project currently under development.¹⁵ This methodology involves the “stem” (the transactions) and the “fluff” (obfuscation). While any obfuscation method is inherently less secure than zk-SNARKs, Dandelion obfuscation could be added to both transparent and shielded transactions of Bitcoin Private, improving privacy across the board.

Allowing for blockchain improvements to Bitcoin Private is of great importance to the project. BIP9 has been incorporated into the blockchain to allow for soft forks and thus, improvements.¹⁶ After the proper coding for improvements has been finished, the miners are asked to signal readiness to accept the chain code change. When 95% of miners accept the change, it becomes “locked in” and the soft fork is completed. However, if the miners do not signal readiness within the specified time period, the soft fork will fail, and no changes will take place. Support and development of the Bitcoin Private project will rely on continued treasury fund collection in a manner other than mining pool donations. However, the Bitcoin Private contribution team strongly opposes any sort of imposed taxation on its community without a democratic vote in favor of such. Therefore, one of the first proposed changes via BIP9 will involve treasury fund collection

parameters. In this way, the miners are able to choose what is a suitable amount they are willing to donate as a collective to ensure the future success of the program.

In the event that BIP9 fails to achieve a multitude of necessary improvements, a “difficulty bomb” has been implemented into Bitcoin Private to allow for significant future development, in a similar manner as with Ethereum.¹⁷ When utilized, the difficulty bomb will be applied to the old blockchain code, reminding miners to adopt new code base for continued improvements. Ideally, the difficulty bomb would be implemented to introduce a new governance system, such as, but not limited to, the system featured by Decred.¹⁸ This will allow for further democratization of the Bitcoin Private blockchain.

8. Commercial applications

Payment processing continues to be one of the most profound use cases of Bitcoin today. Merchants have likely transacted over \$1 billion equivalent of bitcoin for the year of 2017 using bitcoin payment processing companies such as BitPay. Wallet users of this very same company secure over \$1 billion worth of assets per month and send over \$1.5 billion wallet to wallet per month.¹⁹ Just as the internet brought a new, revolutionary method of payment, cryptocurrency is doing the same.

Consumers expect a certain level of convenience when it comes to transferring value in exchange for goods and services, and this is why payment processing on the web has become commonplace. Along with this expectation of convenience, there is an assumed level of privacy that comes with such a transaction. Unfortunately, over the past two decades there have been entities who profit off of creating an online “profile” of a consumer by tracking online credit card transactions.²⁰ This is incredibly invasive and serves as a large supporting premise for why a consumer would want to transact online with cryptocurrency. Despite the technical design of the most popular cryptocurrency, this privacy can no longer be expected on the blockchain.¹⁴ However, Bitcoin Private could fulfill the privacy needs of consumers via zk-SNARKs transactions.

Bitcoin Private will play a major role in peer to peer and commercial transfer of digital assets. It offers vendors a tested, secure, and widely adopted cryptocurrency technology with the added benefit of provable anonymity and privacy. Potentially, hundreds to thousands of natural use cases will come of Bitcoin Private in commercial use. While other z-protocol coins could be capable of fulfilling this role, generally none have opted to or succeeded. However, the Bitcoin Private contribution team has a strong desire to bring the cryptocurrency into mainstream acceptance, allowing for widespread usage. In particular, mobile wallet platforms could be utilized to store and transfer Bitcoin Private via transparent and shielded transactions on-the-go.

9. Community Driven Project

Many cryptocurrency projects, whether utility tokens or coins, claim to be community-driven and open source. While this is true to an extent, a core development team typically exists which controls the entire future of the project. Few exceptions exist (e.g. Decred) whereby the community has actual control of the future, however, development teams are still often closed doors. While community members can suggest modifications on the corresponding code, these requests may go unnoticed. The Bitcoin Private project represents a true community effort, with over 100 contributors currently (Feb. 6, 2018) and is growing daily.

Various initiatives have been implemented which separate Bitcoin Private from other community coins. For instance, a world-wide, localized ambassador program has been launched whereby members of the community can actively engage in helping to promote Bitcoin Private and increase the community. Furthermore, Bitcoin Private has opened a “call for developers” in which anyone can apply, even those new to blockchain technology, and contribute in a meaningful way to the project. Those without prior experience are able to learn from this developer program and become proficient in blockchain technology and engineering. These two programs combined have added over one hundred new contributors in a span of a few days, expanding our daily contributing team to well over 300 members. The size of the Bitcoin Private contribution team shows the project’s dedication to its community-driven inspiration and is a feat that no other cryptocurrency has achieved to the best of the team’s knowledge. This showcases the truly decentralized nature of Bitcoin Private’s development.

10. Conclusion

Bitcoin Private is a cryptocurrency developed and maintained by a diverse community. Team members from around the globe collaborate daily to make this project a success. They do so, because they believe the project fulfills Satoshi’s original vision of financial freedom via fast, low-fee, decentralized, and private transactions. Bitcoin Private’s forward-thinking inclusion of the BIP9 soft fork proposal will allow for future developments, and an included difficulty bomb will advance alternative governance methodologies should BIP9 prove ineffective. The commercial applications of Bitcoin Private are numerous: from fast global transactions to purchasing in local stores. This merger of Bitcoin’s vast, dedicated following and shielded transaction technology of Zclassic will usher in a new era of trusted blockchain privacy.

11. Acknowledgments

We would like to acknowledge the mining community for their generous donations via the Voluntary Miner Contribution Program. We would also like to thank the molecule of caffeine for helping the team push through many long days and nights; without coffee, this project could not

have been possible. Many thanks are also required to our amazing development team, you are the foundation for which we rely on. Finally, we would like to thank the entire Bitcoin Private community; you are the backbone of this project and we would not be here without you.

12. References

- ¹ *Dutch Banks Tax Agency Under DdoS Attacks a Week after Big Russian Hack Reveal.* <https://www.bleepingcomputer.com/news/security/dutch-banks-tax-agency-under-ddos-attacks-a-week-after-big-russian-hack-reveal/> (Accessed Feb. 5, 2018).
- ² *The Biggest Data Breaches of the 21st Century.* <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html> (Accessed Feb. 6, 2018).
- ³ *What Chase and Other Banks won't Tell you about Selling your Data.* <https://www.forbes.com/sites/adamtanner/2013/10/17/what-chase-and-other-banks-wont-tell-you-about-selling-your-data/#5eacaaf62c41> (Accessed Feb. 5, 2018).
- ⁴ *Santander Totta has no Known Legal Basis to Block Bitcoin Related Transactions says Portuguese Consume Watchdog.* <https://www.ccn.com/santander-totta-has-no-known-legal-basis-to-block-bitcoin-related-transactions-says-portuguese-consumer-watchdog/> (Accessed Feb. 5, 2018).
- ⁵ Nakamoto S.; (2008) *Bitcoin: A peer-to-peer electronic cash system.*
- ⁶ *List of Cryptocurrencies.* <https://cryptocurrencyfacts.com/list-of-cryptocurrencies/> (Accessed Feb. 5, 2018).
- ⁷ *Premine Endowment.* <https://bitcoingold.org/premine-endowment/> (Accessed Feb. 2, 2018)
- ⁸ Brandeis, L.; Warren, S.; (1890) *The Right to Privacy.*
- ⁹ "BitFury Group De-Anonymizes Over 15% of the Bitcoin ... - The Merkle." 11 Jan. 2018, <https://themerple.com/bitfury-group-de-anonymizes-over-15-of-the-bitcoin-network-with-new-blockchain-analysis-tool/> (Accessed Jan. 30, 2018).
- ¹⁰ Ben-Sasson, E; Chiesa, A; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. (2014) *Zerocash: Decentralized Anonymous Payments from Bitcoin.*
- ¹¹ Homakov, I. (2017) *Stop. Calling. Bitcoin. Decentralized.* <https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27> (Accessed Feb. 4, 2018)
- ¹² Biryukov, A.; Khovratovich, D.; (2016) *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem.*
- ¹³ "Zcash - How zk-SNARKs work in Zcash." <https://z.cash/technology/zksnarks.html> (Accessed Feb. 3, 2018).
- ¹⁴ *What is Jubjub?* <https://z.cash/technology/jubjub.html> (accessed Feb. 1, 2018).
- ¹⁵ *Bitcoin Developers Reveal Roadmap for 'Dandelion' Privacy Project* <https://www.coindesk.com/bitcoin-developers-reveal-roadmap-dandelion-privacy-project/> (accessed Feb. 5, 2018).
- ¹⁶ *BIP9.* <https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki> (Accessed Feb. 7, 2018)
- ¹⁷ *What is the Ethereum Difficult Bomb.* <https://themerple.com/what-is-the-ethereum-difficulty-bomb/> (accessed Feb. 5, 2018)
- ¹⁸ *Decred Documentation.* <https://docs.decred.org/> (Feb. 1, 2018).

¹⁹ *Bitcoin Transactions aren't as Anonymous as Everyone Hoped.*

<https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/> (Accessed Feb. 5, 2018).

²⁰ *Google Now Tracks Your Credit Card Purchases and Connects them to its Online Profile of you.* <https://www.technologyreview.com/s/607938/google-now-tracks-your-credit-card-purchases-and-connects-them-to-its-online-profile-of-you/> (Accessed Feb. 5, 2018).