X-CASH: Global Blockchain Network to Facilitate Payments through Cryptocurrencies

G. CHAUMONT, P. BUGNOT, Z. HILDRETH

***Abstract*— Since the birth of bitcoin in 2009 and the increase in adoption since then, there are still many obstacles preventing the daily use of cryptocurrencies by the mainstream audience. This paper aims to present the concepts behind X-CASH in detail and how it plans to overcome its challenges. One of the key concepts described in this paper is the triple connection between users, merchants, and banks. By offering an all-in-one solution that connects them, performs the crypto-to-fiat conversion and handles the settlement, X-CASH aims at revolutionizing the payment industry by offering lower costs while increasing the security and guaranteeing scalability and processing time.**

To meet the growing demand of regulation in the cryptocurrency space, X-CASH is also developing a partial anonymity upgrade of the network where users will have the option of making part of their transaction details public. This will be possible through the inclusion of additional data in the blockchain.

With the aim of answering the corporate needs for blockchain solutions and tackling scalability, X-CASH is also developing a sidechain solution where operators will be able to run their own chains with custom sized transactions. Thanks to the zero-knowledge proof nature of the network, participants will be able to share documents or any information, without revealing their identity, or the content itself. One of the key business cases of this solution would be the hidden signature of contracts between two entities where the network would still witness the transaction. The details and nature of the transaction would be kept hidden until there was a need to reveal the information, for legal purposes, for instance.

***Index Terms*—Blockchain, Cryptocurrencies, Payment Gateway, Crypto-to-Fiat Conversion Platform, X-CASH, Sidechains, Zero-Knowledge Proof.**

Table of Contents

I. INTRODUCTION 2
II. The X-CASH project 2
A. Introduction and Goals 2
B. Underlying Technology 2
C. Supply and Emission Structure 2
D. Founding Team 3
E. Roadmap 3
III. X-CASH 1.0: Cryptonote algorithm 4
A. Proof of Work 4
B. Ring Signatures 4
C. Stealth Addresses 5
D. Bulletproof Transactions 5
E. Partial Anonymity Implementation 5
1) Three Kinds of Privacy 5
2) Technical Implementation 5
F. Public Nodes 5
1) Currently Live 5
2) Q4 2018 6
3) Q1-Q2 2019 6
IV. X-CASH 2.0 & BEYOND: PoS implementation 6
A. Proof of Stake 6
B. Masternode 6
1) Stake and Specifications 6
2) Return on Investment 6
C. Sidechains 7
1) Specifications 7
2) Transactions Specifications 7
V. Payment Gateway and transaction settlement solution 7
A. XCASH to FIAT Conversion Process 7
1) Description 7
2) The Process from the Customer Perspective 7
3) The Process from the Merchant's Perspective 7
4) The Process from the Backend Perspective 8
5) Three Level Confirmation Process 8
6) Summary of Costs 8
B. Sidechain Networks 8
1) Description 8
2) Sidechains Networks 8
VI. Increasing liquidity and reducing volatility through derivatives instruments 9
VII. Conclusion 9
VIII. Bibliography 10

I. INTRODUCTION

Real-world digital payments are already a common practice with close to 500 bn transactions every year worldwide [1]. Although reliable from a technical perspective, current digital payment solutions involve high fees for the merchants ranging from 0.1% to 2%. Moreover, these solutions come with extra costs from the customers' perspective as well, more particularly when not used in their country of origin.

At the same time, cryptocurrencies have grown significantly with an adoption rate going exponential since 2017 [2]. Although they have overcome the geographical constraints, they are still rarely used for everyday payments. Some of the reasons may include difficult FIAT conversion, low scalability, high transfer costs [3] and a global context of lack of regulations and transparency [4].

In a context where everything tends to be digitalized, corporations, banks, and institutions still widely tend to use time and money consuming procedures when it comes to legal paperwork or any type of transaction settlement.

By using a proof-of-stake network, derived from Cryptonote and Monero's algorithms, with an embedded sidechain network solution, the X-CASH team believes there is significant potential to disrupt the existing payment solutions as well as offer a new way for corporations to complete transactions.

II. THE X-CASH PROJECT

A. Introduction and Goals

X-CASH [5] is a registered fintech based in Paris, France that started in early 2018. The project is fully self-funded and driven by three blockchain enthusiasts from different backgrounds (finance, engineering, computer science). The primary goal of X-CASH is to provide a global solution for digital payment and transaction settlement reducing fees and transaction time using blockchain technology.

Being incorporated in France, the company aims at being compliant with all existing and upcoming regulations in France and E.U. Similarly, X-CASH will work closely with the financial industry in order to create a tight link with existing banking systems. These steps are compulsory to bring cryptocurrency to mainstream adoption. Regulations will ensure the protection of the users and investors while banks will serve as a catalyst thanks to their solid base of retail clients.

B. Underlying Technology

X-CASH is based on the core code of Monero v7 [6], which itself derives from Cryptonote [7], using the CryptoNight Hash Function [8] [9]. The choice was made to use a proven blockchain source code that has constant improvements and updates to base X-CASH development on.

Monero's main appeal is the fact that it is a privacy coin. It uses an obfuscated public ledger, meaning anybody can broadcast or send transactions, but no outside observer can tell the source, amount, or destination. Privacy is an important factor when managing personal finances, while banks and institutions need to know the source of the funds for traceability. Therefore, X-CASH proposes to let the users have the choice of whether or not they want their transaction to be public.

In addition, to make the synchronization of the blockchain faster than other cryptocurrencies and reduce transaction latency, a worldwide network of dedicated servers has been implemented. This is a crucial component in the deployment of the future improvements of the X-CASH core.

C. Supply and Emission Structure

The total supply of X-CASH is 100,000,000,000 (100 billion) XCASH. The supply is distributed as follow:

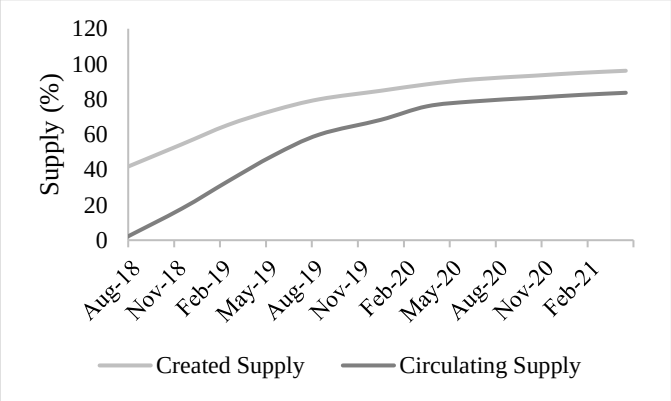
- Out of the 5% dedicated to the team, 2% of the coins have been assigned. The remaining will be made available for the new joiners. The release of these coins is subject to stringent conditions linked to the market capitalization of the coin.
- 10 % of the supply is made available for the company to cover the current salaries of the team, the development of the coin, and the infrastructure costs.
- 5% of the total supply will be sold to private investors through OTC trades with a discount of 5-30% against the spot market price. The idea behind this is to generate some funding in the early stage of the project without impacting the coin spot price (the coins sold are subject to a vesting period).
- 20% of the supply will be released through a 20 months Airdrop Program. This option has been chosen because this is a fair way to distribute the coins to people without mining equipment while getting some involvement from the community.

The current supply increases by ~4%/monthly, meaning that 95% of supply will be reached in late 2020, At this point, the releases of X-CASH 2.0 will already have been enabled with the PoS algorithm, and the inflation rate will switch to 0,1-0,5% constant rate.

Moreover, the release of the team's allocated coins is subjected to conditions depending on the market capitalization of the coin. Indeed, starting from a market cap of $10 million and every time its value is multiplied by 10, 20% of the team's allocated coins will be unlocked. This ensures performance driven objectives and avoids any hard dumping on the market, instead of locking the coins for an arbitrary period.

Since there is no way to track the wallet's funds through a public address, the premined funds will be audited quarterly once listed. An independent audit will confirm the funds are still in their segregated wallet. This process will be physically carried out by the team as the funds are stored in cold wallets secured in bank vaults.

Because the premined supply has been put in segregated accounts and is progressively added back into circulation, there is a difference between the mined supply and the real circulating supply. The figure below gives an overview of the projected circulating supply over time.



D. Founding Team

The founding team of X-CASH is comprised of three people from different academic and professional backgrounds with a common goal: developing a realistic project around the blockchain technology with rational objectives. The team is as follows:

Guilhem CHAUMONT
Chief Executive Officer

Guilhem is a former trader who left his job to start a new cryptocurrency with the aim of filling the gap between blockchain technology and mainstream adoption. Since 2016, Guilhem has been an active trader and investor which led him to start a mining firm at the end of 2017.

Guilhem holds two master's degrees: in Energy Engineering from Ecole Centrale de Lyon and in International Finance from HEC Paris. Thanks to his two-year Rates Derivatives Trading experience in one of the largest banks, Guilhem has acquired a good understanding of the mechanism driving the financial industry. Before that, he was a student researcher in nuclear engineering at Commissariat à l'Energie Atomique.

Zach HILDRETH
Chief Technology Officer

Holder of a Bachelor Degree in Computer Science, Zach is a full-stack developer who programs websites, games, and software. He also specializes in cyber-security which started his interest in blockchain technology. He has been investing in cryptocurrency since 2013 and has been deeply involved in the blockchain community ever since.

Zach is also a writer of comprehensive cryptocurrency mining guides and the Chief Technology Officer for one of the most active mining communities.

Paul BUGNOT
Chief Operating Officer

After graduating with a Master's Degree in Nanotechnology at Institut National des Sciences Appliquées, Paul worked as a research engineer at the Centre National des Recherches Scientifiques, then as a patent attorney for the automobile industry. Looking for exciting opportunities, he then took charge of a company for the distribution of nanotechnology solutions in France and Europe.

Passionate about new technologies and emerging businesses, Paul has joined the X-CASH project.

E. Roadmap

From early 2018 until September 2018: Start of development, main net release, start of the monthly airdrop and exchanges listing

The X-CASH project burgeoned in the first quarter of 2018. The first iteration of the blockchain was introduced quickly, and the project was built around it.

The website and functionalities around it were developed, and the first version of the GUI Wallet was created and tested to enable not tech-savvy users to use the wallet on day one.

After a thorough series of tests and process validation in June, the X-CASH network was released to the public on July 31st. Three weeks after the main net release, the X-CASH monthly airdrop started on August 21st. At the end of the first airdrop distribution on September 11th, X-CASH announced its market entrance with four exchange listings.

End of Q3-Q4 2018: X-CASH 1.3 – Bulletproof and Public Transactions

The first main update of the X-CASH project is the implementation of bulletproof transactions. Bulletproof transactions provide a consequent reduction of transaction sizes. This makes it possible to greatly reduce the blockchain size's increase, as well as reducing the transaction fees. At the same time, public transactions will be implemented which will give the users the choice to make the transaction's content public.

Q4 2018 - Mobile Wallet Release

One of the key components of X-CASH's success is its use by the general population. To this end, users need the most intuitive and convenient interface across all devices.

The GUI Wallet has been designed to be seamless across all platforms. The idea is to offer a similar user experience to everyone whether they are on desktop, laptop, or mobile device.

Thanks to these mobile wallets, the users will automatically connect to the network without worrying about the technical parameters to offer a streamlined user experience.

Q4 2018: Third Party Merchant Implementation

One of the other drivers of X-CASH adoption is the possibility to use the system directly to pay merchants and service providers.
While APIs can already be offered to third parties' merchants to integrate X-CASH payments, the main objective is to build the infrastructure that will handle the X-CASH conversion into Fiat currency.

To allow this, X-CASH plans to offer market-making activities to allow easy liquidation of merchants' position into Fiat to process their payments separately.
Eventually, X-CASH should be able to offer the merchants the option to be paid with either Fiat or X-CASH. X-CASH payments will carry no significant additional charges while fees for Fiat payment would be in the 30-50 basis point (bp) range.

Q1 2019: X-CASH 2.0
Despite being focused on successfully launching the first version of X-CASH at the moment, the team is planning the future of the blockchain. X-CASH 2.0 will need to address two important topics which are scalability and ground base for API development. There are three possibilities:

- **Evolve the current code**: This is the natural path the team is focusing on. It consists of incremental releases that will make the project progressively reach its goal targets while keeping cryptonote and cryptonight PoW as its core code. The next release of X-CASH 1.3 is set up for the end of September, adding Bulletproof transactions.
- **Build a new technology/core code from scratch**: To work towards X-CASH goals, building a new blockchain code including a constant size blockchain or blockchain compression is an exciting path, but the development requires time and resources.
- **Include X-CASH in an existing protocol**: Implementing X-CASH into a more developed blockchain network is another path to follow. ERC20 contracts as other standards on the Ethereum blockchain could be interesting but are not viable at the moment, because they still do not address scalability. Similarly, EOS is offering solutions that could provide some answers to the challenges the X-CASH project is facing. The conclusion is that the technology is not mature enough at the moment but running parallel experiences and revising X-CASH positions accordingly will help decide the path to follow.

After in depth reflection on the subject in early September 2018, the first solution for the evolution of the current X-CASH code has been chosen. This will lead to the release of a PoS version of Cryptonote in early 2019 with an implementation later of a sidechain solution.

Q1 2019: Implementation of X-CASH into Retail Banking Protocols
On the retail payment side, the ultimate goal is to partner with banks (likely online) to offer users the option to manage their X-CASH directly from their bank account.

This would be an interesting feature for the banks as well, as the demand for cryptocurrency is still growing and there is not yet a direct solution to own cryptocurrencies because the bank still plays its role of the responsible holder on behalf of the clients.

At the same time, this would allow further blockchain implementation for the bank such as letters of credit, and loan contracts, among other services.

Q2 2019: Derivative Instruments Linked to X-CASH
While the conversion between X-CASH and FIAT for retailers will be competitive from day one, there is room for improvement to lower the fees.

To this end, X-CASH plans on releasing derivative instruments that will increase the liquidity of X-CASH and enable users to hedge merchants' positions more easily.

The first step is futures contracts with an aim at also releasing options which will enable us to be covered against spikes in volatility.

All-in, thanks to the extensive use of these instruments, we should be able to provide a plug and play solution for merchants with a fixed fee of 10 to 35 bp.

III. X-CASH 1.0: CRYPTONOTE ALGORITHM

A. Proof of Work

Proof of Work (PoW) is a type of algorithm used to achieve consensus across a blockchain network based on the quantity of work (hashes) of the network participants. While the network aggregates potential transactions to add to the next block, miners will adjust the nonce so that the hash of the block matches a specific set of parameters (usually a hash starting with many zeros). This process takes a lot of computing power because it is not possible to predetermine a nonce that satisfies a mining equation. Therefore, miners have to try random or incremental nonce, compute their hashes and see if they can satisfy the set of parameters. The set of parameters can be translated into what is known as the difficulty which is more or less the number of nonce tries/hashes needed to be computed to find a block. As of writing the difficulty of the X-CASH Network is about 186M [10]; implying that the network is computing around 3M hashes per second to satisfy the 60s block parameter.

X-CASH uses the latest Cryptonote v1 algorithm from Monero which is ASIC resistant. It is still internally being discussed whether we will modify the algorithm to make it NiceHash resistant. Unless significant network hash rate manipulation is made, it has been decided to stick to this version as NiceHash currently enables increased liquidity in the network computing power.

B. Ring Signatures

Ring signatures are the ground base of Monero's privacy. In a public transaction blockchain like bitcoin, only the sender's signature is added. In X-CASH every transaction has to be signed by a minimum of two participants. By default,

transactions are signed by 6 participants making it harder to identify the true sender. In the context of the future development of X-CASH, we are also reviewing the possibility of incorporating Unique Ring Signature [11].

C. Stealth Addresses

Stealth addresses [12] [13] are an extra layer of privacy in the transactions by requiring the sender to generate a one-time random address. This means that no public address is recorded on the blockchain and similarly this implies that there is no possibility to view a public address balance using a blockchain explorer. While ring signatures can be seen as a way to prevent tracking history of the transactions, stealth addresses can be seen as a solution to hide transaction details. Section E develops how anonymity can be removed at the discretion of the users by using an extra ledger to store the additional data.

D. Bulletproof Transactions

Bulletproof transactions [14] [15] will replace range proofs used in the current algorithm and allow a reduction in the transaction size. Bulletproofs represent an improvement over range proof by replacing the mathematical method used to hide and confirm the amounts behind a transaction. X-CASH will implement bulletproof transactions once they are audited and live on Monero's network with an expected reduction of the transaction size of 80%. The current implementation of bulletproof transactions on Monero's network is scheduled for September 2018 and will be added to X-CASH shortly after.

E. Partial Anonymity Implementation

Privacy in the cryptocurrency space, similarly as in the financial world, is a very sensitive topic. The purpose of this section is to provide a brief outlook of the X-CASH philosophy with regards to anonymity.

1) Three Kinds of Privacy

Any transaction that involves a transfer of information (such as cryptocurrency payment) can be divided in three major components:

1. Sender: who is initiating the transaction
2. Receiver: who is benefiting from the transaction
3. Content: what is the amount transferred in case of financial payment. What information is shared in the other cases

Similarly, privacy information can be categorized into three layers of anonymity:

1. Full anonymity: there is no way to know the information without a key or a passcode
2. Partial anonymity: the information is traceable but hides underlying information. The best example is an IBAN (Bank account address) or a BTC address. This address is traceable and represents a potential sender or receiver but the final information behind the address, i.e., the human being controlling it remains hidden
3. No anonymity: the intrinsic information is directly accessible to anyone

The combination of these factors leads to two notable cases:

a) Full anonymity for all information

Any information embedded in the transaction is kept hidden for the public users. This is more or less the state of all Cryptonote coins using Monero.

b) Partial anonymity for the sender and/or receiver while content remains public

The most obvious use case is a bitcoin transaction where both senders and receivers are hidden behind a public address while the amount of the transaction is fully displayed.

The goal of the partial anonymity implementation in the Monero code is driven by the need to have these two layers available to any users transacting on the network. This will ensure most of the privacy needs will be satisfied while still offering the necessary ground base to perform non-private transactions, which is a growing topic in the context of increasing regulation in the cryptoworld [16] [17]. Although some of the other cases such as no anonymity for all information could be interesting to review, they are not covered in this document because there is no plan to implement them shortly.

2) Technical Implementation

The solution chosen for the technical implementation of the partial anonymity transactions is a tradeoff between easiness of deployment, scalability on the core code itself, features, and security. To avoid hard-forking the base Monero code, it has been chosen not to modify the transaction components of the core code of X-CASH. This has the advantage of leaving the possibility to the exchanges, mining pools, merchants, and any other parties involved in the X-CASH network to either implement it or not. Two options are being tested at the same time. The first one consists of an integration of the additional data in a segregated ledger while the second would include the data within the transaction block. For the first solution, one of the main drawbacks is that there is a need to ensure a high level of security to guarantee that the information of the 2nd ledger is not compromised. At the same time, because the core code of the original blockchain is not affected, there are no additional security threats added from the perspective of the first blockchain.

F. Public Nodes

To increase the network capacity in terms of synchronization capacity, a network of public nodes running on dedicated servers is being set up [16]. This consists of a 3-phase deployment where the geographical coverage and the bandwidth capacity will gradually increase.

1) Currently Live

The current network consists of 15 dedicated servers with limited geographical coverage. The location of the server has been determined based on a first assessment of the users' origin. Current locations include US, Canada, France, Germany, Poland, China, India, Japan, Singapore, and Australia. The total available bandwidth is 5 GB/S which enables a synchronization capacity of 100,000 full blockchain files[1] per day.

[1] Current blockchain size is 3.09 GB

2) Q4 2018

- Number of servers: 30
- Bandwidth: 10 GB/s
- Added location: Mexico, Brazil, Western Europe, UK, Russia, Indonesia, Morocco & SA.

3) Q1-Q2 2019

- Number of servers: 75
- Bandwidth: 25 GB/s
- Added location: Alaska (US), Remaining Europe, South Kora, Remaining South America & Thailand

IV. X-CASH 2.0 & BEYOND: PoS IMPLEMENTATION

In order to fulfill its long-term goals of efficiency, scalability, and modularity, the X-CASH Network will proceed with two significant network upgrades. The first is scheduled for early 2019 and will include a change in the consensus algorithm. There is also a strong willingness to provide a new technical feature that will allow a significant step forward regarding network specifications: sidechains. Although there is a strong desire to release this feature in the X-CASH 2.0 release, considering the development costs and time involved, as well as a need to clarify some of the specifications, there is a significant chance that this feature will only be included later. The current target is to provide an alpha version during Q2 2019 with a fully working version by the end of 2019.

A. Proof of Stake

Proof of Stake (PoS) is a type of algorithm used to achieve consensus across a blockchain network based on the number of coins (stake) of the network participants. The main advantage against PoW consensus is the reduction of energy consumption [17] which is limited to the servers running the daemons and generating the consensus compared to the need to compute hashes in PoS which is highly computing/power/energy consuming. As an order of magnitude, our estimates suggest that a PoS Network of 20 nodes would achieve a similar or higher security level than the current network hash rate[2] for a consumption of 4kW vs. 220 kW.

The block selection will be randomly chosen among the participants proportionally to the stake they have transferred in their PoS address. During each block selection process, the participants will have to prove to their peers that they own a stake and its amount. This will be achieved without revealing any other information regarding the owner thanks to the use of Ring Signatures as Zero Knowledge Proof.

B. Masternode

X-CASH will use, similarly to DASH [18], a network of masternodes which will validate the transactions in exchange for fees and mining proceeds. Similar to the current mining process, there will be no 'dev' fee in the masternode scheme. This decision to leave 100% of the reward to the masternode owner(s) is made to incentivize the masternode adoption.

1) Stake and Specifications

When discussing the minimum stake needed to run a Masternode, it has been agreed that the stake needed to run a Masternode should constitute a significant entry barrier for two reasons. The first one is a limitation of the total number of Masternodes in the network to increase the speed and the reliability of the nodes in the network. The second, which is linked to the first one, is a need to keep the network of Masternodes to 'serious participants'. One of the best ways to do this is to make the stake to run a masternode significant so that the costs of running the server itself are insignificant. It is also being discussed if any specifications regarding the minimum hardware needed to run the masternode should be expressed and if they should be made compulsory to be part of the network.

A minimum stake of 100m XCASH, still subject to revision, has been currently decided on to run the masternode. The vision of the team is that about half of the supply should be used to run the masternode while the remaining would be the 'true' circulating supply. This means that at full capacity, 50bn XCASH would be used to run a network of 500 masternodes. The team believes this is a good tradeoff between decentralization and network quality. If the long-term goal regarding the XCASH wide adoption is achieved, the typical distribution of the XCASH masternodes could be as follows:

Type	Number of Masternodes
Governments	120
Corporations	150
Institutions	50
NGOs	30
Others	150

It will also be allowed for people with lower stakes to gather into a grouped masternode. The minimum stake allowing to own 1% of a masternode will be 1m XCASH. It is still under consideration whether this solution will be directly implemented into the X-CASH 2.0 code or be done through an external services provider as they already exist in the market [18] [19].

2) Return on Investment

On the short term, there will be a significant incentive to run a masternode because the PoS switch will be done while 30% of the supply remains to be mined. The table below describes what the typical ROI should be under assumptions of network Masternodes:

Year	Estimated Number of Masternodes	Annualized ROI in XCASH (%)
2019	100	255%
2020	350	30%
2021	450	9%
2030	500	1%

[2] As of 06/09/18, the Network Hash rate of X-CASH under Cryptonote v7 is 2 MH/s

It is important to highlight that the high ROI observed in 2019 will be made at the cost of a significant dilution of the XCASH supply (42%). Similarly, in the long term, the ROI of running a masternode will significantly decrease, but it is important to keep in mind that the inflation rate of the supply will be close to null. Therefore, this should fit the goal to have a masternode ROI, USD wise, at 1% above the USD inflation rate.

C. Sidechains

1) Specifications

Sidechains are one of the most essential upgrades planned for the X-CASH network. This consists of running a sidechain where content will not be recorded on the main blockchain but within the participants only [20]. For increased security and reliability, it will be compulsory to include a minimum number of X-CASH Masternodes in the sidechain and leave them a minimum stake of 33% in the consensus. During the inception of the sidechain, each participant will be able to transfer a predetermined amount of XCASH in the sidechain which will remain locked from the main-chain perspective until the neutralization of the sidechain. Within the sidechains, participants will use their stakes to run side Masternodes and carry transactions under the predefined transactions specifications.

2) Transactions Specifications

One of the key characteristics and interest of sidechains is the ability to parametrize the details of the transactions. Users will be able to modify most of the parameters including the fees, minimum number of mixin, and confirmation time.

Sidechains could find most of their interest in the possibility to also change the maximum size of the transactions and include a variable X-Block. The X-Block is a predefined extra block of data embedded in the tx whose characteristics (in terms of size) are also defined at the inception of the chain. One example could be the creation of a sidechain network among suppliers and merchants to share contracts data. The transaction characteristics would remain similar to the main network, but the extra block of data would allow digitally signed contracts of any size (10 MB for instance) to be added. Because all data would be encrypted and transactions would be made using the same stealth addresses as in the main network, only the two parties involved in the transaction would know the content until there was a need to show it to the others. One of the interesting key concepts is that the transaction, although undecipherable, would still be witnessed and timestamped by all participants.

V. PAYMENT GATEWAY AND TRANSACTION SETTLEMENT SOLUTION

In this section two of the main layers which will be implemented on top of the core blockchain network will be described. The first one consists of an easy solution for customers to pay merchants using X-CASH. From the merchants' perspective, this solution will be presented as an alternative to the traditional payment solution where the focus will be on the reduced fees.

The second layer that will be embedded into the X-CASH protocol is a new type of Zero-Knowledge Proof transaction settlement. By running sidechains on top of the master network, institutions, banks, corporations, or individuals will be able to run their own blockchain network and either exchange value through XCASH payments or various kind of information. Because these sidechains will also use Monero's core principles, users will have the option to hide/reveal their transaction to a selected audience, allowing Zero Knowledge Proof.

A. XCASH to FIAT Conversion Process

1) Description

The XCASH to FIAT conversion process can be described as a plug and play solution offered by X-CASH Global payments to convert XCASH coins into FIAT currencies. The primary targeted users for this solution are online and retail merchants. There are two key components in this solution, the first one being financial, the second one being technical. Because the conversion process will imply buying or selling X-CASH against (most likely) other altcoins, there is a need to have a significant market depth across a higher number of exchanges and/or a substantial number of trade volume per second. This will be achieved by registering XCASH to a large number of exchanges with significant volumes and by being market-maker of the XCASH coin on all markets. Because of the early stage nature of the regulation on cryptocurrencies, this activity can be part of the same company carrying the X-CASH development. In the near future, it will be a consideration to move this activity into a segregated company with a Chinese wall with regards to all information subject to X-CASH.

The second layer is technical with the actual liquidation of the coins on the market and their conversion to FIAT currencies. This process is at the discretion of the team and can take several forms. In the following subsection, the typical process is described from the customer and merchant's perspective as well as the liquidation process happening in the back end.

2) The Process from the Customer Perspective

- A customer fills the cart, hits Payment button on the merchant's website and chooses XCASH Payment solution
- Customer sends an EUR equivalent of XCASH within an x (likely 1 or 2) minutes timeframe
- The customer receives payment confirmation once Level 1 confirmation is met and is redirected to the merchant's website

3) The Process from the Merchant's Perspective

- The merchant receives an order confirmation with payment confirmation pending
- The merchant receives Level 1 confirmation of payment
- The merchant receives Level 2 confirmation of payment and can confirm the order to the client by email

- The merchant receives Level 3 confirmation of payment and can deliver the goods
- The merchant receives the funds in FIAT currency from the transaction

4) The Process from the Backend Perspective

- Level 1 confirmation of payment is received
- Identification of best market to convert X-CASH to ALT and execution
- Short selling of ALT against FIAT
- Level 3 confirmation of payment is received, FIAT transfer to merchant
- Reconciliation of ALT and FIAT amounts

When XCASH is converted into ALT coins, it is imperative to convert the ALT coins into FIAT currency in a short timeframe to avoid market risk. Because the conversion is likely made on different exchanges, it is essential to short sell the asset which is why the final step consists of sending the altcoin to the exchange where they were sold to neutralize the position.

5) Three Level Confirmation Process

Although blockchain transactions are relatively fast compared to other means of payments, they are still not compatible with the live payment world where the confirmation needs to be received in a matter of seconds. To make them compatible with instant payment and still allow for a smooth process from the user's end, three levels of confirmation are set up:

- Level 1 corresponds to when the transaction is broadcasted to the network and added to the mempool
- Level 2 corresponds to when the transaction is included in a block
- Level 3 corresponds to a certain number of blocks (confirmations) after the transaction has been added to a block

Each level is a tradeoff between time and security as the higher the level, the lower the chances of rejection/double spending, etc. From a user perspective, it is compulsory to keep the transaction time close to instantaneous which is allowed by level 1 as the broadcasting is done in 1-3 seconds. At the same time, this carries a market risk as the blockchain is still not including the transaction but the liquidation of XCASH to cover the payment has started. The worst-case scenario would be a rejection of the transaction (which could happen for a limited number of reasons unless intentional) and therefore a conversion back from the FIAT currency to XCASH. This would translate into an overall cost of 1-2% which at an aggressive occurrence estimate of 1 in 100 turns into a cost of 1-2bp per transaction provision.

6) Summary of Costs

The below table aims at giving a high-level summary of the costs involved in the conversion:

Item	Costs (bp)
XCASH/ALT Conversion	25
ALT/FIAT Conversion	5
FIAT Reconciliation	1
ALT Reconciliation	2
Short sell funding	0
X-CASH Fee	0
Total Costs	**33**

In the critical step of the conversion, the XCASH/ALT conversion, the cost of 25 bp is a conservative estimate assuming a market price of 400 sat. per XCASH with a bid-ask spread of 1 sat. Because X-CASH will be carrying their own market-making activities, it is expected to reach an effective cost below these numbers. These targets of reducing market costs will also be reached thanks to the use of derivatives which will grant higher liquidity.

B. Sidechain Networks

1) Description

The sidechain networks will offer an important extra feature in the X-CASH network which in short is the possibility for anyone to start their own blockchain network, with specific block characteristics. The idea behind it is to offer an easy and more adaptable solution for the corporations, institutions, or governments which need to use blockchain without having transactions recorded on a large scale blockchain. Moreover, the block and transaction size limit is a significant barrier to the use of the main blockchains by most of the professional entities because they limit the quantity of information to a few kB. For this reason, a solution of sub blockchain networks is being developed with the aim to answer the customized needs of the corporations. At the same time, sub blockchain networks can be an answer to scalability as any sub blockchain can be used to perform transactions off the main blockchain. This has a great potential more particularly with regards to electronic payment [21] where the fees on the main blockchain would not allow micropayments.

2) Sidechains Networks

a) Information Network

Information networks can be seen as semi-private networks where only some limited participants are allowed to perform transactions. But the network doesn't remain entirely private as sidechains need to incorporate mainchain Masternodes to be operable. For these reasons, they are also displayed to the public but given no access nor view keys granted to them, the content remains inaccessible.

The main functionality of information networks relies on the possibility to add additional information in any tx block. There is no limit to the type or the size of the added data besides the ones set at the inception of the chain. This solution is designed to become an easy way for a group of (most likely) corporations or banks to share documents and files, digitally signed and time stamped. The two main advantages behind this solution over the traditional method are the high speed of execution (minutes) and minimal costs (the annual cost of a sidechain network of 20 nodes would be less than $10,000 from a hardware perspective) [22].

There are several potential use cases for this technology, and new applications to discover. It is possible to imagine a network of banks running a sidechain network to settle their major

transactions. This potential use is often cited as one of the most promising blockchain applications for the financial services industry [22]. Banks & corporations could also share a network where they would digitally share letters of credit without the need to disclose it to other members. Similarly, contracts of propriety could be exchanged on a sidechain network. On these aspects, the main challenge is not technical but more on the recognition of the legal nature of these agreements.

b) Payments Networks

As X-CASH will be gaining traction, it will become quickly congested with transactions, especially if the payment gateway proves to be successful and cost-efficient. For this reason, it is essential to enable off chain transactions, or micropayments will become impossible as transaction fees will shoot up.

One of the ways to do this is to create sidechains which will share the same characteristics from a transaction perspective as the main chain. The goal of these chains is to find the best tradeoff between a lower decentralization and a cost efficiency while guaranteeing a satisfactory level of privacy. It can be easily argued that a transaction happening in a country does not have to be witnessed by servers on the other side of the world, but it is still yet to be determined at which level payments sidechains should be created: geographical (country, city district…etc.), sectorial or by the entity handling the payment. The suggestion behind this last possibility is that every bank could run their own network(s), which also raises questions from a regulatory perspective.

VI. Increasing Liquidity and Reducing Volatility through Derivatives Instruments

One of the main components of the fee described in section V.A.6) is the market spread between XCASH and the other altcoins. This spread arises from two major sources which are the volatility of the pair and its liquidity which are also tightly linked.

One of the effective methods to reduce volatility is to introduce derivatives instruments [22] [23]. This is especially true for cryptocurrency where this has been witnessed in the Bitcoin market [24]. With regards to X-CASH, there is a similar goal that can be split into two steps.

The first one will be the introduction of futures instruments which will increase the liquidity and reduce the market impacts of large XCASH to FIAT conversion. They will also enable an easier hedging of the market-making trading books while spreading the settlement of the contracts over time.

The second planned instruments are the release of options. The goal of these derivatives will be similar to futures, but they will also enable the market-making books to be covered against spikes in prices by keeping a long volatility. Overall the combination of these two instruments should reduce and neutralize the volatility of the XCASH to ALT conversion spread.

VII. Conclusion

The X-CASH Project aims at offering an effective payment solution using cryptocurrencies. By developing an easy to use API and platform that connects users, markets, and merchants, this solution has been created to become a standard in digital payment, notably thanks to low processing fees.

As its main objective is to satisfy the network needs, X-CASH will integrate a functionality for users to make the details of their transaction public. This will also be an important step towards meeting the growing regulations regarding blockchain technology.

Finally, by improving the network, switching to PoS, and enabling sidechains network, X-CASH hopes to tackle the scalability of its payment grid while meeting corporations' needs for zero-knowledge proof information systems.

VIII. BIBLIOGRAPHY

[1] Capgemini, "World Payments Report 2017," 2017.

[2] CoinMarketCap, "Global Charts - Total Market Capitalization," [Online]. Available: https://coinmarketcap.com/charts/.

[3] bitcoinfees, "Historic daily average Bitcoin transaction fees (in dollars per transaction)," [Online]. Available: https://bitcoinfees.info.

[4] A. I. Joy, "THE FUTURE OF CRYPTO-CURRENCY IN THE ABSENCE OF REGULATION, SOCIAL AND LEGAL IMPACT".

[5] "X-CASH - Global blockchain network to receive & send payments across the world using cryptocurrency," X-CASH, [Online]. Available: https://www.x-cash.org.

[6] T. M. Project.. [Online]. Available: https://github.com/monero-project/monero.

[7] "An open-source technology and concepts for the cryptocurrencies of the future," [Online]. Available: https://cryptonote.org/.

[8] M. J. T. N. N. A. M. J. Seigen, "CRYPTONOTE STANDARD 008 : CryptoNight Hash Function".

[9] "SHA-3," [Online]. Available: https://en.wikipedia.org/wiki/SHA-3.

[10] X-CASH, "X-CASH Explorer," [Online]. Available: https://explorer.x-cash.org/.

[11] R. Mercer, "Privacy on the Blockchain: Unique Ring Signatures".

[12] R. M. Nicolas T. Courtois, "Stealth Address and Key Management Techniques in Blockchain Systems".

[13] Monero, "Monero - Stealth Addresses," [Online]. Available: https://getmonero.org/resources/moneropedia/stealthaddress.html.

[14] J. B. D. B. A. P. P. W. a. G. M. Benedikt Bünz, *Bulletproofs: Short Proofs for Confidential Transactions and More.*

[15] S. Noether, 07 12 2017. [Online]. Available: https://getmonero.org/2017/12/07/Monero-Compatible-Bulletproofs.html.

[16] Smartereum, "Japan's Financial Regulators want Cryptocurrency Exchanges to delist hard-to-track coins.," [Online]. Available: https://smartereum.com/11843/japans-financial-regulators-want-cryptocurrency-exchanges-to-delist-hard-to-track-coins/.

[17] Cryptobriefing, "Privacy coins under threat regulation - Governments: Privacy Is Bad. Everyone Else: No It's Not.," [Online]. Available: https://cryptobriefing.com/privacy-coins-under-threat-regulation/.

[18] X-CASH, "X-CASH - Official remote nodes," [Online]. Available: https://x-cash.org/remotenodes/.

[19] BitFury Group, "Proof of Stake versus Proof of Work".

[20] D. D. Evan Duffield, "Dash: A Privacy-Centric Crypto-Currency".

[21] "CoinWatch," [Online]. Available: https://coinwatch.center.

[22] "MyNode," [Online]. Available: https://mynode.rocks/.

[23] Forbes, "Explaining Side Chains, The Next Breakthrough In Blockchain," [Online]. Available: https://www.forbes.com/sites/shermanlee/2018/02/07/explaining-side-chains-the-next-breakthrough-in-blockchain/#795c287d52eb.

[24] O. Hueber, "The blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework".

[25] X-CASH, "Memo on sidechain network: characteristics, pricing and transaction output".

[26] Techcrunch, "Bank-based blockchain prokects are going to transform the financial services industry," [Online]. Available: https://techcrunch.com/2018/01/28/bank-based-blockchain-projects-are-going-to-transform-the-financial-services-industry/?guccounter=1.

[27] A. S. Nair, "Impact of Derivative Trading on Volatility of the Underlying: Evidence from Indian Stock Market".

[28] S. N. P. N. Drimbetas Evangelos, "The effect of derivatives trading on volatility of the underlying asset: evidence from the Greek stock market".

[29] S. Shi, "The Impact of Futures Trading on Intraday Spot Volatility and Liquidity: Evidence from Bitcoin Market".