Whitepaper

Umbru aims to provide users and developers a first class experience while employing next generation tools and software.

Version 1.0

Contents

CHAPTER 1

INTRODUCTION

The technologies and protocols of the Umbru network allow for a decentralized, self funding governance platform. It also allows for tools and software to be developed to expand and enhance features on the network.

1. Abstract

Dash with its uprages from the Bitcoin codebase and protocols represented a jump forward for further decentralization of cryptocurrencies. However, Dash was launched in 2014 and further developments are needed to facilitate a faster, more secure and anonymous private cryptocurrency. Umbru aims to take the core upgrades that Dash has developed and expand on the ideology of a decentralized, private, secure and anonymous cryptocurrency.

Umbru builds upon the Dash codebase, incorporating several core features. Including the deterministic decentralized masternode system, blockchain governance and network budget and funding systems.

Bitcoin is the root and foundation for cryptocurrency infrustructure, it is the 'gold standard' when it comes to digitally storing value. One thing Bitcoin and its successors have failed to acheive is scaling as a decentralized, private and anonymous payment system. Transaction details are never completely anonymous due to the nature of its transactions and public ledger. Transactional data can be analyzed and followed undermining any online privacy required. This creates a permanent public trail of all transactions past and present. Bitcoin and most of its successors transactions are pseudonymous and not private and/or anonymous.

Created in 2019, Umbru visions a fully decentralized, private, anonymous and secure blockchain. Where users and merchants can take/make transactions without the risk or worry of transactions and/or infomation becoming available to the public. Privacy in this day and age is a nescessity and not something to be bargained with.

The network launched with no ICO, no premine, development funds or fees and is secured by Proof-of-Work and chainlocks to ensure a fair distribution. It is secured by proof-of-work (mining) using the X25X hashing algorithm created by Sinovate, which is an ASIC, FPGA, Quantam Resistant algorithm ensuring a further decentralized network.

2. Network

2.1. Decentralized Governance

Umbru's choice on how to solve two important problems in cryptocurrency: governance and funding. Governance in a decentralized project is difficult, because by definition there are no central authorities to make decisions for the project. In Umbru, such decisions are made by the network, that is, by the owners of masternodes. The governance system allows each masternode to vote once (yes/no/abstain) for each proposal. If a proposal passes, it can then be implemented (or not) by Umbru's developers.

2.2. Masternodes

In addition to traditional Proof of Work (PoW) rewards for mining Umbru, users are also rewarded for running and maintaining special servers called masternodes. Thanks to this innovative two tier network, Umbru can offer innovative features in a trust-less and decentralized way. Masternodes are currently used to power the governance and treasury system. Users are rewarded for running masternodes; starting at 20% of the block reward increasing 5% monthly until 50% is allocated to pay the masternode network.

Masternodes enable the following services:

ChainLocks, which protects the Umbru blockchain against 51% mining attacks by signing blocks as they are mined.

Governance and Treasury, allows masternode holders to determine the direction of the project and devotes 10% of the block reward to development of the project and ecosystem.

Masternode owners must have possession of 5000 UMBRU, which they prove by signing a message included in a special transaction written to the blockchain. The Umbru can be moved or spent at any time, but doing so will cause the masternode to fall out of queue and stop earning rewards. Masternode users are also given **voting rights** on proposals. Each masternode has one vote and this vote can be used on budget proposals or important decisions that affect Umbru.

Masternodes cost money and effort to host so they are paid a percentage of the block reward as an incentive. Because only one masternode is paid in each block, the frequency of the payment can vary, as well as the value of the Umbru paid out. There is also the possibility for masternodes to earn money from fees in the future.

10%

Of each block reward is held by the network for the monthly budget.

Proposals are created/voted on each month from the total pool available. If the budget is not spent it is not carried over to the next month.

3. Technologies

MASTERNODES

In addition to traditional Proof of Work (PoW) rewards for mining Umbru, users are also rewarded for running and maintaining special servers called masternodes. Thanks to this innovative two tier network, Umbru can offer innovative features in a trust-less and decentralized way. Masternodes are currently used to power the governance and treasury system.

DARK GRAVITY WAVE

DGW or Dark Gravity Wave is an open source difficulty-adjusting algorithm for Bitcoin-based cryptocurrencies that was first used in Dash and has since appeared in other digital currencies. DGW was authored by Evan Duffield, the developer and creator of Dash, as a response to a time-warp exploit found in Kimoto's Gravity Well.

CHAINLOCKS

ChainLocks are a feature provided by the Umbru Network which provides certainty when accepting payments. This technology creates an environment in which payments can be accepted immediately and without the risk of "Blockchain Reorganization Events".

X25X ALGORITHM

Umbru uses the X25X Proof-of-Work algorithm created and used by the Sinovate project, which is an ASIC, FPGA, Quantam Resistant algorithm ensuring a further decentralized network.

4. Project Overview

4.1. Why Umbru?

Created in 2019, Umbru visions a fully decentralized, private, anonymous and secure blockchain. Where users and merchants can take/make transactions without the risk or worry of transactions and/or infomation becoming available to the public. Privacy in this day and age is a nescessity and not something to be bargained with.

The network launched with no ICO, no premine, development funds or fees and is secured by Proof-of-Work and chainlocks to ensure a fair distribution. It is secured by proof-of-work (mining) using the X25X hashing algorithm created by Sinovate, which is an ASIC, FPGA, Quantam Resistant algorithm ensuring a further decentralized network.

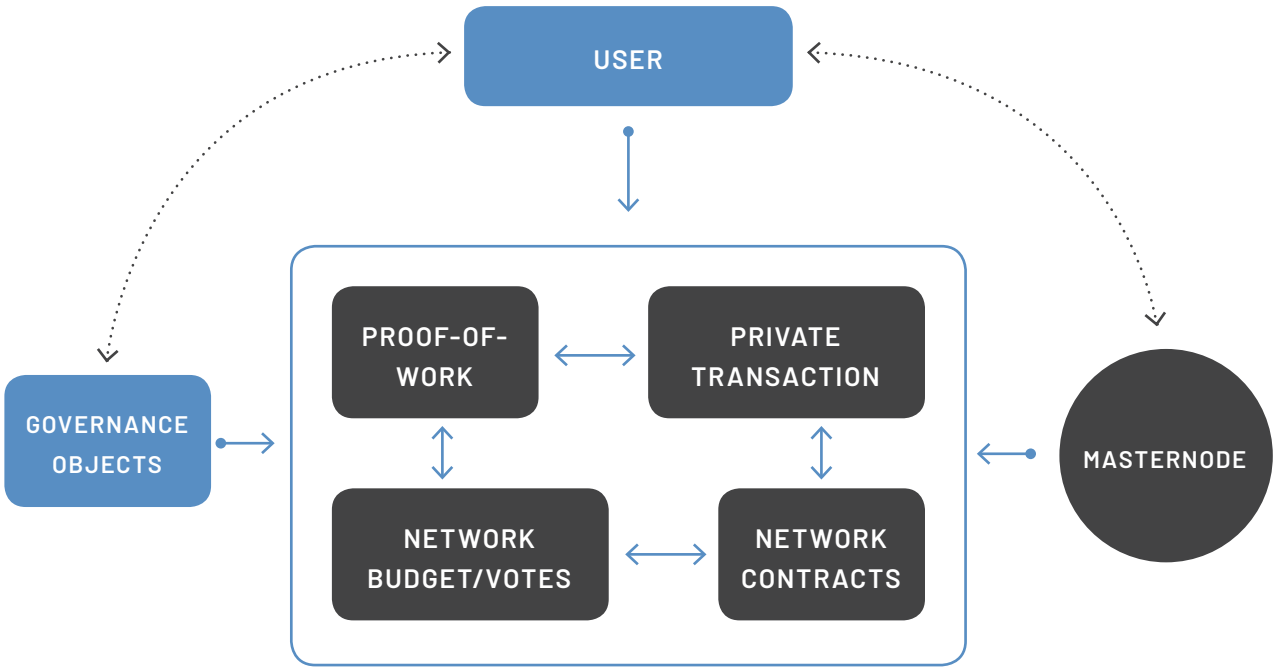
4.2. Problems

The major problems we have seen with successors of Bitcoin is either the lack of privacy, scalability or incetive to help decentralize the network. Most projects seem to focus on one of these issues but lack direction or motivation to include the other. Umbru aims to focus on all negative aspects seen in projects and come up with fast, secure and stable solutions for all.

Blockchain Reorganization Events - The risk of blockchain reorganization is typically addressed by requiring multiple "confirmations" before a transaction can be safely accepted as payment. This type of indirect security is effective, but at a cost of time and user experience. ChainLocks are a solution for this problem.

Project Funding - Decentralized Governance, is Umbru's choice on how to solve two important problems in cryptocurrency: governance and funding. Governance in a decentralized project is difficult, because by definition there are no central authorities to make decisions for the project. In Umbru, such decisions are made by the network, that is, by the owners of masternodes.

Initial features have been cherry picked to create a stable, fast and secure base for Umbru to build upon. Dash's masternode and governance system is the most ideal base for our decentralized, self funded and secure blockchain providing features to protect against network and blockchain attacks. On this basis we can then work on implementing the features missing - privacy and scalability.



Tier 2 Network Layerss

4.3. Solutions

The blockchain itself is the first layer with the second tier layer being built upon it. With this second tier layer Umbru can offer innovative features in a trust-less and decentralized way. Masternodes are currently used to power the governance and treasury system, in the near future they will be used to power features outlined in this Whitepaper and more. Providing a truely decentralized layer for future features, Masternodes are also reimbursed by block rewards for their contribution to helping decentralize the network.

This also allows Umbru to create private, anonymous and trust-less transactions in the near future providing users and business the privacy and security the deserve and need. Network contracts are also enabled with this tier 2 layer providing another source of decentralization not seen in many of Bitcoin's successors.

Decentralized Governance, is Umbru's choice on how to solve two important problems in cryptocurrency: governance and funding. Governance in a decentralized project is difficult, because by definition there are no central authorities to make decisions for the project. In Umbru, such decisions are made by the network, that is, by the owners of masternodes.

5. Distribution Model

5.1. Proof-of-Work (Mining)

Mining in the context of cryptocurrency such as Umbru refers to the process of searching for solutions to cryptographically difficult problems as a method of securing blocks on the blockchain. The process of mining creates new currency tokens as a reward to the miner. Mining is possible on a range of hardware. Umbru implements an algorithm known as X25X, which the miner must solve in order to earn rewards. The simplest and most general hardware available for mining is the general purpose CPU present in every computer. A CPU is designed to be versatile but offers less efficiency than a GPU, which is designed to rapidly calculate millions of vectors in parallel. While specific CPU instruction enhancements related to cryptography such as AES or AVX can provide a decent boost, GPUs offer a significant performance increase due to their multiple pipelines capable of processing the predictably repetitive calculations associated with cryptocurrency mining.

5.2. Masternodes

Umbru works a little differently from Bitcoin, however, because it has a two-tier network. The second tier is powered by Masternodes, which enable network functions, and the decentralized governance and budget system. Because this second tier is so important, masternodes are also rewarded when miners discover new blocks. The breakdown is detailed in the table below. The masternode system is referred to as Proof of Service, since the masternodes provide crucial services to the network.

Block Reward Breakdown

MONTH	MINERS	MASTERNODES	BUDGET
1	70%	20%	10%
2	65%	25%	10%
3	60%	30%	10%
4	57.5%	32.5%	10%
5	55%	35%	10%
6	52.5%	37.5%	10%
7	50%	40%	10%
8	47.5%	42.5%	10%
9	45%	45%	10%

6. Overview

Short overview of current, planned and future features of the Umbru blockchain and tier 2 network.

Decentralized

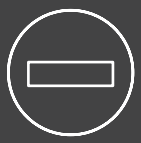
No governing body over the Umbru blockchain. Direction of project voted on by community members and their feedback/input. Trustless system resistant to centralization attempts.

Transparency

All voting and proposals available to view at any time through the Umbru wallet and Governance UI making voting, creating proposals and giving feed back nice and easy.

Security

Our tier 2 layer provides blockchain security through ChainLocks to create an environment that is resistant to 'blockchain reogranization attacks' (51% attacks)



Irreversibility

All transactions whether anonymous, private, shielded or normal are recorded in the blockchain and protected by LLMQ members (Masternode holders) allowing instant confirmations in the future.

Scalable

With UmbruScript the number of private networks, assets/tokens that can be integrated within the Umbru network are unlimited. Each addition can run a specific application or multiple funcitons.

Data

Apart from the security of private networks/ applications by using Umbru enterprises and institutions will be able to access an enterprise ready solution for applications and/or functions.

CHAPTER 2

UMBRU PROJECT

7. The Vision

7.1. Our vision helps users to maintain fundamental rights

DDPS (Dynamic, Decentralized, Private and Secure) is the vision of Umbru. Fundamental rights are just that, not optional, not privelaged a basic human essential. We are commited to provide a network where you do not need to be constantly worried about your privacy. Or that a higher governing body is controlling you or the network. Umbru aims to provide this in a safe and secure environment that is easily adaptable and dynamic for problems that arrise. If you believe in our vision join our community board and have your say in what/where/how Umbru should head!

DYNAMIC | DECENTRALIZED | PRIVATE | SECURE

PRIVACY

Transactional privacy is a necessity, not just for users but also businesses and institutions that wish to build upon the Umbru network.

Using zk-STARKS and our second tier layer (masternodes in particular) we aim to provide a fully trust-less decentralised payment and transaction system.

Gone are the days where you have to worry if your financial transaction and payment history is bundled and sold to third parties.

Long term we aim to include these private or anonymous transactions into our instantaneous zero confirmation transactions. Eliminating the need to wait potentially several minutes plus to confirm on the network.

Businesses, institutions, investors, miners and end users all benefit from this.

DECENTRALIZED

The Umbru network has no governing body. Miners secure the network through their proof-of-work and Masternodes enforce a decentralized consensus.

Our tier 2 network layer of Masternodes and governance objects further enforce this ideology. This network layer also allows for a fully decentralized self funding network budget.

This budget can be accessed by all, proposals can be generated by anyone who wishes to gain funding for services provided to improve and adapt Umbru.

These proposals are then voted on by Masternode holders ensuring a fair and tamper free consensus.

8. Umbru Labs

DEVELOPMENT FUND PROPOSAL

The Umbru labs is a network funding proposal to provide a budget for the Core developers to maintain and improve Umbru in its infancy. Its main purpose is to provide funding for research and development, cover costs of development and increase awareness through social media and marketing.

FULLY TRANSPARENT

Funding provided by the network is fully transparent with any payments made or recevied available for anyone to audit at any stage they wish. Monthly financial statements will also be issued by the Umbru Core team to ensure everyone is kept up-to date with expenditure and progress.

OPEN SOURCE

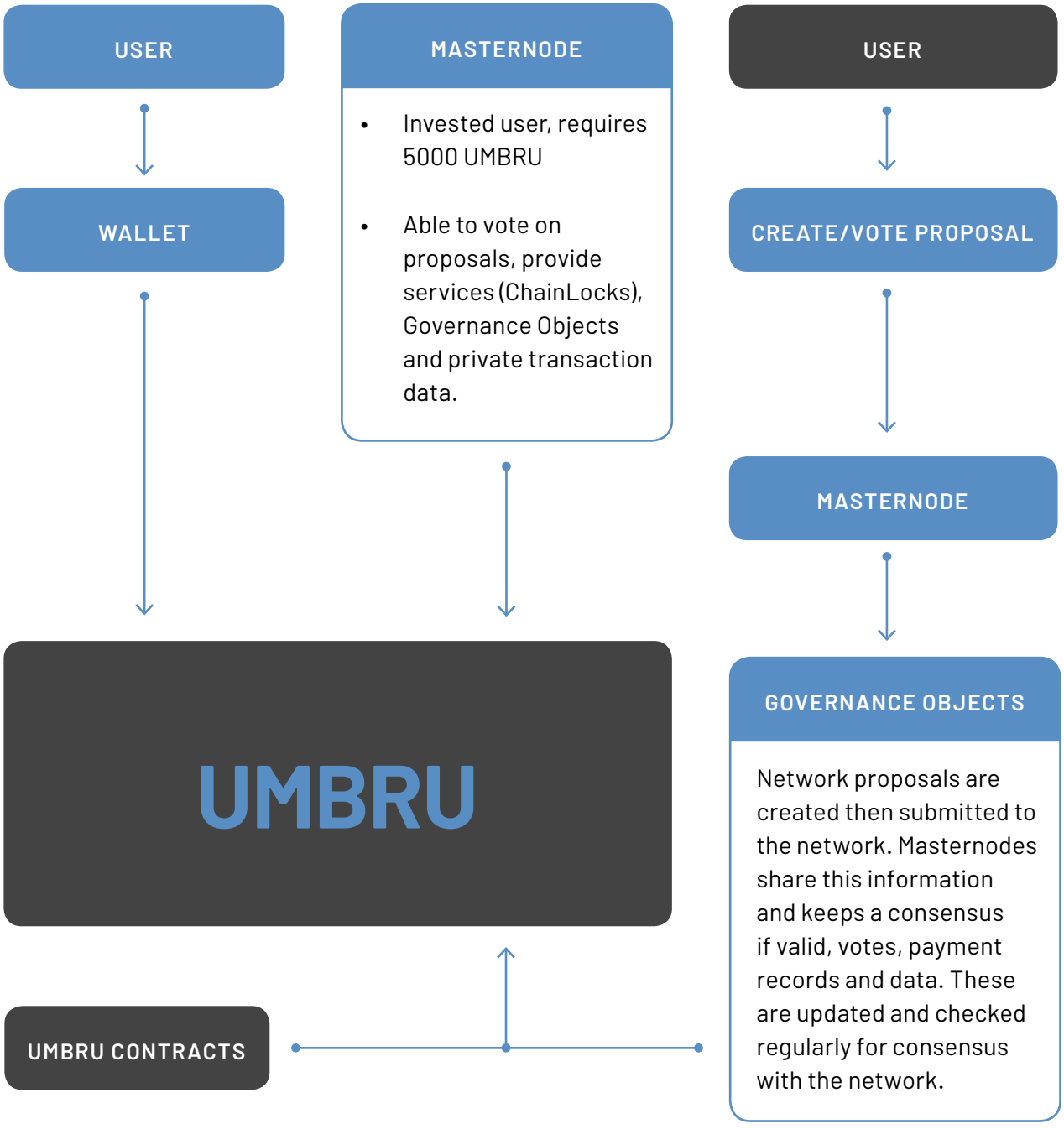
We believe that open source is the future. All tools, software and programs developed with funds provided by the Umbru Labs will be made open-source and auditable. This also aligns with our fully transparent ideology and also lets other users/developers catch any potential risks/bugs in any code.

FEEDBACK/SUPPORT

We will always welcome feedback and support. We realise that there is never a wrong way to go about things so your feedback and support is appreciated and requested. Umbru is as much yours as it is the Core developers so please speak up and have your say!

9. Protocol Architecture

User and network interaction detailed below. Umbru is a Tier 1 layer with the following Tier 2 protocols added below. Protocols and layers are continuously updated, increased or decreased as development continues.



10. Roadmap

Q3 2019

- Umbru Genesis block mined and network launch.

Q3 2019

- Official mining pool launch.
- Block explorer, API and website launched.
- Network tools, Wallets and Media available.
- Trezor hardware wallet support submitted and accepted.

Q4 2019

- Mobile Android/iOS Wallets released.
- Umbru labs proposal created for voting.

Q4 2019

- Exchange and service listings announced.
- Markting campaign.

Q4 2019

- Instantaneous zero confirmation transactions deployed on testnet.

Q1 2020

- Tumbru zk-STARK trustless transactions implementation on testnet.

Q1 2020

- Multi-asset/currency Umbru wallet, with updated UI/UX.
- Payment gateway integration with new wallet, developer toolkit released with launch.

Q2 2020

- Proposal/Governance web UI and wallet interface for users/developers to interact and create.

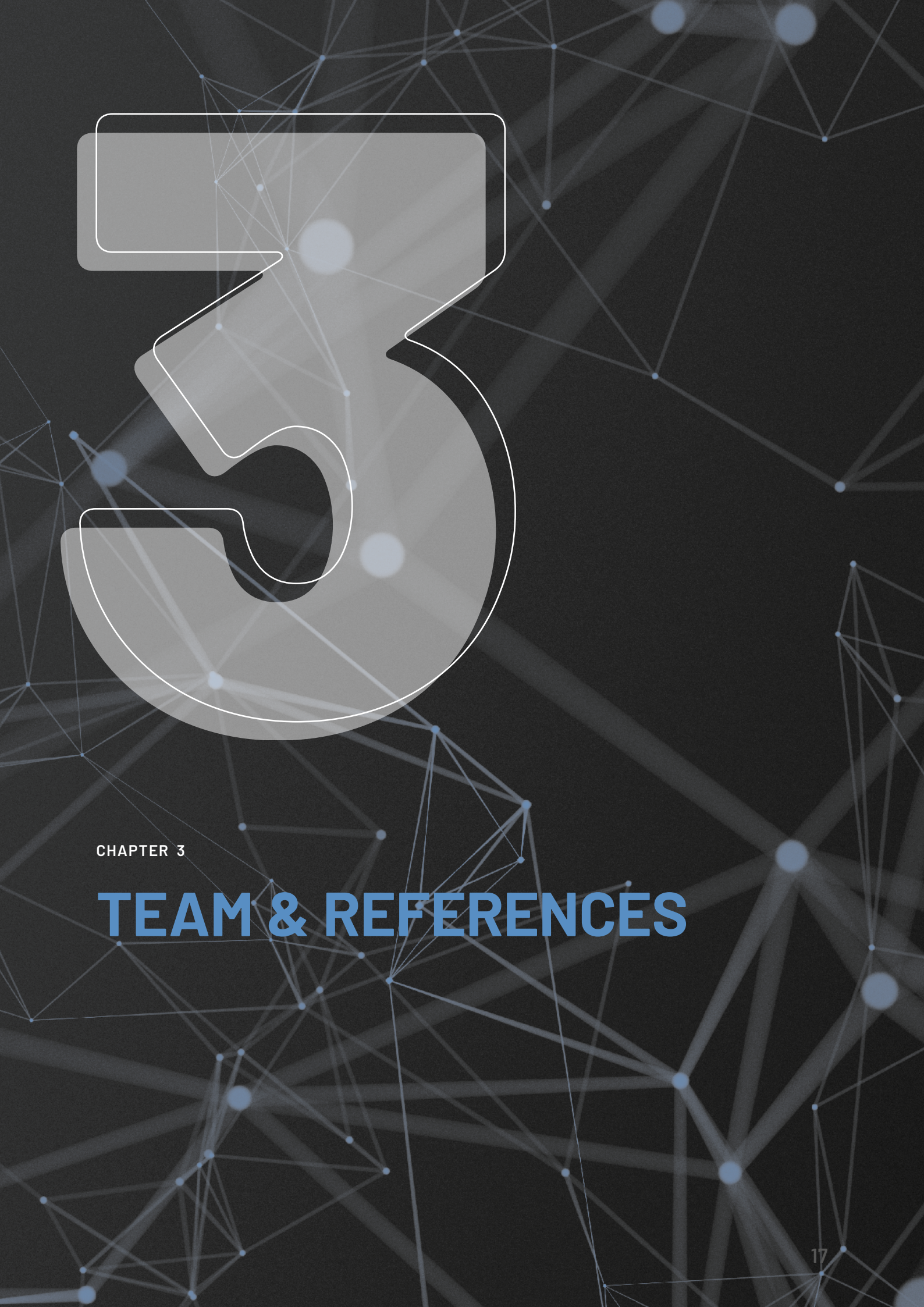
Q2 2020

- UmbruScript multi/cross chain decentralized contracts.

Q3+ 2020

Futher development (additions/removals) will be based upon feedback and votes on proposals generated.

Community lead development/initiatives can also be paid/voted on this way.



CHAPTER 3

TEAM & REFERENCES

11. Management Team

Founder

Ryan Lorz, Founder and Developer

What started off as a curiosity with mining Bitcoin, transitioned from curiosity to hobby and now Umbru. Ryan's technical and entrepreneurial background helps develop maintain and market the Umbru umbrella of projects. Ryan loves a good laugh and socializing when you can pry him away from the keyboard and the large lists of tasks to be completed.

Community Members

Bryan Evans, Social Media/Support

12. References

[1] https://sinovate.io/whitepaperv2light.pdf - X25X Algorithm
[2] https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof - zk-STARKS
[3] https://en.bitcoin.it/wiki/Mining - Bitcoin Mining
[4] https://docs.dash.org - Dash background
[5] https://docs.umbru.io - Umbru documentation
[6] https://umbru.io/ - Umbru website
[7] https://pool.umbru.io/ - Official mining pool

13. Legal Note

THIS WHITEPAPER AND THE DETAILS HEREIN ARE BEING MADE AVAILABLE SOLELY FOR GENERAL INFORMATIONALPURPOSES.

NO ONE, INCLUDING BUT NOT LIMITED TO, ANY DEVELOPERS ASSOCIATED WITH OR FOUNDERS OF UMBRU WARRANT THE ACCURACY, COMPLETENESS, OR USEFULNESS OF THIS INFORMATION. THIS WHITEPAPER IS NOT A CONTRACT OF ANY KIND, INCLUDING AN INVESTMENT CONTRACT.

UMBRU WILL BE FULLY FUNCTIONAL FROM BLOCK ONE, AND YOUR CHOICE TO USE THE UMBRU NETWORK DOES NOT GIVE RISE TO A LEGAL RELATIONSHIP WITH ANYONE.

UMBRU IS A DECENTRALIZED CRYPTOCURRENCY NETWORK, NOT A COMPANY. THUS, YOU SHOULD NOT EXPECT ANY PROFITS, DIVIDENDS, EARNINGS, OR PRICE APPRECIATION OF ANY KIND IN CONNECTION WITH THE EFFORTS OF ANY OTHER USERS OR
CONTRIBUTORS TO UMBRU.

UNDERSTANDING VIRTUAL CURRENCY, SUCH AS UMBRU, REQUIRES ADVANCED TECHNICAL KNOWLEDGE. THE TECHNOLOGY BEHIND VIRTUAL CURRENCY IS NOVEL AND RELATIVELY UNTESTED. VIRTUAL CURRENCY IS OFTEN DESCRIBED IN EXCEEDINGLY TECHNICAL LANGUAGE THAT REQUIRES A COMPREHENSIVE UNDERSTANDING OF APPLIED CRYPTOGRAPHY AND COMPUTER SCIENCE IN ORDER TO APPRECIATE THE INHERENT RISKS.

PLEASE USE UMBRU AT YOUR OWN RISKS.