|  |  |
| --- | --- |
| EN | RU |
| **Detailed analysis of Decred fork resistance**  Dec 12, 2018  It is not a secret anymore that pure PoW networks are vulnerable to forking. We have witnessed the creation of several minority forked coins, most notably Ethereum Classic, Bitcoin Gold, Bitcoin Cash, and Bitcoin SV.  This post explains how the Decred network prevents minority forks, based on an analysis originally [posted on Reddit](https://www.reddit.com/r/decred/comments/7f9ie1/detailed_analysis_of_decred_fork_resistance/) by davecgh.  It describes important aspects of Decred’s hybrid Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus system and provides a detailed walkthrough of what would happen if any entity attempted to split the Decred blockchain.  If you need a reminder on why forks should be avoided, read this article:  [Blockchain forks and chain splits: why we should avoid them. Everyone with an interest in blockchain technology or cryptocurrency has heard about the concept of forking. Although…blog.goodaudience.com](https://blog.goodaudience.com/blockchain-forks-and-chain-splits-why-we-should-avoid-them-f54c693a90f1)  **Preliminary knowledge**  The Decred network is secured by both PoW miners and PoS voters.  The PoS voting system works by locking up chunks of coins into what is called a *voting ticket*.  These tickets function as fundamental building blocks which allow stakeholders to participate in [Decred’s governance](https://docs.decred.org/governance/introduction-to-decred-governance/" \t "_blank).  Per block, maximum 20 new tickets are available.  Once acquired, there is a 256-block maturity period after which the ticket is placed into the live ticket pool.  This pool has a target size of 40960 tickets, but it can grow or shrink throughout the course of operation. PoS difficulty (ticket price) is adjusted via supply and demand to maintain the 40960 target size.  The algorithm that controls the ticket price is described in [DCP0001](https://github.com/decred/dcps/blob/master/dcp-0001/dcp-0001.mediawiki).  Live tickets are waiting in the pool to cast their vote and the selection process is impossible for PoW miners to manipulate.  The algorithm that controls ticket selection is primarily based on the hash of the previous block, which means it is both pseudorandom and deterministic.  If you are building block 100 on top of block 99, the tickets to be included in block 100 are known to every full node on the network.  Ticket selection can only be changed by finding a new solution to block 99 with a different hash, which in turn would cause a new set of random tickets to be selected for voting eligibility.  Each block, 5 tickets are eligible to vote. At least 3 out of the 5 votes must be included in the block, otherwise it will not be accepted by the network.  The reward for PoW miners is reduced if only 3 or 4 votes are included, by 40% and 20%, respectively, to discourage miners from ignoring votes and in that way attempting to game the system.  It is important to note that stakeholders **must be present** on a given chain fork when their tickets are selected.  The act of acquiring a ticket does not mean it automatically votes, your wallet (or your Voting Service Provider) has to cast your vote when the ticket is selected. This distinction is key because it means that the live ticket pool on a minority fork is largely comprised of non-voting tickets, since its owners are on another chain.  A detailed treatment of the theory behind each of these aspects is beyond the scope of this post, however, it primarily has to do with protection against various adversarial situations.  **Scenario, Assumptions, and Methodology**  With all of this in mind, let’s imagine a scenario in which an entity attempts to create a fork that 75% of the stakeholders don’t agree with.  Let’s assume that both sides of the attempted fork have equal hash power (so 50% hash power on each fork).  As stated, 75% of the stakeholders are on the majority chain, while 25% are on the minority chain.  Further, let’s assume the most recent block at the point of the fork is block 99999. Thus both sides of the fork are working on finding block 100000, one side on the minority rule set, the other side on the majority rule set.  Finally, in order to simplify the description and make it easier to follow the logic, since only 25% of the stakeholders are on the minority chain, let’s say that every 4th ticket in the live ticket pool is a stakeholder on the minority chain.  In other words, ticket numbers 0, 4, 8, 12, 16, 20, …, 40956 are tickets in the live pool which represent stakeholders on the minority chain, while ticket numbers 1, 2, 3, 5, 6, 7, 9, …, 40957, 40958, 40959, are tickets in the live pool which represent stakeholders on the majority chain.  Remember: stakeholders **must be present** on a given chain fork when their tickets are selected to successfully cast their votes.  Illustration of the imaginary scenario.  **Step-by-step walkthrough**  The following is a sequence of events that would happen in the scenario of a forking attempt, as described and illustrated above.  **Block 100000**   * The hash power on both chains will try to build a new block on top of block 99999. * In order for this new block to be built on the minority chain, it needs to acquire at least 3 votes from the live ticket pool and the selected votes depend on block 99999. * The tickets required to build block 100000, based on a block 99999 hash, are ticket numbers 17113, 17331, 21307, 21328, and 24903. * As we can see, 4 out of those 5 tickets are stakeholders on the majority chain (ticket numbers 17113, 17331, 21307, and 24903), which means they are going to cast their votes for block 100000 on the majority chain. * The minority chain is only able to acquire 1 vote (ticket number 21328), so it can’t build a block 100000. Instead, it must go back and find a new solution to block 99999 to cause a new set of tickets to be selected.   At this point, the chains look as follows. Parentheses with the \* in this notation indicate blocks that are being worked on.  ... -> [99999] -> (100000\*) majority stakeholders (75%) are on this chain  \-> (99999a\*) minority stakeholders (25%) are on this chain  In other words, the majority chain is now working on block 100000, while the minority chain is stuck trying to find a new solution for block 99999 in order to get a new set of tickets hoping this time they’ll be able to get at least 3 votes.  Since, per our thought experiment, both chains have equal hash power, we can safely assume that, on average, both block 100000 on the majority chain and new block 99999 (call it 99999a) on the minority chain will be found around the same time.  **Block 100001**  At this point, the following will happen:   * The hash power on the majority chain will try to build a new block on top of the majority chain’s block 100000. The votes required for this block are ticket numbers 563, 6766, 21009, 37394, and 37775. * This time, all 5 out of those 5 tickets happen to be stakeholders on the majority chain, which means they are going to provide their votes for block 100000 on the majority chain which allows block 100001 to be built. * The minority chain, now with a new version of block 99999 (99999a) has a new hash, so it ends up requiring ticket numbers 1069, 8007, 16413, 19172, and 31821. * The minority chain is still only able to acquire 1 vote (ticket number 19172), so it must once again go back and find yet another new solution to block 99999 in order to cause a new set of tickets to be selected.   The chains now look as follows:  ... -> [99999] -> [100000] -> (100001\*)  majority stakeholders (75%) are on this chain  \-> (99999b\*) minority stakeholders (25%) are still on this chain  In other words, the majority chain is now working on block 100001, while the minority chain is still stuck trying to find yet another new solution for block 99999 in order to get a new set of tickets hoping this time they’ll be able to get at least 3 votes.  Since, per our thought experiment, both chains have equal hash power, we can again safely assume that, on average, both block 100001 on the majority chain and a new block 99999 (call it 99999b) on the minority chain will be found around the same time.  **Block 100002**  At this point, the following will happen:   * The hash power on the majority chain will try to build a new block on top of the majority chain’s block 100001. The votes required for this block are ticket numbers 174, 1999, 12808, 31928, and 38317. * This time, 3 out of those 5 tickets are stakeholders on the majority chain (ticket numbers 174, 1999, 38317), which means they are going to provide their votes for block 100001 on the majority chain which allows block 100002 to be built. * The minority chain, now with a new version of block 99999 (99999b) has a new hash, so it ends up requiring ticket numbers 4653, 15211, 29988, 35175, and 35665. * The minority chain is still only able to acquire 1 vote (ticket number 29988), so it must once again go back and find yet another new solution to block 99999 in order to cause a new set of votes to be selected.   The chains now look as follows:  ... -> [99999] -> [100000] -> [100001] -> (100002\*) majority stakeholders (75%) are on this chain  \-> (99999c\*) minority stakeholders (25%) are still on this chain  In other words, the majority chain is now working on block 100002, while the minority chain is still stuck trying to find yet another new solution for block 99999 in order to get a new set of tickets hoping this time they’ll be able to get at least 3 votes.  **Fast-forward to Block 100010**  The process repeats until, eventually, some variant of block 99999 on the minority chain gets lucky and happens to select 3 tickets that are on the minority chain.  This turns out to be roughly 1 in 10 tries. So, fast forwarding a bit to see the chain by the time this happens, the chains would look as follows:  ... -> [99999] -> [100000] -> [100001] -> [100002] -> ... -> [100009] -> (100010\*) majority stakeholders (75%) are on this chain  \-> [99999j] -> (100000a\*) minority stakeholders (25%) are still on this chain  It should be pretty clear, since both chains have equal hash power, there is no way the minority chain can now ever catch up to the majority chain. Furthermore, the same process is going to repeat for the minority chain’s block 100001 where it will have to go back and remine (find new solutions) for its block 100000 over and over until it gets a lucky draw again such that it gets the 3 votes it needs.  Consequently, *miners are not going to stay* on the minority chain because they are hardly getting any rewards.  The minority chain will never be profitable and hence all mining power will eventually return to the majority chain.  **Common objections**  **What if the minority chain gets more than 10x the hash power of the main chain?**  Theoretically, if the minority chain with only 25% stakeholder approval had 10x the hash power of the main chain, yes, it could keep up with the majority chain.  However, this is not a realistic scenario because of the economic incentives.  Mining the minority chain with 10x the hash power effectively means that the miners would only be getting 1/10 of the block reward as they would on the majority chain, based on hash power alone.  In our scenario it’s reduced even further to 1/10 of 60% due to only being able to include 3 votes on average.  In other words, miners would only receive 6% of the rewards they would by mining the majority chain.  Looking at it from another angle, they would receive 94% less by mining the minority chain.  Putting that into numbers, if a miner had, say 5% of the total network hash power, they could expect to receive roughly 5% of the PoW reward per block, or 5% of ~13.89 ≈ 0.6945 DCR at the [current time](https://www.reddit.com/r/decred/comments/7f9ie1/detailed_analysis_of_decred_fork_resistance/).  However, on the minority chain, first the reward would be 60% of ~13.89 ≈ 8.334 DCR, and then that 5% hash power would only be 0.5% of the total hash power on the minority chain, thus 0.5% of ~8.334 ≈ 0.04167 DCR.  Looking at the numbers, we can see that 0.04167 DCR is indeed 6% of 0.6945 DCR.  PoW mining is *very* competitive since it is a zero sum game.  Most miners, even those with huge advantages such as free electricity, have thin margins and are often banking on future appreciation to pick up the slack.  Given the 94% reduction in income, most miners would actually have to pay in order to mine on the minority chain.  **Can’t somebody just change the consensus rules to ignore the stakeholders?**  If the minority chain removed or disabled ticket voting for a certain period of time, it would be able to produce blocks and fork away from the majority chain.  While it is theoretically possible, doing so would completely destroy the hybrid system and return the forked currency to effectively being a pure PoW network.  It would undoubtedly no longer be Decred.  Unlike in pure PoW coins where nobody can say which chain is the “real” one due to the lack of a provable and formalized governance system, Decred has a very clear and well understood governance model.  Decred stakeholders make the decision which chain is the real Decred and they do so in an on-chain and cryptographically provable fashion.  Stakeholders sign up for Decred with the expectation that major consensus decisions are made by the stakeholders themselves.  Removing the authority of the stakeholders would be akin to removing Proof-of-Work from a pure PoW coin.  In other words, it would completely destroy the security properties of the system.  How much confidence are holders going to have in a coin that ignores one of the primary characteristics it claims to offer?  **Conclusion**  Decred’s hybrid PoW and PoS consensus system makes blockchain forks extremely difficult — if not impossible — without majority stakeholder approval.  The walkthrough has demonstrated why a Classic, Gold, or Cash scenario is highly unlikely on the Decred network.  The costs to maintain a minority fork with even 10x of the hash power are substantial; miners can expect a severe reduction in income if they decide to participate.  Alternatively, it is possible to remove or disable the PoS system and split the Decred chain like any other PoW network.  However, this defeats the purpose of Decred and it is doubtful whether anyone would take such an attempt seriously.  Getting the fundamentals of fork resistance right is critical to longevity.  The hybrid PoW and PoS system creates checks and balances to ensure that small groups cannot dominate the flow of transactions or make changes to Decred without agreement among stakeholders.  It incentivizes coordination and collaboration, which turns Decred into an uncommonly strong network that is built to last for the long-term.  **Further reading**  This post has covered the important topic of fork resistance, but there is much more to discover.  For example, the hybrid PoW and PoS system of Decred is also a superior deterrent to majority (51%) attacks. If you want to know how this works, read this post by [Zubair Zia](https://medium.com/@zubairzia" \t "_blank):  [Decred’s hybrid protocol, a superior deterrent to majority attacks This article demonstrates how the unique hybrid protocol of Decred provides superior security against majority attacks.medium.com](https://medium.com/decred/decreds-hybrid-protocol-a-superior-deterrent-to-majority-attacks-9421bf486292)  For more advanced topics, you could investigate how Decred can smoothly upgrade its network via [voting on consensus rule changes](https://medium.com/decred/blockchain-governance-how-decred-iterates-upon-bitcoin-3cc7030c655e), or how people can submit proposals to the [off-chain governance system called Politeia](https://docs.decred.org/governance/politeia/).  If you prefer technical details, check out the [Decred Documentation](https://docs.decred.org/).  Pick one of the chat platforms listed [here](https://www.decred.org/community/) if you want to interact with the Decred community.  We are a pragmatic bunch of people — come join us!  **Credits**  If it wasn’t for the [original analysis by davecgh](https://www.reddit.com/r/decred/comments/7f9ie1/detailed_analysis_of_decred_fork_resistance/), this post would probably not exist. Furthermore, [Artikozel](https://medium.com/@artikozel" \t "_blank)’s review and the constructive comments in the writers room improved this post tremendously. The illustration of the scenario was created by [Zubair Zia](https://medium.com/@zubairzia" \t "_blank). Thank you, all! | **Детальный анализ устойчивости Decred к форку**  12 декабря, 2018  Уже не секрет, что классические сети PoW являются уязвимыми к форкингу. Мы уже стали свидетелями создания миноритарных монет, которые появились в результате форкинга. В первую очередь, речь идёт о Ethereum Classic, Bitcoin Gold, Bitcoin Cash и Bitcoin SV.  В этом посте объясняется то, как сеть Decred предотвращает осуществление миноритарных форков, на основе анализа, изначально [опубликованного davecgh в Reddit](https://www.reddit.com/r/decred/comments/7f9ie1/detailed_analysis_of_decred_fork_resistance/). В нём излагаются важные аспекты гибридной консенсусной системы Decred на основе Proof-of-Work (PoW) и Proof-of-Stake (PoS), а также предоставляется детальный анализ того, к чему приведёт попытка разделить блокчейн Decred.  Эта статья будет полезной для тех, кто хотел бы освежить в памяти причины, по которым следует избегать форков:  [Форки в блокчейне и разделения чейна: Почему мы должны их избегать.](https://blog.goodaudience.com/blockchain-forks-and-chain-splits-why-we-should-avoid-them-f54c693a90f1)  [Каждый, кто интересуется технологией блокчейна или криптовалютами, слышал о том, что такое форкинг. Несмотря на то, что…](https://blog.goodaudience.com/blockchain-forks-and-chain-splits-why-we-should-avoid-them-f54c693a90f1)  [blog.goodaudience.com](https://blog.goodaudience.com/blockchain-forks-and-chain-splits-why-we-should-avoid-them-f54c693a90f1)  **Исходная информация**  Безопасность сети Decred обеспечивается одновременно майнерами PoW и голосующими PoS. Система голосования PoS работает таким образом, что небольшие количества монет складываются в так называемый *«тикет для голосования»* («voting ticket»). Такие тикеты являются фундаментальными строительными блоками, которые позволяют стейкхолдерам участвовать в [Управлении Decred](https://docs.decred.org/governance/introduction-to-decred-governance/).  Максимальное количество доступных новых тикетов на один блок равно 20. Как только они куплены, предусмотрен период созревания (256 блоков), после которого тикет перемещается в пул тикетов «live». Таргетный размер этого пула – 40960 тикетов, но он может расти или сокращаться в ходе операций. Сложность PoS (цена тикета) корректируется посредством спроса/предложения, чтобы поддерживать таргетный размер на уровне 40960 тикетов. Алгоритм, который контролирует цену тикета, описан в [DCP0001](https://github.com/decred/dcps/blob/master/dcp-0001/dcp-0001.mediawiki).  Тикеты «live» ждут в пуле, пока им не будет предоставлено право голоса, и благодаря этому манипулирование процессом отбора майнерами PoW  становится невозможным. Алгоритм, который контролирует отбор тикетов, в первую очередь, базируется на хеше предыдущего блока: это означает, что он является одновременно псевдорандомным и детерминистским. Если вы строите блок 100 на блоке 99, информация о тикетах, включённых в блок 100, передаётся каждой ноде «full» в сети. Отбор тикетов может быть изменён только в том случае, если будет найдено новое решение для блока 99 с другим хешем, который, в свою очередь, формирует новую серию рандомных тикетов, отбираемых для голосования.  В каждом блоке 5 тикетов имеют право голоса. Как минимум 3 из 5 голосов должны быть включены в блок, в противном случае он не будет принят сетью. Вознаграждение для майнеров PoW сокращается, в случае если включены только 3 или 4 голоса, на 40% и 20% соответственно. Именно так пресекаются действия майнеров, направленные на игнорирование голосов и осуществляемые в попытке обмануть систему.  Очень важным является то, что стейкхолдеры **должны присутствовать** в заданном чейне, когда их тикеты выбираются. Получение тикета не означает, что он автоматически голосует, ваш кошелёк (или ваш «Voting Service Provider») должен отдать ваш голос в момент, когда тикет выбирается. Это крайне важная особенность, так как она означает, что пул тикетов «live» при миноритарном форке преимущественно состоит из тикетов, не принимающих участие в голосовании, так как их владельцы находятся в другом чейне.  Более детальный обзор теории, на которой базируется каждый из данных аспектов, выходит за рамки этого поста. Тем не менее, речь идёт преимущественно о предотвращении всевозможных конфликтных ситуаций.  **Сценарий, предположения и методология**  Не забывая обо всём вышеупомянутом, давайте представим себе сценарий, в котором какой-то участник делает попытку осуществить форк, с которым не согласны 75% стейкхолдеров.  Давайте предположим, что обе стороны замышляемого форка обладают равной хеш-мощностью (а именно, 50% на каждый форк). Как указано выше, 75% стейкхолдеров находятся в мажоритарном чейне, а 25% – в миноритарном чейне.  Также давайте предположим, что самый последний блок на момент форка – это блок 99999. Следовательно, обе стороны форка работают над поиском блока 100000, одна сторона – по миноритарному набору правил, а другая – по мажоритарному набору правил.  И наконец, чтобы упростить изложение этого материала и чтобы его логика была более понятной, давайте предположим следующее. Так как только 25% стейкхолдеров находятся в миноритарном чейне, давайте представим, что каждый 4-й тикет в пуле тикетов «live» – это стейкхолдер в миноритарном чейне. Другими словами, тикеты 0, 4, 8, 12, 16, 20, …, 40956 – это тикеты в пуле «live», которые относятся к стейкхолдерам в миноритарном чейне, а тикеты 1, 2, 3, 5, 6, 7, 9, …, 40957, 40958, 40959 – это тикеты в пуле «live», которые относятся к стейкхолдерам в мажоритарном чейне.    Не забывайте: стейкхолдеры **должны присутствовать** в заданном чейне, когда их тикеты выбираются, чтобы иметь возможность отдавать свои голоса.  Иллюстрация воображаемого сценария.  **Пошаговое объяснение**  Далее будет представлена цепочка событий, которые произойдут в случае сценария, включающего попытку форкинга, согласно изложенному выше объяснению и иллюстрации.  **Блок 100000**   * Хеш-мощность в обоих чейнах будет пытаться построить новый блок на блоке 99999. * Чтобы этот новый блок был построен в миноритарном чейне, он должен получить как минимум 3 голоса из пула тикетов «live», а выбранные голоса будут зависеть от блока 99999. * Тикеты, необходимые для построения блока 100000, базирующегося на хеше блока 99999, – это номера тикетов 17113, 17331, 21307, 21328 и 24903. * Очевидно, что 4 из этих 5 тикетов – это стейкхолдеры в мажоритарном чейне (номера тикетов 17113, 17331, 21307 и 24903). Это означает, что они будут голосовать за блок 100000 в мажоритарном чейне. * Миноритарный чейн может получить только один голос (номер тикета 21328), поэтому он не может построить блок 100000. Вместо этого, он должен вернуться и найти новое решение для блока 99999, чтобы сформировать новый набор тикетов для последующего отбора.   На данном этапе, чейны выглядят таким образом. Скобки с символом \* в этом случае означают блоки, над которыми ведётся работа.  ... -> [99999] -> (100000\*)  мажоритарные стейкхолдеры (75%) находятся в этом чейне  \-> (99999a\*)  миноритарные стейкхолдеры (25%) находятся в этом чейне  Другими словами, мажоритарный чейн сейчас работает над блоком 100000, а миноритарный чейн останавливается в поиске нового решения для блока 99999, чтобы получить новый набор тикетов в надежде, что в этот раз они смогут получить как минимум 3 голоса. В связи с тем, что в нашем мысленном эксперименте оба чейна обладают равной хеш-мощностью, мы можем с уверенностью предположить, что в среднем блок 100000 в мажоритарном чейне и новый блок 99999 (назовём его 99999a) в миноритарном чейне будут найдены приблизительно в одно и то же время.  **Блок** **Block 100001**  На данном этапе произойдёт следующее:   * Хеш-мощность в мажоритарном чейне будет пытаться построить новый блок на блоке 100000 мажоритарного чейна. Голоса, необходимые для этого блока, – это номера тикетов 563, 6766, 21009, 37394 и 37775. * В этот раз все 5 из этих 5 тикетов – это стейкхолдеры в мажоритарном чейне. Это означает, что они предоставят свои голоса за блок 100000 в мажоритарном чейне, и благодаря этому построение блока 100001 будет возможным. * Миноритарный чейн, теперь с новой версией блока 99999 (99999a) обладает новым хешем, поэтому ему нужны номера тикетов 1069, 8007, 16413, 19172 и 31821. * Миноритарный чейн по-прежнему может получить только 1 голос (номер тикета 19172), поэтому он должен ещё раз вернуться назад и найти ещё одно решение для блока 99999, чтобы создать новый набор тикетов для последующего отбора.   Чейны теперь выглядят таким образом:  ... -> [99999] -> [100000] -> (100001\*)  мажоритарные стейкхолдеры (75%) находятся в этом чейне  \-> (99999b\*)  миноритарные стейкхолдеры (25%) по-прежнему находятся в этом чейне  Другими словами, мажоритарный чейн теперь работает над блоком 100001, а миноритарный чейн ещё раз останавливается в поисках ещё одного решения для блока 99999, чтобы получить новый набор тикетов в надежде, что в этот раз они смогут получить как минимум 3 голоса. В связи с тем, что в нашем мысленном эксперименте оба чейна обладают равной хеш-мощностью, мы опять можем с уверенностью предположить, что в среднем блок 100001 в мажоритарном чейне и новый блок 99999 (назовём его 99999 b) в миноритарном чейне будут найдены приблизительно в одно и то же время.  **Блок 100002**  На данном этапе произойдёт следующее:   * Хеш-мощность в мажоритарном чейне будет пытаться построить новый блок на блоке 100001 мажоритарного чейна. Голоса, необходимые для этого блока, – это номера тикетов 174, 1999, 12808, 31928 и 38317. * В этот раз 3 из этих 5 тикетов – это стейкхолдеры в мажоритарном чейне (номера тикетов 174, 1999, 38317). Это означает, что они предоставят свои голоса за блок 100001 в мажоритарном чейне, и благодаря этому построение блока 100002 будет возможным. * Миноритарный чейн, теперь с новой версией блока 99999 (99999 с), обладает новым хешем, поэтому ему нужны номера тикетов 4653, 15211, 29988, 35175 и 35665. * Миноритарный чейн по-прежнему может получить только 1 голос (номер тикета 29988), поэтому он должен ещё раз вернуться назад и найти ещё одно решение для блока 99999, чтобы создать новый набор тикетов для последующего отбора.   Чейны теперь выглядят таким образом:  ... -> [99999] -> [100000] -> [100001] -> (100002\*)  мажоритарные стейкхолдеры (75%) находятся в этом чейне  \-> (99999c\*)  миноритарные стейкхолдеры (25%) по-прежнему находятся в этом чейне  Другими словами, мажоритарный чейн теперь работает над блоком 100002, а миноритарный чейн ещё раз останавливается в поисках ещё одного решения для блока 99999, чтобы получить новый набор тикетов в надежде, что в этот раз они смогут получить как минимум 3 голоса.  **Быстрая перемотка к блоку** **100010**  Эта процедура повторяется до тех пор, пока, в конце концов, какой-то версии блока 99999 в миноритарном чейне не посчастливится выбрать 3 тикета в миноритарном чейне. Вероятность такого развития событий 1:10. И когда это случится, то чейны будут выглядеть следующим образом:  ... -> [99999] -> [100000] -> [100001] -> [100002] -> ... -> [100009] -> (100010\*)  мажоритарные стейкхолдеры (75%) находятся в этом чейне  \-> [99999j] -> (100000a\*)  миноритарные стейкхолдеры (25%) по-прежнему находятся в этом чейне  Очевидно, что, так как оба чейна характеризуются равной хеш-мощностью, миноритарный чейн ни в коем случае теперь не может догнать мажоритарный чейн. Более того, такая же процедура будет повторяться для миноритарного блока 100001, и он должен будет возвращаться и заново майнить (искать новые решения) для своего блока 100000 снова и снова, пока ему не посчастливится ещё раз получить 3 голоса, которые ему необходимы.  Как следствие, *майнеры не будут оставаться* в миноритарном чейне, потому что они практически не получают в нём никаких вознаграждений. Миноритарный чейн никогда не будет прибыльным, и поэтому вся майнинговая активность рано или поздно вернётся к мажоритарному чейну.  **Распространённые возражения**  **Что случится, если миноритарный чейн получит хеш-мощность, в 10 раз превышающую хеш-мощность главного чейна?**  Теоретически, если миноритарный чейн, утверждённый только 25% стейкхолдеров, получит хеш-мощность, в 10 раз превышающую хеш-мощность главного чейна, он может успешно конкурировать с мажоритарным чейном. Тем не менее, этот сценарий не является реалистичным по причине экономических поощрений.  Майнинг миноритарного чейна с 10-кратной хеш-мощностью на практике означает, что майнеры могут получить лишь 1/10 того вознаграждения по блоку, которое они могли бы получить в мажоритарном чейне, исходя лишь только из хеш-мощности. В нашем сценарии это вознаграждение сокращается ещё больше: это 1/10 от 60% из-за того, что среднем можно включить только 3 голоса. Это означает, что майнеры получают только 6% вознаграждения, которое они могли бы получить в результате майнинга в мажоритарном чейне. Если посмотреть на проблему под другим углом, то они получают на 94% меньше, занимаясь майнингом в миноритарном чейне.  Говоря языком цифр, если, к примеру, майнер обладает 5% общей хеш-мощности сети, он может получить приблизительно 5% вознаграждения PoW за один блок или 5% от ~13,89 ≈ 0,6945 DCR на [данный момент](https://www.reddit.com/r/decred/comments/7f9ie1/detailed_analysis_of_decred_fork_resistance/). Тем не менее, в миноритарном чейне поначалу вознаграждение составляет 60% от ~13,89 ≈ 8,334 DCR, а затем 5% хеш-мощности будет составлять лишь 0,5% от общей хеш-мощности в миноритарном чейне: таким образом, 0,5% от ~8,334 ≈ 0,04167 DCR. Проанализировав эти цифры, можно сделать вывод, что 0,04167 DCR это в действительности 6% от 0,6945 DCR.  Майнинг PoW отличается *очень* сильной конкуренцией, так как это игра с нулевой суммой. Большинство майнеров, даже те, которые обладают большими преимуществами (как, например, бесплатное электричество), работают с небольшими прибылями и зачастую полагаются на повышение ценности в будущем, чтобы наверстать упущенное. Учитывая сокращение дохода на 94%, большинство майнеров фактически должны платить за то, чтобы майнить в миноритарном чейне.  **Может ли кто-то изменить правила консенсуса для того, чтобы игнорировать стейкхолдеров?**  Если бы миноритарный чейн мог устранять или деактивировать голосование по тикетам на определённый период, то он мог бы создавать блоки и осуществлять форки за пределами мажоритарного чейна. Это теоретически возможно. Тем не менее, такие действия бы полностью разрушили гибридную систему и превратили бы разделённую после форка валюту в классическую сеть PoW. И это, безусловно, уже не будет Decred.  В случае классических монет PoW, никто не может с уверенностью утверждать, какой чейн является «настоящим» по причине отсутствия доказуемой и формализированной системы управления. В отличие от монет PoW, Decred обладает очень чёткой и понятной моделью управления. Стейкхолдеры Decred принимают решение касательно того, какой чейн является настоящим и соответствует принципам Decred, и они это делают в манере он-чейн, которая может быть доказана криптографически.  Стейкхолдеры регистрируются на Decred, ожидая, что ключевые консенсусные решения будут приниматься самими стейкхолдерами. Лишить стейкхолдеров полномочий – это всё равно, что исключить Proof-of-Work из классической монеты PoW. Другими словами, это полностью нивелирует особенности системы, связанные с безопасностью. Как повлияет на уровень доверия стейкхолдеров к монете, если эта монета будет игнорировать одну из ключевых характеристик, которую она пообещала предоставить?  **Вывод**  Благодаря гибридной консенсусной системе Decred на основе PoW и PoS, осуществление форков блокчейна является крайне сложной задачей (если не невозможной), при условии отсутствия утверждения большинством стейкхолдеров. Обзор продемонстрировал, почему сценарий Classic, Gold или Cash крайне маловероятен для сети Decred.  Затраты на поддержание миноритарного форка даже с 10-кратной хеш-мощностью очень существенные; майнеры могут ожидать серьёзное сокращение дохода, если они решат принять участие. В качестве альтернативы, можно устранить и деактивировать систему PoS, и разделить чейн Decred, как любую другую сеть PoW. Тем не менее, это противоречит миссии Decred, и очень сомнительно, что кто-либо всерьёз решится на такой шаг.  Правильное понимание основ устойчивости к форку является очень важным для обеспечения долговечности проекта. Гибридная система PoW и PoS гарантирует сдержки и противовесы, чтобы маленькие группы не могли доминировать над потоком транзакций или производить изменения в Decred без получения согласия со стороны стейкхолдеров. Это поощряет согласованность и сотрудничество, и именно эти характеристики превращают Decred в исключительно сильную сеть, которая нацелена на долгосрочную перспективу.  **Дополнительные материалы**  В этом посте была изложена важная тема, касающаяся устойчивости к форку, но ещё есть много других аспектов, на которые нужно обратить внимание. Например, гибридная система (PoW и PoS) Decred обладает высоким уровнем защиты от мажоритарных (51%) атак. Если вам интересно было узнать, как это работает, вы можете прочесть пост от [Zubair Zia](https://medium.com/@zubairzia):    [Гибридный протокол Decred в качестве средства защиты от мажоритарных атак.](https://medium.com/decred/decreds-hybrid-protocol-a-superior-deterrent-to-majority-attacks-9421bf486292)  [Эта статья демонстрирует то, как уникальный гибридный протокол Decred предоставляет высокий уровень защиты от мажоритарных атак.](https://medium.com/decred/decreds-hybrid-protocol-a-superior-deterrent-to-majority-attacks-9421bf486292)  [medium.com](https://medium.com/decred/decreds-hybrid-protocol-a-superior-deterrent-to-majority-attacks-9421bf486292)  Что касается более продвинутых тем, вы можете узнать, как Decred может беспрепятственно осуществлять апгрейд своей сети посредством [голосования по изменениям к правилу консенсуса](https://medium.com/decred/blockchain-governance-how-decred-iterates-upon-bitcoin-3cc7030c655e), или как люди могут отправлять предложения в [офф-чейн системе управления, которая называется Politeia](https://docs.decred.org/governance/politeia/). Если вам нужна техническая информация, пожалуйста, ознакомьтесь с [документацией Decred](https://docs.decred.org/governance/politeia/).  Выберите одну из платформ для чатов, перечисленных [тут](https://www.decred.org/community/), если вы бы хотели пообщаться с представителями сообщества Decred. Мы являемся прагматичной группой людей — присоединяйтесь к нам!  **Кто сделал вклад в написание этого поста**  Если бы не [исходный анализ от davecgh](https://www.reddit.com/r/decred/comments/7f9ie1/detailed_analysis_of_decred_fork_resistance/), этот пост, возможно, не был бы опубликован. Кроме того, обзор от [Artikozel](https://medium.com/@artikozel) и конструктивные комментарии в «writers room» кардинально улучшили это пост. Иллюстрация для сценария была создана [Zubair Zia](https://medium.com/@zubairzia). Спасибо вам всем! |